Post Schrems II Customer Assurance Guide

Introduction

NAVEX Global recognizes the importance of data protection and is committed to protecting customer data that is entrusted to us. As part of that commitment, we understand that recent decisions by the European Union Court of Justice have raised questions for our customers. NAVEX Global has provided, and will continue to provide, proactive communication with its customers. We are continuously assessing the impact this may have on our customers to support their compliance objectives.

Please read below for information on our data processing activities and how we safeguard personal data transferred from the European Union (EU), European Economic Area (EEA), and United Kingdom (UK) to our facilities and sub-processors in the United States (US) and other third countries in order to best ensure that the adequate level of protection is afforded to European individuals.

Table of Contents

Schrems II Decision Overview

Since the Court of Justice of the European Union (CJEU) released its ruling that Privacy Shield is no longer an adequate method to transfer personal data from the EEA to the US, organizations have been assessing another facet of the court's decision, the viability of the Standard Contractual Clauses (SCCs). The validity of the SCCs, the CJEU underlined, depends on whether "the level of protection of natural persons guaranteed by [the GDPR] is not undermined." The court held that other transfer mechanisms, including the SCCs, must still provide the "essential equivalence" to the protections afforded in the GDPR.

On 4 June 2021, the European Commission finalized and adopted the new set of standard contractual clauses ("New SCCs"). The New SCCs replace prior versions of the SCCs (the "Old SCCs"), some of which date back to 2001 and pre-date the GDPR. The New SCCs serve as an appropriate safeguard for the legitimate transfer of personal data from the EU to third countries. The New SCCs came into force 27 June 2021. Organizations have a 3-month grace period from the foregoing date to rely on the existing SCCs for new transfers and an 18-month grace period from the foregoing date to replace the old standard contractual clauses with the New SCCs for existing contracts.

While the New SCCs do address several concerns raised by the Schrems II decision, on 18 June 2021 the European Data Protection Board (EDPB) also adopted its final recommendations on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (the "EDPB Recommendations"). The EDPB Recommendations are designed to assist data exporters with assessing their transfers. They provide some examples of supplementary measures that could be put in place alongside the SCCs where applicable.

On 11 August 2021, the UK Commissioner's Office (ICO) launched a consultation on its draft international data transfer agreement ("IDTA") and guidance for organizations on international transfers (the "Guidance"). Once finalized, the IDTA will replace the existing EU Standard Contractual Clauses ("SCCs") in the UK. The consultation follows both the UK's exit from the EU and the Schrems II decision. The New SCCs from the European Commission do not apply in the UK following the UK's departure from the EU. The ICO must therefore publish its own set of SCCs under the UK GDPR (the GDPR as incorporated into the law of the UK). The consultation is open until 7 October 2021. As such, organizations must continue relying on the old version of the SCCs to account for transfers from the UK to third countries, until the UK publishes its version. NAVEX Global is committed to updating its agreements and documentation in a timely manner once the UK finalizes IDTA and Guidance.

Do the SCCs Remain a Valid Mechanism for Transfers to the United States?

In its determination that US laws do not ensure an essentially equivalent level of protection, the court cited the breadth of U.S. surveillance programs (particularly Section 702 of FISA and Executive Order 12333). Therefore, although the old SCCs were not strictly invalided by the Schrems II decision, their validity depended on whether there were effective mechanisms in place to ensure the essentially equivalent level of protection is afforded to European individuals.

Now that the much-anticipated New SCCs and final EDPB Recommendations are both in force, a full analysis can and has been conducted by NAVEX Global. While the New SCCs themselves contain a number of contractual commitments aimed at serving as safeguards for EU personal data, Step 3 of the EDPB Recommendations require organizations relying on the New SCCs to assess whether they are effective in light of all circumstances of the transfer. Data exporters may decide to proceed with the transfer without supplementary measures, if they consider there to be no reason to believe that the relevant and problematic legislation (those in the U.S. in this instance) will be applied, in practice, to the transferred data and/or NAVEX Global.

In NAVEX Global's reasonable opinion upon internal and outside counsel review, it does not find US surveillance laws, including Section 702 FISA and Executive Order 12333, to practically apply to its transfers. A key factor organizations should be assessing are the circumstances surrounding the transfers, including the scope and application of US surveillance programs on the US based data importer. They may consider the industry sector, for example (some industries may rarely

be the subject of US government surveillance and therefore pose a minimal risk). To this point, **NAVEX Global has never received a FISA or EO 12.333 request**. While NAVEX Global takes the approach that applicable problematic legislation does not apply in practice, we still have elected to provide for supplementary measures with regard to its transfers. Please read the NAVEX Global Transfer Risk Assessment section below for full details of our assessment and analysis.

Customer Assurance Guide: New Controller to Processor Standard Contractual Clauses

We are applying the New Controller to Processor SCCs (Module Two) with those customers who have elected US hosting and/or are contracted directly with our US entity, NAVEX Global, Inc.

To assist our customers in their evaluation of whether the new standard contractual clauses adopted pursuant to the European Commission's Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council C/2021/3972 ("the Clauses") provide sufficient protection of personal data transferred to NAVEX Global as its processor, we have prepared the below analysis of NAVEX Global's compliance with the Clauses. We encourage you to read the Clauses alongside our assurance guide.

SECTION I

Clause 1 Purpose and scope

(a) NAVEX Global fully endorses the purpose of these Clauses to ensure compliance with the GDPR for the transfer of personal data to third countries.

(b) Our customers are the data exporters and NAVEX Global is the data importer.

(c) We have completed Annex I.B in detail on behalf of our customers.

(d) NAVEX Global understands the Appendix to the Clauses containing the Annexes form an integral part of the Clauses.

Clause 2 Effect and invariability of the Clauses

(a) NAVEX Global understand these Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies under Article 46(1) and Article 26 (2)(c) of the GDPR. For data transfers, we understand these Clauses set out appropriate safeguards pursuant to Article 28 (7) of the GDPR provided they are not modified outside of selecting the appropriate Module(s) or to complete and update the content of the Appendix. NAVEX Global will not modify the Clauses in accordance with the foregoing. Any wider contract or additional Clauses between ourselves and our customers will not contradict these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) We understand that these Clauses are without prejudice to the obligations which our customers, as the data exporters, are subject to under the GDPR.

Clause 3 Third-party beneficiaries

(a) NAVEX Global understands Clause 3 of the Clauses enables data subjects to invoke and enforce these Clauses as third-party beneficiaries against our customers and/or NAVEX Global, subject to a list of exceptions set forth in Clause 3 (a).

(b) We understand the exceptions set forth in Clause 3 (a) is without prejudice to the data subject rights set forth in the GDPR.

Clause 4 Interpretations

(a) NAVEX Global understands where these Clauses use terms defined under the GDPR, those terms shall have the same meaning as in the GDPR.
(b) We will read and interpret these Clauses in light of the provisions of the GDPR.
(c) NAVEX Global will not interpret these Clauses in a way that conflicts with the rights and obligations under the GDPR.

Clause 5 Hierarchy

NAVEX Global understands in the event of a contradiction between these Clauses and the provisions of related agreements between ourselves and our customers, these clauses shall prevail.

Clause 6 Description of the transfer(s)

NAVEX Global has completed Annex I.B on behalf of its customers, which provide details of the transfers, the particular categories of personal data transfers, and the purposes for which they are transferred.

Clause 7 Optional - Docking clause

(a) NAVEX Global understands Clause 7 is Optional. An entity that is not Party to these Clauses, upon agreement between ourselves and our customers, may accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.
(b) We understand that once the new entity completes the Appendix and signs Annex I.A, the acceding entity becomes a Party to these Clauses and shall have the rights and obligations of a data exporter or data importer in accordance with the applicable designation in Annex I.A.
(c) NAVEX Global agrees the new entity shall have no rights or obligations under these Clauses prior to becoming a Party to these Clauses in accordance with the foregoing.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8 Data protection safeguards

Clause 8 requires our customers, as the data exporters, to warrant they have used reasonable efforts to determine NAVEX Global, as the data importer, is able to satisfy the obligations under these Clauses through the implementation of appropriate technical and organsational measures. NAVEX Global agrees to support its customers with these efforts in order for them to make this warranty.

MODULE TWO: Transfer controller to processor

8.1 Instructions

(a) NAVEX Global processes the personal data only on the documented instructions from its customers as the data exporters. We understand our customers may give us such instructions throughout the duration of our agreement.
(b) NAVEX Global agrees to immediately inform its customers if we are unable to follow its instructions.

8.2 Purpose Limitation

NAVEX Global agrees to process the personal data only for the specific purposes of the transfer, unless on further instructions from its customers. We have completed Annex I.B on behalf of our customers.

8.3 Transparency

This Clause requires our customers to provide a copy of these Clauses, including the Appendix completed by ourselves and our customer, available to a data subject on request and free of charge. NAVEX Global supports customer with the foregoing requirement. In accordance with this Clause, we agree to redact any text of the Appendix that includes business secrets or other confidential information prior to sharing a copy. However, we have elected to complete the requisite details of the Appendix without including what we would consider to be business secrets or other confidential information, to seamlessly be able to provide copies of these Clauses to data subjects. In any event, we will support the customer with its decisions regarding the requirements of this Clause, including assistance with a meaningful summary for any chosen redacted sections, where the data subject would otherwise not be able to understand the content or exercise their rights. We will also support with any reasonings for elected redactions. NAVEX Global understands this Clause is without prejudice to its customers obligations under Articles 13 and 14 of the GDPR.

8.4 Accuracy

This Clause requires NAVEX Global, as the data importer, to inform our customers without undue delay if we become aware that the personal data we have received is inaccurate or has become outdated. We commit to providing our customers this information to the extent we are aware, however, please note that given the nature of the services we provide, we won't be in a position to determine whether or not the personal data submitted to our services is inaccurate out of date. Further, our customers typically do not want NAVEX Global making such determinations. Regardless, we commit to compliance with this Clause. NAVEX Global also generally cooperates with its customers to erase or rectify personal data. Typically, our customers are able to manage the personal data within our services on their own through the use of such services. To the extent you need assistance or are unable to rectify and/or delete the personal data on your own, we will fully cooperate.

8.5 Duration of processing and erasure or return of data

NAVEX Global has specified the duration of the processing in Annex I.B. Please know that the duration will be for as long as we are providing our customers the applicable services in accordance with our agreements. Throughout the term of our agreements, our customers are typically able to manage the personal data within our services on their own through the use of such services. To the extent you need assistance or are unable to perform a desired function on the personal data on your own, we will fully cooperate. Our customers, as the data exporters and the data controllers, manage the personal data in accordance with their own retention requirements throughout the life of the agreement. At the end of our applicable relationship, where we are no longer providing our customer the processing services, we agree, at your choice, to delete all personal data

processed on your behalf and certify via email that we have done so or return to you all personal data processed on your behalf and we will delete existing copies. We will certify any deletion via email regardless. Deletion and returning of our customer's data at the end of the relationship is typically reflected in our agreements. Our process is to reach out to you to wind up your services, allowing you to retrieve your data on your own for a certain timeframe or, if applicable, allowing you to purchase a data export from us if you desire. When everything is completed and/or confirmed as applicable, we will delete all customer data in its entirety. Customer data stored in back-ups shall be overwritten in accordance with our backup and retention cycle. Until the data is deleted or returned (and copies deleted in this instance), we will continue to ensure our processing is in compliance with these Clauses. In case there is a local law applicable to NAVEX Global that would prohibit our ability to return or delete the personal data, we warrant we will continue to ensure compliance with these Clauses and would only process it to the extent and for as long as is required under that local law. At this time, no local laws applicable to NAVEX Global prohibit our ability to return or delete personal data in accordance with these Clauses. NAVEX Global understands the foregoing is without prejudice to the requirements under Clause 14, especially the requirement under Clause 14 (e) requiring us to notify our customers throughout the duration of our agreement if we have reason to believe that we are or have become subject to laws or practices not line with the requirements under Clause 14 (a).

8.6 Security of processing

- **(a)** NAVEX Global has implemented and is committed to the continuous implementation of appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data ("personal data breach"). Our customers shall also implement the foregoing measures during transmission of the data to NAVEX Global. When we assess what the appropriate level of security is, we take into account the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. We take particular consideration to encryption or pseudonymisation, including during transmission, where the purpose of the processing can be fulfilled in this manner. In the event pseudonymisation is used, we commit to, where possible, keeping the additional information for attributing the personal data to a specific data subject under the exclusive control of our customers. At the very least, NAVEX Global will implement the technical and organisational measures specified in Annex II. We have completed Annex II on behalf of our customers. NAVEX Global carries out regular checks on its security operations as part of its information security program to ensure these measures continue to provide an appropriate level of security. We offer a Data Security Addendum for which we are happy to provide and execute with our customers upon request. NAVEX Global also maintains a Standard Gathering Information (SIG) questionnaire, which details all of our technical and organisational measures, along with all of our supporting policies and processes. The SIG can also be provided upon request.
- **(b)** NAVEX Global follows the principle of least privilege with respect to access to personal data by its personnel. We ensure access is granted only to the extent strictly necessary for the implementation, management and monitoring of the contract. Select individuals required for support, administrative, technical, and security functions have varying levels of access dependent upon their job duties as required to fulfill our agreements with our customers. All personnel with access to customer data are under appropriate confidentiality agreements or are under appropriate statutory obligation of confidentiality.
- **(c)** NAVEX Global has robust incident response processes and policies in place. Specifically, in the event of a personal data breach we will take appropriate measures to address the breach, including taking

measures to mitigate any adverse effects. Our process and commitment include notifying our customers without undue delay after we become aware of a breach. We commit to include a point of contact for where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects, in such notifications. If we are unable to provide all the foregoing information at the same time, the initial notification shall contain the information then available and we will send further information as it becomes available without undue delay.

(d) NAVEX Global commits to cooperating and assisting its customers to enable them to comply with their obligations under the GDPR, especially to assist them in notifying the competent supervisory authorities and the affected data subjects, taking into account the nature of the processing and the information available to us.

8.7 Sensitive data

It is possible for sensitive data to be submitted to certain services NAVEX Global provides. The most common circumstance would be through our EthicsPoint services, where a whistleblower reporter may submit personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("sensitive data"). We have completed Annex I.B on behalf of our customers, which details the specific restrictions and/or additional safeguards as required by this Clause. The extent of the processing of such sensitive data post submission by the individual is determined and controlled by our customer in their sole discretion.

8.8 Onward transfers

NAVEX Global only discloses customer personal data under the agreement to third parties on documented instructions from the customer. We also only disclose the data to third parties outside the European Union if the third party is or agrees to be bound by these Clauses under the appropriate Module. Please see Clause 9 below for the details around our use of sub-processors. All applicable sub-processors involving onward transfers ensure appropriate safeguards pursuant to Article 46 or Article 47 of the GDPR. We have entered into appropriate data processing addendums with all sub-processors. Where applicable, our sub-processor data processing addendums include, or will include, the Clauses under Module Three (Processor to Processor). Any standard contractual clauses still in process with our applicable sub-processors are within the applicable grace periods for implementation and execution. Other compliant ways to engage in such onward transfers include: (i) having the third party agree to these Clauses by docking under Clause 7; (ii) transferring to a country under an adequacy decision; (iii) where the transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or (iv) where the transfer is necessary in order to protect the vital interests of the data subject or of another natural person. NAVEX Global understands that any onward transfer is subject to compliance by us with all other safeguards under the Clauses, in particular purpose limitation. We only process customer data for the purpose of providing services under the agreement and in accordance with our customer's documented instructions.

8.9 Documentation and compliance

(a) NAVEX Global is fully committed to promptly and adequately dealing with enquiries from its customer that relate to the processing under these Clauses.

(b) We will keep appropriate documentation on the processing activities carried out on behalf of our customers. NAVEX Global has completed Annex I. A on behalf of its customers, which sets forth the records of processing activities for data processors. Please also refer to our agreements for specifics regarding the services themselves. If there is additional documentation you may require, please let us know and we will promptly assist.

(c) Upon our customer's request, NAVEX Global will make available all information necessary to demonstrate compliance with the obligations set forth in these Clauses. We allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. NAVEX Global supports onsite and desk audits. We contractually require reasonable parameters be put in place to allow us to support the audit. For example, we require any onsite audit to be conducted during regular business hours and with reasonable notice. Additionally, we contractually ask our customers in good faith to take into account our relevant certifications in deciding on a review or audit, which in our opinion include our SOC 2 Audit Report plus all of our SIG and other relevant documentation made readily available.

(d) NAVEX Global understands its customers may choose to conduct the audit on their own or utilize an independent auditor. We contractually require any independent auditors to execute a confidentiality and non-disclosure agreement as presented by and for the benefit of all parties involved. In accordance with these Clauses, we permit inspections at our premises or applicable physical facilities with reasonable notice.

(e) On request from a competent supervisory authority, we will make the information referred to in this Clause, including any audit results, available. Please note our customers are required to do the same.

Clause 9 Use of sub-processors

MODULE TWO: Transfer controller to processor

Clause 9 sets forth two options for how our customers can provide authorisation of sub-processors. NAVEX Global has selected OPTION 2: GENERAL WRITTEN AUTHORISATION. In accordance with this Clause, we have our customer's general authorisation for the engagement of sub-processor(s) from an agreed list. The agreed list is our current list of sub-processors, set forth at the following link, as applicable: https://www.navexglobal.com/en-us/service-hosting-providers. The foregoing link contains a mechanism to subscribe to notifications of the addition of any new sub-processors, or the replacement of sub-processors, as required by this Clause. We agree to specifically inform our customers in writing via the foregoing subscription mechanism of any intended changes to this list through the addition or replacement of sub-processors at least thirty (30) calendar days in advance, thereby giving our customers sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). NAVEX Global will provide its customers the information necessary to enable them to exercise their right to object. We contractually require any objections to be reasonable and ask that they relate to the sub-processor's processing of personal data under these Clauses. Additionally, any objection by the customer must be sent to NAVEX Global in writing at privacy@navexglobal.com within thirty (30) days after receipt of our notice. In such event, the parties will work in good faith to discuss a resolution. NAVEX Global may choose to: (i) not use the sub-processor to process personal data for customer or (ii) take the corrective steps requested by customer in its objection and use the sub-processor. If neither of these options are reasonably possible and customer continues to object, customer

may provide notice of termination of the affected portion of the service as to customer.

We enter into robust data processing agreements with our sub-processors that provide for, or will provide for, in substance, the same data protection obligations as those binding NAVEX Global under these Clauses, including in terms of third-party beneficiary rights for data subjects. NAVEX Global understands that by complying with this Clause, we fulfil our obligations under Clause 8.8. We will ensure our sub-processors comply with the obligations to which data importers are subject pursuant to these Clauses.

Upon our customer's request, we will provide them a copy of the applicable sub-processor agreement and any subsequent amendments. In order to protect the parties involved, we will redact text from these agreements as permitted by this Clause to protect business secrets or other confidential information, including personal data.

NAVEX Global understand and agrees it is fully responsible to its customers for the performance of the sub-processor's obligations under the agreements between ourselves and our sub-processors. We will notify our customers of any failure by the sub-processors to fulfil their obligations under the agreement between ourselves and our sub-processors. We interpret the foregoing as pertaining to any failure by the sub-processor that materially impacts the services NAVEX Global provides to its customers, or to any failure pertaining to the sub-processor's compliance with the Clauses or other applicable data protection obligations.

Our agreements with our sub-processors include, or will include, a third-party beneficiary clause whereby – in the event the sub-processor has factually disappeared, ceased to exist in law or has become insolvent – we have the right to terminate the sub-processor agreement and to instruct the sub-processor to erase or return the personal data, as applicable.

Clause 10 Data subject rights

MODULE TWO: Transfer controller to processor

(a) NAVEX Global's process is to notify its customers in the event it received a data subject request. Please note this is a rare occurrence and we always forward those directly to the applicable customer promptly upon receipt. We will not respond to the request ourselves unless our customers authorise us to do so. Notwithstanding the foregoing, we do confirm receipt with the data subject and let them know we have sent the request to the applicable customer. We believe this is appropriate in order to support the data subject under applicable data protection obligations. NAVEX Global does not foresee any reason for our customers to authorise us to respond otherwise to a data subject request but will of course assist and cooperate as needed or required.

(b) We will assist our customers in fulfilling their obligations to respond to data subject rights requests under the GDPR. NAVEX Global has completed Annex II on behalf of its customers, which detail the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and extent of the assistance required.

(c) In fulfilling the above obligations, NAVEX Global will comply with its customer's instructions.

Clause 11 Redress

(a) NAVEX Global informs data subjects in a transparent and easily accessible format, through our Privacy Statement available on our website (https://www.navexglobal.com/en-us/privacy-statement), of a contact point authorised to handle complaints. For avoidance of doubt, data subjects are directed to contact privacy@navexglobal.com. For unresolved privacy or data use concerns that we have not

addressed satisfactorily under our Privacy Shield requirements, data subjects can contact our U.S.-based third party dispute resolution provider (free of charge) at https://feedback-form.truste.com/watchdog/request. Under certain conditions, more fully described on the Privacy Shield website [https://www.privacyshield.gov/article?id=How-to-Submit-a-Complaint], data subjects may be entitled to invoke binding arbitration when other dispute resolution procedures have been exhausted. Data subjects are not required to use our third party dispute resolution provider, nor do they have to follow a particular sequence in seeking redress.

MODULE TWO: Transfer controller to processor

(b) NAVEX Global agrees to use best efforts to resolve any disputes between a data subject and one of the parties to these Clauses as regards compliance with these Clauses in an amicably and timely fashion. We agree to keep everyone informed about such disputes and will cooperate in resolving them where appropriate.

(c) Where a data subject invokes a third-party beneficiary right under Clause 3 of these Clauses, NAVEX Global will accept the data subject's decision to: (i) lodge a complaint with the supervisory authority in the Member State of where they reside or where they work, or the competent supervisory authority pursuant to Clause 13; and/or (ii) refer the dispute to competent courts pursuant to Clause 18.

(d) NAVEX Global understands the data subject may be represented by a not-for-profit body, organisation or association under the conditions within Article 80(1) of the GDPR.

(e) We will abide by a decision that is binding under the applicable EU or Member State law.

(f) NAVEX Global understands and agrees that the choice made by the data subject will not prejudice their substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12 Liability

MODULE TWO: Transfer controller to processor

(a) NAVEX Global agrees and understands it shall be liable to the other party/ies for any damages it may cause such party by any breach of these Clauses.

(b) We also understand and agree we shall be liable to a data subject, and that data subjects will be entitled to receive compensation, for any material or non-material damages NAVEX Global or its sub-processors cause such data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b) above, our customers shall be liable to such data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages themselves or NAVEX Global (or its sub-processors) causes to such data subject by breaching the third-party beneficiary rights under these Clauses. The foregoing is without prejudice to the liability of our customers and, if our customer is a processor acting on behalf of a controller (if applicable), to the liability of the controller under the GDPR or Regulation (EU) 2018/1725.

(d) NAVEX Global agrees and understands that if its customer is held liable under paragraph (c) above for damages caused by NAVEX Global (or its sub-processors), its customer shall be entitled to claim back from NAVEX Global that part of the compensation corresponding to our responsibility for the damage.

(e) We agree and understand if more than one party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible parties shall be jointly and severally liable and the data subject is entitled to bring action in court against any of the parties.

(f) NAVEX Global agrees and understands if one party is held liable under paragraph (e) above, it shall be entitled to claim back from the other party/ies that part of the compensation corresponding to their responsibility of the damage.

(g) We may not invoke the conduct of a sub-processor to avoid our own liability. NAVEX Global has always contractually committed to being fully liable for its sub-processor's activities.

Clause 13 Supervision

MODULE TWO: Transfer controller to processor

(a) This Clause sets forth how to select the responsible supervisory authority, depending on the scenario. Where our customer, as the data exporter, is established in an EU Member State, the supervisory authority indicated in Annex I.C. shall be responsible for ensuring compliance by our customer with GDPR as regards the transfer. Where our customer, as the data exporter, is not established in an EU Member State, but is subject to the GDPR's territorial scope and has appointed a representative under Article 27(1) of the GDPR, the supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of the GDPR is established, as indicated in Annex I.C, shall act as competent supervisory authority. Where our customer, as the exporter, is not established in an EU Member State, but is subject to the GDPR's territorial scope without however having to appoint a representative under Article 27(2) of the GDPR, the supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of good and services to them, or whose behavior is monitored are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) NAVEX Global agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. We agree to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. NAVEX Global will provide the supervisory authority with written confirmation that any necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14 Local laws and practices affecting compliance with the Clauses

****NAVEX Global has performed appropriate transfer risk assessments to support our compliance, as well as our customer's compliance, with this Clause 14. Please see our full assurance guide for our transfer risk assessment documentation. ****

MODULE TWO: Transfer controller to processor

(a) NAVEX Global warrants we have no reason to believe the laws and practices in the third countries of destination applicable to the processing of personal data by us, including any requirements to disclose personal data or measures authorising access by public authorities, prevent NAVEX Global from fulfilling our obligations under these Clauses. The foregoing warranty is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed under Article 23(1) of the GDPR, are not in contradiction with these Clauses.

(b) In order to provide the foregoing warranty in paragraph (a) above, we have taken due account of the following elements:

(i) the specific circumstances of the applicable transfer(s), the length of the processing chain, the number of actors involved and transmission channels used, intended onward transfers, recipient type, purpose of processing, categories and format of the transferred personal data, the economic sector for which the transfer occurs, storage location of the data, and duration of a given processing activity (as applicable).

(ii) the laws and practices of the third country of destination, including those requiring the disclosure of data to public authorities or authorising access by such authorities, relevant considering the specific circumstances of the transfer, and the applicable limitations and safeguards. Please note we have also taken into account Footnote 12 for this portion of our assessment as authorised by these Clauses. The additional elements include our relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. NAVEX Global has internal records and implemented new documentation which shall continue to be drawn up on a continuous basis in accordance with due diligence at senior management level (specifically, our General Counsel, Data Privacy Officer, Deputy Compliance Officer, Senior Privacy Counsel, and Privacy Counsel). We will share this information with third parties to the fullest extent permitted by applicable law. NAVEX Global does take this practical experience into account but does not rely on it in totality to conclude we will not be prevented from complying with these Clauses. We support our assessment via all of the foregoing elements outlined above, along with other relevant and objective factors. NAVEX Global understands it is for the parties to consider carefully whether all the elements taken together carry sufficient weight in terms of their reliability and representatives to support this conclusion. We commit to corroborating our practical experience to ensure it is not contradicted by publicly available or otherwise accessible or reliable information on the existence or absence of requests within the same sector and/or the application of law in practice, such as case and reports by independent oversight bodies.

(iii) the relevant contractual, technical and organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of personal data in the country of destination. Please see NAVEX Global's full assurance guide for all the details around our use of and approach to supplementary measures.

(c) NAVEX Global warrants it has made best efforts to provide its customers with all relevant information in carrying out its transfer risk assessments and we agree we will continue to cooperate with our customers in ensuring compliance with these Clauses.

(d) We have documented our assessment on behalf of our customers and agree to make it available to competent supervisory authorities on request. Even though NAVEX Global has performed this assessment, we understand our customers may want to undertake their own assessments. We agree to support our customers with any assessments they wish to complete under these Clauses.

(e) NAVEX Global agrees and understands it must notify its customers promptly if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements of paragraph (a) above,

including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a) above.

(f) In the event we do notify our customer pursuant to paragraph (e) above, or if our customers have reason to believe NAVEX Global no longer can fulfil its obligations under these Clauses, we agree and understand our customers shall promptly identify appropriate measures to be adopted by the parties (as applicable) to address the situation. NAVEX Global understands its customers shall suspend data transfers to us if they consider that no appropriate safeguards for such transfer can be ensured, or if they are instructed by the competent supervisory authority to do so. We understand in this case, our customer shall be entitled to terminate the applicable agreement, insofar as it concerns the processing of personal data under these Clauses. If the applicable agreement involves more than two parties, the data exporter may exercise this right to termination only with respect to the relevant party, unless agreed upon otherwise. If an agreement is terminated under this Clause, Clause 16 (d) and (e) shall apply.

Clause 15 Obligations of the data importer in case of access by public authorities

****NAVEX Global has updated its Requests for Disclosure of Customer Data Policy to support our compliance, as well as our customer's compliance, with this Clause 15. Please see our full assurance guide for a copy of this policy. ****

MODULE TWO: Transfer controller to processor

15.1 Notification

(a) NAVEX Global agrees it will notify its customer and, where possible, the data subject promptly (if necessary with the help of our customer) if we:
(i) receive a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses. Any such notification will include information about the personal data requested, the requesting authority, the legal basis for the request, and any response provided by us (as applicable).

(ii) become aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination. Any such notification shall include all information NAVEX Global has available.

(b) If we are prohibited from notifying our customer and/or the data subject under the laws of the country of destination, NAVEX Global will use best efforts to obtain a waiver of the prohibition and will communicate as much information to our customer as possible, as soon as possible. We will document these best efforts so that we can demonstrate them on customer request.

(c) NAVEX Global agrees to provide its customer, where permissible under the laws of the country of destination and at regular intervals for the duration of our agreement, with as much relevant information as possible on the requests we have received. Specifically, we have made available the number of requests, the type of data requested, the requesting authorities, whether the requests have been challenged and the outcome of such challenges.

(d) We agree to retain the information pursuant to paragraphs (a) to (c) above for the duration of our agreements and will make it available to competent supervisory authorities on request.

(e) NAVEX Global agrees and understands paragraphs (a) to (c) are without prejudice to our obligations under Clause 14 (e) and Clause 16 to inform our customers promptly in a situation where we are unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) NAVEX Global will review the legality of any request for disclosure, in particular whether it remains within the powers granted to the requesting public authority. We will challenge any such request after we carefully assess and conclude there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. Under the same conditions NAVEX Global will pursue possibilities of appeal. When challenging a request, we agree to seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. NAVEX Global won't disclose the personal data requested until required under the applicable procedural rules. We understand these requirements are without prejudice to our obligations under Clause 14 (e).

(b) We will document these legal assessments and any challenge to the request we make for disclosure. To the fullest extent permissible under the laws of the country of destination, NAVEX Global will make available such documentation to our customer. On request, we'll also make it available to the competent supervisory authorities.

(c) Regardless, NAVEX Global will provide the minimum amount of information permissible when responding to a request for disclosure, based on our reasonable interpretation of the request.

SECTION IV – FINAL PROVISONS

Clause 16 Non-compliance with the Clauses and termination

(a) NAVEX Global will promptly inform its customer if we are unable to comply with these Clauses, for whatever reason.

(b) If we are in breach of these Clauses or are unable to comply, we understand our customer will suspend the transfer of personal data to NAVEX Global until compliance is again ensured or our agreement is terminated. We agree and understand the foregoing is without prejudice to Clause 14 (f).

(c) NAVEX Global agrees and understand our customer will be entitled to terminate our applicable agreements, insofar as it concerns the processing of personal data under these Clauses, where: (i) our customer has suspended the transfer under paragraph (b) above and compliance is not restored within a reasonable time and in any event within one month of suspension; (ii) we are in substantial or persistent breach of these Clauses; or (iii) NAVEX Global fails to comply with a binding decision of a competent court of supervisory authority regarding our obligations under these Clauses. In these cases, we understand our customer will inform the competent supervisory authority of such non-compliance. If there are more than two parties under our agreement, our customer may exercise this termination right only with respect to the relevant party unless the parties have agreed otherwise.

(d) At the choice of our customer, personal data transferred prior to the termination of our agreement under paragraph (c) above will be immediately returned or deleted in its entirety. The same applies to any copies of the data. NAVEX Global will certify the deletion of the data to our customer. Until the data is deleted or returned, we will continue to ensure compliance with these Clauses. If NAVEX Global is subject to applicable local laws that would prohibit the return or deletion of the transferred personal data, we warrant we will continue to ensure compliance with these Clauses and only process the data to the extent and for as long as required under that local law.

(e) NAVEX Global agrees and understands either party may revoke its agreement to be bound by these Clauses where the European Commission adopts an adequacy decision under the GDPR that cover the personal data under these Clauses, or if the GDPR becomes part of the legal framework of the country to which the personal data is transferred. We understand this is without prejudice to our other obligations that apply under the GDPR.

Clause 17 Governing law

MODULE TWO: Transfer controller to processor

This Clause allows for two options, either of which are acceptable to NAVEX Global. We have elected Option 1 for our standard templates, which allows ourselves and our customers to choose the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. Option 2 allows ourselves and our customers to have the governing law be the EU Member State in which our customer is established. However, if such law does not allow for third-party beneficiary rights, these Clauses will be governed by an EU Member State that does.

Clause 18 Choice of forum and jurisdiction

MODULE TWO: Transfer controller to processor

(a) NAVEX Global agrees and understands any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
(b) We agree to specify which EU Member State when completing these Clauses with our customers.
(c) NAVEX Global understand a data subject may bring legal proceedings against our customer and/or us before courts of the Member State in which they reside.
(d) We agree to submit ourselves to the jurisdiction of such courts.

APPENDIX

NAVEX Global has completed the Appendix on behalf of its customers. We have clearly distinguished the information applicable to the transfers. Who the exporters and importers are easily determined. We believe transparency is fully achieved through the completion of one Appendix across our customer base.

ANNEX I

A. LIST OF PARTIES

MODULE TWO: Transfer controller to processor

As previously noted, our customers are the data exporters and NAVEX Global is the data importer. We have completed the data importer information on behalf of our customers and ask our customers to complete the data exporter information.

B. DESCRIPTION OF TRANSFER

MODULE TWO: Transfer controller to processor

We have completed the details of the transfers in this section of the Annex on behalf of our customers as required by these Clauses.

C. COMPETENT SUPERVISORY AUTHORITY

MODULE TWO: Transfer controller to processor

NAVEX Global and our customer will identify the competent supervisory authority/ies in this section, in accordance with Clause 13.

ANNEX II – TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

MODULE TWO: Transfer controller to processor

NAVEX Global has completed the technical and organisational measures on behalf of its customers. They have been described in specific terms. We have indicated which measures apply to the transfers, as applicable.

NAVEX Global has utilized the examples these Clauses provide, in addition to providing all other relevant information it provides its customers in its normal course of business in the interest of full transparency and compliance. We have also described the measures taken by our applicable sub-processors.

ANNEX III – LIST OF SUB-PROCESSORS

MODULE TWO: Transfer controller to processor

This Annex III is not applicable, as NAVEX Global has chosen OPTION 2 under Clause 9 (a). As a result, this Annex III has not been completed.

Customer Assurance Guide: New Processor to Processor Standard Contractual Clauses

We are applying the New Processor to Processor SCCs (Module Three) for our intra affiliate transfers between the NAVEX Global entities (specifically between our European entities and our US entity) and between NAVEX Global and our sub-processors.

To assist our customers in their evaluation of whether the new standard contractual clauses adopted pursuant to the European Commission's Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council C/2021/3972 ("the Clauses") provide sufficient protection of personal data transferred to NAVEX Global's US affiliate and its external vendors as sub-processors, we have prepared the below analysis of their compliance with the Clauses. We encourage you to read the Clauses alongside our assurance guide.

SECTION I

Clause 1 Purpose and scope

(e) The parties fully endorse the purpose of these Clauses to ensure compliance with the GDPR for the transfer of personal data to third countries.

(f) NAVEX Global's customers are the data controllers, NAVEX Global is the data exporter, and NAVEX Global's US affiliate and NAVEX Global's sub-processors are the data importers.

(g) Annex I.B is completed in detail for each arrangement.

(h) All parties understand the Appendix to the Clauses containing the Annexes form an integral part of the Clauses.

Clause 2 Effect and invariability of the Clauses

(c) Our data importers understand these Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies under Article 46(1) and Article 26 (2)(c) of the GDPR. For data transfers, they understand these Clauses set out appropriate safeguards pursuant to Article 28 (7) of the GDPR provided they are not modified outside of selecting the appropriate Module(s) or to complete and update the content of the Appendix. They will not modify the Clauses in accordance with the foregoing. Any wider contract or additional Clauses between ourselves, our affiliates, and our sub-processors will not contradict these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(d) We understand that these Clauses are without prejudice to the obligations which NAVEX Global, as the data exporter, is subject to under the GDPR.

Clause 3 Third-party beneficiaries

(c) NAVEX Global understands Clause 3 of the Clauses enables data subjects to invoke and enforce these Clauses as third-party beneficiaries against NAVEX Global and/or its US affiliate and/or NAVEX Global's sub-processors, subject to a list of exceptions set forth in Clause 3 (a).

(d) All parties understand the exceptions set forth in Clause 3 (a) is without prejudice to the data subject rights set forth in the GDPR.

Clause 4 Interpretations

(d) All parties understand where these Clauses use terms defined under the GDPR, those terms shall have the same meaning as in the GDPR.

(e) They will read and interpret these Clauses in light of the provisions of the GDPR.

(f) No one will interpret these Clauses in a way that conflicts with the rights and obligations under the GDPR.

Clause 5 Hierarchy

All parties understand in the event of a contradiction between these Clauses and the provisions of related agreements between NAVEX Global and its US affiliate or our sub-processors, these clauses shall prevail.

Clause 6 Description of the transfer(s)

Annex I.B, which provide details of the transfers, the particular categories of personal data transfers, and the purposes for which they are transferred, are completed for each arrangement.

Clause 7 Optional - Docking clause

(d) All parties understand Clause 7 is Optional. An entity that is not Party to these Clauses, upon agreement between the applicable entities, may accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(e) They understand that once the new entity completes the Appendix and signs Annex I.A, the acceding entity becomes a Party to these Clauses and shall have the rights and obligations of a data exporter or data importer in accordance with the applicable designation in Annex I.A.

(f) All agree the new entity shall have no rights or obligations under these Clauses prior to becoming a Party to these Clauses in accordance with the foregoing.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8 Data protection safeguards

Clause 8 requires NAVEX Global, as the data exporter, to warrant it has used reasonable efforts to determine its US affiliate and sub-processors, as the data importers, are able to satisfy the obligations under these Clauses through the implementation of appropriate technical and organisational measures. NAVEX Global is fully committed to this warranty.

MODULE THREE: Transfer processor to processor

8.1 Instructions

(c) NAVEX Global's US affiliate and our sub-processors have been informed that they act as processors under the ultimate instructions of our customers as the data controllers. The instructions have been made available, and we are committed to continuously ensuring such instructions are available, to these data importers prior to processing. Typically, our contracts with our customers encompass the entirety of the instructions from the data controllers.

(d) NAVEX Glboal's US affiliate and our sub-processors are required to only process data on controller documented instructions, as communicated by NAVEX Global, along with additional documented instructions from NAVEX Global directly. We will ensure any instructions from us to not conflict with our customers' instructions as the data controllers. All entities understand our customers or NAVEX Global may give the data importers further documented instructions throughout the duration of the agreements. Typically, the contracts with the applicable entities encompass the entirety of the instructions from our customers and NAVEX Global.

(e) NAVEX Global's US affiliate and our sub-processors are required to immediately inform NAVEX Global if it is

unable to follow these instructions. NAVEX Global will immediately notify its customers if these data importers are unable to follow the instructions of our customers.

(f) NAVEX Global has imposed the same data protection obligations on its US affiliate and its sub-processors as is set forth in the contract (or as set out under applicable law) between our customers and NAVEX Global.

8.2 Purpose Limitation

NAVEX Global's US affiliate and its sub-processors agree to process the personal data only for the specific purposes of the transfer, unless on further instructions from our customers, as gets communicated to our data importers by us. Annex I.B is completed for all arrangements.

8.3 Transparency

This Clause requires NAVEX Global to provide a copy of these Clauses, including the Appendix completed by ourselves and our US affiliate and our sub-processors, available to a data subject on request and free of charge. NAVEX Global and its data importers agree to comply with the foregoing requirement. In accordance with this Clause, we agree to redact any text of the Appendix that includes business secrets or other confidential information prior to sharing a copy. However, we have elected to complete the requisite details of the Appendix without including what we would consider to be business secrets or other confidential information, to seamlessly be able to provide copies of these Clauses to data subjects. In any event, if any content were to be redacted, a meaningful summary will be provided for any chosen redacted sections, where the data subject would otherwise not be able to understand the content or exercise their rights. We will also provide any reasonings for elected redactions.

8.4 Accuracy

This Clause requires NAVEX Global's US affiliate and our sub-processors, as data importers, to inform NAVEX Global without undue delay if they become aware that the personal data it has received is inaccurate or has become outdated. Our data importers are committed to providing us this information to the extent they are aware, however, please note that given the nature of the services they provide, they won't be in a position to determine whether or not the personal data submitted to our services is inaccurate out of date. Further, our customers typically do not want NAVEX Global making such determinations. Regardless, all parties commit to compliance with this Clause. NAVEX Global's data importers also will generally cooperate with us to erase or rectify personal data where needed or required.

8.5 Duration of processing and erasure or return of data

The duration of the processing for each arrangement is set forth in Annex I.B. Please know that with respect to our customers, the duration will be for as long as we are providing our customers the applicable services in accordance with our agreements. Our data importers, at our choice, are required to delete the data processed on behalf of our customers where applicable and will certify to us that they have done so or will return to us the data as applicable and then delete existing copies. However, the foregoing processing activities are temporary, and our US affiliate and sub-processors are not engaging in persistent processing activities. As applicable, until the data is deleted or returned (and copies deleted in this instance), our data importers will continue to ensure their processing is in compliance with these Clauses. In case there is a local law applicable to our US affiliate or sub-processors that would prohibit their ability to return or delete the personal data, they warrant they will continue to ensure compliance with these Clauses and would only process it to the extent and for as long as is required under that local law. At this time, no local laws applicable to our data importers prohibit their ability to return or delete personal data in accordance with these Clauses. Our data importers understand the foregoing

is without prejudice to the requirements under Clause 14, especially the requirement under Clause 14 (e) requiring them to notify us throughout the duration of our agreement if they have reason to believe that they are or have become subject to laws or practices not line with the requirements under Clause 14 (a).

8.6 Security of processing

(e) NAVEX Global's US affiliate and our sub-processors have implemented and are committed to the continuous implementation of appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data ("personal data breach"). NAVEX Global shall also implement the foregoing measures during transmission of the data to our data importers. When they assess what the appropriate level of security is, they take into account the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. They take particular consideration to encryption or pseudonymisation, including during transmission, where the purpose of the processing can be fulfilled in this manner. In the event pseudonymisation is used, they commit to, where possible, keeping the additional information for attributing the personal data to a specific data subject under the exclusive control of us or our customers. At the very least, NAVEX Global's US affiliate and our sub-processors will implement the technical and organisational measures specified in the completed Annex II for each arrangement. Our data importers carry out regular checks on their security operations as part of their information security program to ensure these measures continue to provide an appropriate level of security.

(f) NAVEX Global's US affiliate and our sub-processors follow the principle of least privilege with respect to access to personal data by its personnel. They ensure access is granted only to the extent strictly necessary for the implementation, management and monitoring of the contract. All personnel with access to customer data are under appropriate confidentiality agreements or are under appropriate statutory obligation of confidentiality.

(g) Our data importers are required to have robust incident response processes and policies in place. Specifically, in the event of a personal data breach they will take appropriate measures to address the breach, including taking measures to mitigate any adverse effects. Their process and commitment include notifying us (and where appropriate and feasible, our customers) without undue delay after they become aware of a breach. They commit to include a point of contact for where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects, in such notifications. If they are unable to provide all the foregoing information at the same time, the initial notification shall contain the information then available and they will send further information as it becomes available without undue delay.

(h) NAVEX Global's US affiliate and our sub-processors commit to cooperating and assisting us to enable us to comply with our obligations under the GDPR, especially to assist us in notifying our customers as the controllers and the affected data subjects, taking into account the nature of the processing and the information available to them.

8.7 Sensitive data

It is possible for sensitive data to be submitted to certain services NAVEX Global's US affiliate and our sub-

processors provide. The most common circumstance would be through our EthicsPoint services, where a whistleblower reporter may submit personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("sensitive data"). We have sub-processors who intake this information by way of example. Annex I.B is completed for each arrangement, which details the specific restrictions and/or additional safeguards as required by this Clause. The extent of the processing of such sensitive data post submission by the individual is determined and controlled by our customer in their sole discretion.

8.8 Onward transfers

NAVEX Global's US affiliate and our sub-processors only disclose customer personal data under the agreement to third parties on documented instructions from the customer, as communicated to them through us. Typically, the contract sets forth such documented instructions as the contract details the nature of the service for the transfer. They also only disclose the data to third parties outside the European Union if the third party is or agrees to be bound by these Clauses under the appropriate Module, where applicable. All applicable activities involving onward transfers by our sub-processors ensure appropriate safeguards pursuant to Article 46 or Article 47 of the GDPR. They have entered into, or are in the process of entering into, appropriate data processing addendums with their sub-processors. Where applicable, these data processing addendums include, or will include, the Clauses under Module Three (Processor to Processor). Any standard contractual clauses still in process by our data importers are within the applicable grace periods for implementation and execution. Other compliant ways to engage in such onward transfers include: (i) having the third party agree to these Clauses by docking under Clause 7; (ii) transferring to a country under an adequacy decision; (iii) where the transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or (iv) where the transfer is necessary in order to protect the vital interests of the data subject or of another natural person. Our data importers understand that any onward transfer is subject to compliance with all other safeguards under the Clauses, in particular purpose limitation. They only process customer data for the purpose of providing services under the agreements and in accordance with the documented instructions.

8.9 Documentation and compliance

- **(f)** NAVEX Global's US affiliate and our sub-processors are fully committed to promptly and adequately dealing with enquiries from us or our customer that relate to the processing under these Clauses.
- **(g)** Our data importers will keep appropriate documentation on the processing activities carried out on behalf of our customers. Annex I. A is completed for each arrangement, which sets forth the records of processing activities.
- **(h)** They will make all information necessary to demonstrate compliance available to us, and we will provide it to our customers. If there is additional documentation you may require, please let us know and we will promptly assist.
- **(i)** NAVEX Global's US affiliate and our sub-processors are required to allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same applies for when our customers instruct us to conduct such audit. They contractually require reasonable parameters be put in place to allow them to support the audit. For example, they require any onsite audit to be conducted during regular business hours and with reasonable notice. Additionally, they contractually ask our customers in good faith to take into account their relevant certifications in deciding on a review or audit, which may be considered in accordance

with this Clause.

(j) If such an audit is performed on the instructions of our customer, we will make the results available to said customer.

(k) NAVEX Global may choose to conduct the audit on our own or utilize an independent auditor. We contractually require any independent auditors to execute a confidentiality and non-disclosure agreement as presented by and for the benefit of all parties involved. In accordance with these Clauses, our data importers permit inspections at our premises or applicable physical facilities with reasonable notice.

(l) On request from a competent supervisory authority, the information referred to in this Clause, including any audit results, will be made available.

Clause 9 Use of sub-processors

MODULE THREE: Transfer processor to processor

(a) Clause 9 sets forth two options for how our customers can provide authorisation of sub-processors for our US affiliate or additional sub-processors engaged by our sub-processors ("sub-sub-processors"). NAVEX Global has selected OPTION 2: GENERAL WRITTEN AUTHORISATION. In accordance with this Clause, we have our customer's general authorisation for the engagement of sub-sub-processors from an agreed list. The agreed list is our current list of sub-sub-processors, set forth at the following link, as applicable: https://www.navexglobal.com/en-us/service-hosting-providers. Our data importers are required to notify us in writing of the addition of any new sub-sub-processors, or the replacement of sub-sub-processors, and we are required to notify our customers, thereby giving our customers reasonable time to exercise their right to object. NAVEX Global and its data importers will provide its customers the information necessary to enable them to exercise their right to object. In such event, the parties will work in good faith to discuss a resolution. Our data importers are required to inform us of the engagement of such sub-sub-processors.

(b) They have, or will, enter into robust data processing agreements with their sub-sub-processors that provide for, or will provide for, in substance, the same data protection obligations as those binding them under these Clauses, including in terms of third-party beneficiary rights for data subjects. Our data importers understand that by complying with this Clause, they fulfil their obligations under Clause 8.8. They will ensure their sub-sub-processors comply with the obligations to which our data importers are subject pursuant to these Clauses.

(c) Upon our or our customer's request, they will provide a copy of the applicable sub-sub-processor agreement and any subsequent amendments. In order to protect the parties involved, text may be redacted from these agreements as permitted by this Clause to protect business secrets or other confidential information, including personal data.

(d) NAVEX Global's US affiliate and our sub-processors understand and agree they are fully responsible for the performance of the sub-sub-processor's obligations under the agreements. They will notify us of any failure by the sub-sub-processors to fulfil their obligations under the agreement. We interpret the foregoing as pertaining to any failure by the sub-sub-processor that materially impacts the services NAVEX Global provides to its customers, or to any failure pertaining to the sub-sub-processor's compliance with the Clauses or other applicable data protection obligations.

(e) Their agreements with their sub-sub-processors include, or will include, a third-party beneficiary clause whereby – in the event our data importer has factually disappeared, ceased to exist in law or has become insolvent – we have the right to terminate the sub-sub-processor agreement and to instruct the sub-sub-

processor to erase or return the personal data, as applicable.

Clause 10 Data subject rights

MODULE THREE: Transfer processor to processor

(d) NAVEX Global's US affiliate and our sub-processor's process is to notify us in the event it received a data subject request. Please note this is a rare occurrence and we always forward those directly to the applicable customer promptly upon receipt. They will not respond to the request themselves unless our customers authorise them to do so. Notwithstanding the foregoing, we do confirm receipt with the data subject and let them know we have sent the request to the applicable customer. We believe this is appropriate in order to support the data subject under applicable data protection obligations. NAVEX Global does not foresee any reason for our customers to authorise us to respond otherwise to a data subject request but will of course assist and cooperate as needed or required.

(e) Our data importers will assist, in direct cooperation with us, our customers in fulfilling their obligations to respond to data subject rights requests under the GDPR. Annex II is completed for each arrangement, which detail the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and extent of the assistance required.

(f) In fulfilling the above obligations, our data importers will comply with our customer's instructions, as directly communicated by us.

Clause 11 Redress

(g) NAVEX Global's US affiliate and our sub-processors inform data subjects in a transparent and easily accessible format, through the privacy notices available on their websites, of a contact point authorised to handle complaints. They will promptly deal with any complaints they receive from data subjects.

MODULE THREE: Transfer processor to processor

(h) NAVEX Global's US affiliate and our sub-processors agree to use best efforts to resolve any disputes between a data subject and one of the parties to these Clauses as regards compliance with these Clauses in an amicably and timely fashion. All agree to keep everyone informed about such disputes and will cooperate in resolving them where appropriate.

(i) Where a data subject invokes a third-party beneficiary right under Clause 3 of these Clauses, our data importers will accept the data subject's decision to: (i) lodge a complaint with the supervisory authority in the Member State of where they reside or where they work, or the competent supervisory authority pursuant to Clause 13; and/or (ii) refer the dispute to competent courts pursuant to Clause 18.

(j) They understand the data subject may be represented by a not-for-profit body, organisation or association under the conditions within Article 80(1) of the GDPR.

(k) Our data importers will abide by a decision that is binding under the applicable EU or Member State law.

(l) They understand and agree that the choice made by the data subject will not prejudice the data subject's substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12 Liability

MODULE THREE: Transfer processor to processor

(h) NAVEX Global's US affiliate and our sub-processors agree and understand it shall be liable to the other party/ies for any damages it may cause such party by any breach of these Clauses.

(i) They also understand and agree they shall be liable to a data subject, and that data subjects will be entitled to receive compensation, for any material or non-material damages they or their sub-sub-processors cause such data subject by breaching the third-party beneficiary rights under these Clauses.

(j) Notwithstanding paragraph (b) above, we shall be liable to such data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages we or our data importers (or their sub-sub-processors) causes to such data subject by breaching the third-party beneficiary rights under these Clauses. The foregoing is without prejudice to the liability of NAVEX Global and, where we are acting on behalf of a controller (if applicable), to the liability of the controller under the GDPR or Regulation (EU) 2018/1725.

(k) Our data importers agree and understand that if NAVEX Global is held liable under paragraph (c) above for damages caused by them (or their sub-sub-processors), NAVEX Global shall be entitled to claim back from its data importer that part of the compensation corresponding to its responsibility for the damage.

(l) All agree and understand if more than one party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible parties shall be jointly and severally liable and the data subject is entitled to bring action in court against any of the parties.

(m) All agree and understand if one party is held liable under paragraph (e) above, it shall be entitled to claim back from the other party/ies that part of the compensation corresponding to their responsibility of the damage.

(n) Our data importers may not invoke the conduct of a sub-sub-processor to avoid their own liability. Our data importers have always contractually committed to being fully liable for their sub-sub-processor's activities.

Clause 13 Supervision

MODULE THREE: Transfer processor to processor

(c) This Clause sets forth how to select the responsible supervisory authority, depending on the scenario. Where NAVEX Global, as the data exporter, is established in an EU Member State, the supervisory authority indicated in Annex I.C. shall be responsible for ensuring compliance by us with GDPR as regards the transfer. NAVEX Global is established in, and has selected, Ireland.

(d) NAVEX Global's US affiliate and our sub-processors agree to submit themselves to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. They agree to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. They will provide the supervisory authority with written confirmation that any necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC

AUTHORITIES

Clause 14 Local laws and practices affecting compliance with the Clauses

****NAVEX Global's US affiliate and our sub-processors have performed appropriate transfer risk assessments to support compliance with this Clause 14. Please see our full assurance guide for our transfer risk assessment documentation. ****

MODULE THREE: Transfer processor to processor

(g) NAVEX Global's US affiliate and our sub-processors warrant they have no reason to believe the laws and practices in the third countries of destination applicable to the processing of personal data by them, including any requirements to disclose personal data or measures authorising access by public authorities, prevent our data importers from fulfilling their obligations under these Clauses. The foregoing warranty is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed under Article 23(1) of the GDPR, are not in contradiction with these Clauses.

(h) In order to provide the foregoing warranty in paragraph (a) above, they have taken due account of the following elements:

(i) the specific circumstances of the applicable transfer(s), the length of the processing chain, the number of actors involved and transmission channels used, intended onward transfers, recipient type, purpose of processing, categories and format of the transferred personal data, the economic sector for which the transfer occurs, storage location of the data, and duration of a given processing activity (as applicable).

(ii) the laws and practices of the third country of destination, including those requiring the disclosure of data to public authorities or authorising access by such authorities, relevant considering the specific circumstances of the transfer, and the applicable limitations and safeguards. Please note they have also taken into account Footnote 12 for this portion of our assessment as authorised by these Clauses. The additional elements include our relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. NAVEX Global's US affiliate and our sub-processors maintain internal records and documentation which shall continue to be drawn up on a continuous basis in accordance with due diligence at senior management level. They will share this information with third parties to the fullest extent permitted by applicable law. Our data importers do take this practical experience into account but do not rely on it in totality to conclude they will not be prevented from complying with these Clauses. They support assessments via all of the foregoing elements outlined above, along with other relevant and objective factors. Our data importers understand it is for the parties to consider carefully whether all the elements taken together carry sufficient weight in terms of their reliability and representatives to support this conclusion. They commit to corroborating our practical experience to ensure it is not contradicted by publicly available or otherwise accessible or reliable information on the existence or absence of requests within the same sector and/or the application of law in practice, such as case and reports by independent oversight bodies.

(iii) the relevant contractual, technical and organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of personal data in the country of destination. Please see NAVEX Global's full assurance guide for all the details around the approach to supplementary measures.

(i) NAVEX Global's US affiliate and our sub-processors warrant they have made best efforts to provide us with all relevant information in carrying out its transfer risk assessments and they agree they will continue to cooperate with us and our customers in ensuring compliance with these Clauses.

(j) Our data importers have documented their assessments on behalf of us and our customers and agree to make it available to competent supervisory authorities on request. Even though they have performed these assessments, we understand our customers may want to undertake their own assessments. Our data importers and NAVEX Global agree to support our customers with any assessments they wish to complete under these Clauses.

(k) NAVEX Global's US affiliate and our sub-processors agree and understand they must notify us promptly if they have reason to believe that it is or has become subject to laws or practices not in line with the requirements of paragraph (a) above, including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a) above. NAVEX Global agrees to forward such notification to its customers.

(l) In the event our data importers do notify us pursuant to paragraph (e) above, or if we have reason to believe they no longer can fulfil their obligations under these Clauses, they agree and understand NAVEX Global shall promptly identify appropriate measures to be adopted by the parties (as applicable) to address the situation. NAVEX Global will consult its customers where appropriate. They understand we shall suspend data transfers if we or our customers consider that no appropriate safeguards for such transfer can be ensured, or if they are instructed by the competent supervisory authority to do so. Our data importers understand in this case, we shall be entitled to terminate the applicable agreement, insofar as it concerns the processing of personal data under these Clauses. If the applicable agreement involves more than two parties, we may exercise this right to termination only with respect to the relevant party, unless agreed upon otherwise. If an agreement is terminated under this Clause, Clause 16 (d) and (e) shall apply.

Clause 15 Obligations of the data importer in case of access by public authorities

MODULE THREE: Transfer processor to processor

15.1 Notification

(f) NAVEX Global's US affiliate and our sub-processors agree it will notify us and, where possible, the data subject promptly (if necessary, with our help) if they:
(i) receive a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses. Any such notification will include information about the personal data requested, the requesting authority, the legal basis for the request, and any response provided by them (as applicable).

(ii) become aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination. Any such notification shall include all information our data importers have available. NAVEX Global will then forward this notification to its customers.

(g) If they are prohibited from notifying our customer and/or the data subject under the laws of the country of destination, they will use best efforts to obtain a waiver of the prohibition and will communicate as much information to us as possible, as soon as possible. They will document these best efforts so that they can demonstrate them on our request.
(h) NAVEX Global's US affiliate and our sub-processors agree to provide us, where permissible under the laws of the country of destination and at regular intervals for the duration of the agreements, with as much relevant information as possible on the requests they have received. Specifically, they are required to make available the number of requests, the type of data requested, the requesting authorities, whether the requests have been challenged and the outcome of such challenges. NAVEX Global will forward such information to its customers upon request.
(i) They agree to retain the information pursuant to paragraphs (a) to (c) above for the duration of the agreements and will make it available to competent supervisory authorities on request.
(j) Our data importers agree and understand paragraphs (a) to (c) are without prejudice to our obligations under Clause 14 (e) and Clause 16 to inform us promptly in a situation where we are unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(d) NAVEX Global's US affiliate and our sub-processors will review the legality of any request for disclosure, in particular whether it remains within the powers granted to the requesting public authority. They will challenge any such request after we carefully assess and conclude there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. Under the same conditions our data importers will pursue possibilities of appeal. When challenging a request, they agree to seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. They won't disclose the personal data requested until required under the applicable procedural rules. They understand these requirements are without prejudice to our obligations under Clause 14 (e).
(e) Our data importers will document these legal assessments and any challenge to the request made for disclosure. To the fullest extent permissible under the laws of the country of destination, they will make available such documentation to us. On request, they will also make it available to the competent supervisory authorities. NAVEX Global will forward such information to its customers on request as well.
(f) Regardless, they will provide the minimum amount of information permissible when responding to a request for disclosure, based on our reasonable interpretation of the request.

SECTION IV – FINAL PROVISONS

Clause 16 Non-compliance with the Clauses and termination

(f) NAVEX Global's US affiliate and our sub-processors will promptly inform us if they are unable to comply with these Clauses, for whatever reason.
(g) If they are in breach of these Clauses or are unable to comply, they understand NAVEX Global will suspend the transfer of personal data until compliance is again ensured or the agreement is terminated. They agree and understand the foregoing is without prejudice to Clause 14 (f).
(h) Our data importers agree and understand we will be entitled to terminate the applicable agreements, insofar as it concerns the processing of personal data under these Clauses, where: (i) we have suspended the transfer under paragraph (b) above and compliance is not restored within a reasonable time and in any event within one month of suspension; (ii) they are in substantial or persistent breach of these Clauses; or (iii) they fail to comply with a binding decision of a competent court of supervisory authority regarding our obligations under

these Clauses. In these cases, they agree to inform the competent supervisory authority and our customers of such non-compliance. If there are more than two parties to the agreement, we may exercise this termination right only with respect to the relevant party unless the parties have agreed otherwise.

(i) At NAVEX Global's choice, personal data transferred prior to the termination of the agreement under paragraph (c) above will be immediately returned or deleted in its entirety. The same applies to any copies of the data. Our data importers will certify the deletion of the data to us. Until the data is deleted or returned, they will continue to ensure compliance with these Clauses. If they are subject to applicable local laws that would prohibit the return or deletion of the transferred personal data, they warrant they will continue to ensure compliance with these Clauses and only process the data to the extent and for as long as required under that local law.

(j) Our data importers agree and understand either party may revoke its agreement to be bound by these Clauses where the European Commission adopts an adequacy decision under the GDPR that cover the personal data under these Clauses, or if the GDPR becomes part of the legal framework of the country to which the personal data is transferred. They understand this is without prejudice to our other obligations that apply under the GDPR.

Clause 17 Governing law

MODULE THREE: Transfer processor to processor

This Clause allows for two options. NAVEX Global's US affiliate and our sub-processors have elected Option 1, which allows the parties to choose the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The parties have agreed to specify Ireland.

Clause 18 Choice of forum and jurisdiction

MODULE THREE: Transfer processor to processor

(e) NAVEX Global's US affiliate and our sub-processors agree and understand any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(f) The parties have agreed to specify Ireland.

(g) Our data importers understand a data subject may bring legal proceedings against them and/or us before courts of the Member State in which they reside.

(h) We all agree to submit ourselves to the jurisdiction of such courts.

APPENDIX

NAVEX Global's US affiliate and our sub-processors have completed the Appendix for each of the applicable agreements. They have clearly distinguished the information applicable to the transfers. Who the exporters and importers are easily determined.

Supplementary Measures

What are "Supplementary Measures"?

The EDPB Recommendations provide non-exhaustive lists of examples of potential technical, contractual, and organizational measures organizations can consider implementing alongside the SCCs, where applicable.

Examples include, but are not limited to:

- Additional Schrems II contractual assurance addendums to the data processing agreements
- The implementation of transparency, audit and monitoring obligations regarding the level of government access to data
- Written processes and procedures for review of and limit the scope of EU personal data disclosed in response to requests from public authorities
- Maintenance of internal records of requests made by public authorities concerning EU personal data
- Assurances that steps are taken to limit the volume of disclosed data, where possible
- Data minimization measures such as redacting unnecessary identifiable personal data or personal data that may be of increased interest to intelligence agencies before complying with a request to disclosure EU personal data
- Encryption in transit and at rest

- Enhanced access controls
- Enhanced data minimization (e.g., store the least amount of data necessary)
- Limit timespan for using personal data "in the clear" (i.e., in identifiable form)
- Store personal data in the EU and enable only remote access or view-only access.
- Expanded recourse mechanisms for EU individuals (such as Privacy Shield independent recourse mechanism or alternative dispute resolution mechanism to provide redress to EU individuals)

How is NAVEX Global addressing this with its customers?

NAVEX Global is actively involved in monitoring legal developments related to its business. Please see NAVEX Global's practices to suggested supplementary measures and additional assurances in the table below. Please also see the supplementary measures within our Transfer Risk Assessment section below.

Supplementary Measure or Additional Assurance	NAVEX Global Approach
Additional Contractual Requirements	The SCCs themselves contain a number of contractual commitments by NAVEX Global and its customer, aimed at serving as safeguards for EU personal data. NAVEX Global provides a data processing agreement to support GDPR compliance, which includes the SCCs. As the data processor/importer, we process personal data strictly in accordance with your instructions and to provide the services. Our customers are the owners of the personal data within our service applications. NAVEX Global offers a Data Security Addendum, providing for contractual commitments to its information security program. Supplementary contractual assurances are offered via our standard data processing addendum or an amendment to the data processing addendum. Please reach out to privacy@navexglobal.com or your account executive in order to get this in place.
Encryption in transit and at rest	NAVEX Global employs encryption at rest using either full-disk encryption or within the database using TDE. Data at rest will be encrypted using AES 256 or better, data in flight will be accomplished using TLS 1.2 or higher on public untrusted networks.
Additional Organizational Requirements	NAVEX Global maintains written processes and procedures which provide for review of and limit the scope of EU personal data disclosed by NAVEX Global in response to requests from public authorities. Please see our Public Authority Disclosure Request Policy. NAVEX Global agrees to audit and monitor its obligations, and to support its customers auditing and monitoring obligations, regarding the level of government access to data. NAVEX Global maintains internal record of requests

	made by public authorities concerning EU personal data. NAVEX Global takes steps to limit the volume of disclosed data, where possible.
Transfer Risk Assessments	Please see below for details on the Transfer Risk Assessments NAVEX Global has conducted on behalf of its customers.
Standard Contractual Clauses Assurance Guides	NAVEX Global has developed the above Standard Contractual Clauses Assurance Guides, which detail our commitment, and our sub-processor's commitment, to compliance with the SCCs.
Privacy Shield certified	NAVEX Global remains a participant and has certified its compliance with the EU-U.S. Privacy Shield Framework and the Swiss- U.S. Privacy Shield Framework. NAVEX Global, Inc. is committed to subjecting all personal information received from the European Economic Area, United Kingdom, and Switzerland, respectively, in reliance on each Privacy Shield Framework, to the Frameworks' applicable Principles. To learn more about the Privacy Shield program, and to view our certification, please visit https://www.privacyshield.gov.
Additional technical measures and agreements	NAVEX Global engages a recognized, independent third party to conduct a Statement on Standards for Attestation Engagements No. 16, Service Organization Control 2, Type 2 ("SSAE 18 SOC 2 Type 2") audit (or its equivalent or successor) of its information security program and its administrative, technical, and physical safeguards for all facilities used to deliver the Services, which specifically includes privacy controls. NAVEX Global maintains an annual Standardized Information Gathering Questionnaire ("SIG"), which details our robust security program with supporting documentation. NAVEX Global offers a Data Security Addendum, providing for contractual commitments to its information security program.
EU storage	NAVEX Global offers the option to select EU servers for our service applications.
Recourse mechanisms for EU individuals	NAVEX Global provides an independent recourse mechanism to EU individuals, currently TrustArc.

NAVEX Global Data Transfer Risk Assessments

NAVEX Global has conducted Transfer Risk Assessments (TRAs) for each product by hosting and storage location (EU or US), as elected by customer. Sub-processing activity TRAs are also incorporated below where applicable. Please select your applicable product and hosting location for your applicable TRA information.

Hotline and Incident Management: EU Hosted

NAVEX GLOBAL

EU HOSTED HOTLINE AND INCIDENT MANAGEMENT - EU/UK DATA TRANSFER RISK ASSESSMENTS

I. INTRODUCTION

NAVEX Global must conduct Transfer Risk Assessments ("TRA" or "TRAs") for transfers of personal data from the European Economic Area ("EEA")[1] or the United Kingdom ("UK") (collectively "EU personal data") to third countries that are not deemed to provide an adequate level of data protection.

II. SCOPE

These TRAs apply to NAVEX Global's EU Hosted Hotline and Incident Management customers*.

This TRA process applies to personal data transferred to NAVEX Global pursuant to the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council. This TRA is specifically designed to address Clause 14 of the foregoing set of Standard Contractual Clauses. Personal data from the UK is also in scope and shall be assessed pursuant to the European Commission's decision (C(2010)593) of 5 February 2010 on Standard Contractual Clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection. We collectively refer to the sets of Standard Contractual Clauses as the "SCCs." NAVEX Global agrees and acknowledges the UK will be issuing its own set of standard contractual clauses and related Schrems II guidance. We will update this TRA on an ongoing basis as needed.

This TRA process takes into account the European Data Protection Board's Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data adopted on 18 June 2021 (the "EDPB Guidance").

NAVEX Global has separate TRAs for its non-affiliate sub-processing activities, where NAVEX Global utilizes such sub-processors for the processing of personal data who receive customer EU personal data in third countries that have not been deemed adequate by the European Commission. These are available as part of our compliance documentation and on request.

This TRA is not intended for transfers (i) within the EEA, (ii) between the EEA and the UK, or (iii) from the EEA or UK to a country recognized by the European Commission or UK law as adequate at this time (i.e., Andorra, Argentina, Canada (commercial organizations subject to PIPEDA), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, UK, and Uruguay).

The TRA is completed by the NAVEX Global Privacy Team, which consists of the Data Privacy Officer & Senior Counsel, Deputy Data Privacy Officer & Senior Counsel, and Privacy Counsel.

[1] The European Economic Area consists of the Member States of the EU (Austria, Belgium, Bulgaria, Croatia, Cyprus, Czechia, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain and Sweden), plus Iceland, Liechtenstein and Norway.

**Hotline and Incident Management (HLIM) consists of either AlertLine/Integrlink or EthicsPoint. NAVEX Global is decommissioning AlertLine/Integrilink as a legacy product. These TRAs apply generally to both services, however, for the most enhanced functionality, we recommend AlertLine/Integrlink customers migrate to EthicsPoint. All AlertLine/Integrilink customers will be asked to migrate in the near future.*

III. ASSESSING THE ADEQUACY OF EU/UK DATA TRANSFERS – TO NAVEX GLOBAL IN THE U.S.

In assessing the adequacy of transfers of personal data from the EU/UK to NAVEX Global in the U.S. we have taken the following steps:

1. **STEP 1:** Identified the relevant data transfers and the legal mechanism that NAVEX Global is relying on for such transfers (e.g., SCCs).

2. **STEP 2:** Conducted due diligence and collected information about the scope of the transfers, the exposure of NAVEX Global to local law that may require disclosure of EU personal data about individuals, and any other relevant information.

3. **STEP 3:** Completed the "Transfer Risk Assessment" in **Section IV** to assess whether the SCCs is effective in light of all circumstances of the transfer.

4. **STEP 4:** Included additional "Supplementary Measures" as set forth in **Section IV (D)**.

5. **STEP 5:** Documented the assessment for accountability purposes. We encourage our customers to do the same.

6. **STEP 6:** NAVEX Global is responsible for the periodic review of the assessment, which should take place at least annually, to ensure that the transfer of the EU personal data continues to be afforded an adequate level of protection.

IV. TRANSFER RISK ASSESSMENT

Name Of Data Importer: NAVEX Global
Scope of TRA: Transfers to NAVEX Global's affiliates in the United States as part of the Hotline and Incident Management Services provided to EU Hosted Customers
Completed By: NAVEX Global's Privacy Team
Date: 25 September 2021

A. Type of Data Importer

Name of data importer: NAVEX Global. The SCCs between customer and NAVEX Global is part of a master services agreement between customer and NAVEX Global UK Limited (registered in the UK) or GCS Compliance Services Europe Unlimited Company trading as NAVEX Global (registered in Ireland), both with their principal places of business at Vantage West – 4th floor, Great West Road, Brentford TW8 9AG, United Kingdom. Some EU Hosted customers elect to contract directly with our U.S. entity, NAVEX Global, Inc., a Delaware corporation with its principal place of business at 5500 Meadows Road, Suite 500, Lake Oswego, OR 97035.

Upon reviewing the broad definitions set forth within U.S. surveillance laws under scrutiny pursuant to the CJEU ruling in the Schrems II case, NAVEX Global identifies itself as follows:

NAVEX Global does not consider itself a "telecommunications carrier" as defined in 47 U.S.C. 152.

NAVEX Global acknowledges that certain of its services could be viewed by U.S. government authorities as an "electronic communication service" as defined in 18 U.S.C. 2510.

NAVEX Global acknowledges that certain of its services could be viewed by U.S. government authorities as a "remote computing service" as defined in 18 U.S.C. 2711.

NAVEX Global acknowledges that certain of its services could be viewed by U.S. government authorities as other communication services where there may be access to wire or electronic communications.

B. Details of Data Transfers

Data transfer mechanism Appropriate Controller to Processor SCCs between customer and NAVEX Global.
Scope of personal data covered by the data transfer mechanism in place The SCCs cover transfers of EU personal data from the EEA/UK to the U.S., including the following categories of data subjects: • Employees of data exporter • Clients, business partners and vendors of data exporter (who are natural persons) • Employees or contact persons of data exporters' third-party suppliers, business partners and vendors • Data exporter's users authorized by data exporter to use the relevant Service(s)

C. Transfer Risk Assessment

The table below aids identification and evaluation of risk factors in relation to the specific data transfer. The assessment of each risk factor is recorded in appropriate detail.

#	Factor	Response
Scope of the transfers		
1.	What is the type of transfer?	Remote access only by direct NAVEX Global personnel located in the U.S. to personal data stored in the EU. Personal data is not stored in the U.S. as part of this transfer.
2.	Is the transfer necessary?	Yes. NAVEX Global has critical resources located in the U.S., requiring access to the EU hosted database for the following purposes: • Support. General support cases that are submitted, depending on the case, may require access to customer data to address the issue at hand. To meet our service level commitments, U.S. support may be involved accordingly. This is mainly due to certain resource limitations based on location, an overflow of support cases, and time zone challenges. • Administrative Service Functions. There is certain work, for example setting up the landing page, that does not necessarily require a deep level access, but for which can result in a transfer of personal data to the U.S. depending on the service need. • Contact Center Oversight. Senior personnel in the U.S. have access for supervision and quality assurance purposes. • Technical Work. Many of our technical resources are in the U.S. which requires access to customer data. Examples include certain data extract services, certain data migration services, integration services, user setups instances, and hosting installations. again, depending on the task, we need the option to leverage those resources which involves a certain level of access. • IT/Hosting. Select members of the hosting and information security group must have access for maintenance and troubleshooting. Without the above, our service level

#	Factor	Response
		commitments would greatly suffer, and the overall maintenance and security of our service would be put at great risk.
3.	Is the transfer proportionate?	Yes. Access is not provided to personnel in the U.S. in a general sense. Access is provided to those personnel in the U.S. on a strict need to know basis to perform their given job function.
4.	Is the transfer occasional/non-routine or frequent/routine?	The transfer is non-routine to NAVEX Global personnel in the U.S. for the purposes detailed in Factor #2 above.
5.	Will the transferred personal data be processed for a relatively long or short period of time?	Personal data transferred to the U.S. in this context is processed for a relatively short period of time to provide the applicable service support.
6.	Is the transferred data encrypted and/ or pseudonymized?	Yes. NAVEX Global employs encryption at rest using either full-disk encryption or within the database using TDE. Data at rest will be encrypted using AES 256 or better, data in flight will be accomplished using TLS 1.2 or higher on public untrusted networks. Upon reviewing pseudonymization in the context of this transfer, it is inapplicable to the services we need to support.
Specific circumstances of the transfer		
7.	What are the purposes for which the data are transferred and processed?	To provide the best support, maintenance, and services as committed to in our agreements with our customers.
8.	What are the types of entities involved in the processing?	NAVEX Global is a data processor and a private company. Our customers are the data controllers and may consist of both private and public companies.
9.	In which sector does the transfer occur?	NAVEX Global provides risk and compliance management SaaS based software. ***This factor is especially important as the purposes of our services is to enable organizations support their risk, ethics, and compliance programs. ***

#	Factor	Response
10.	What are the categories of personal data transferred?	As instructed by NAVEX Global's customer, including but not limited to: • name, job title, job position, location, employer, relationship with the organization, e-mail address, telephone number, log-in credentials, date of birth; • for whistle-blower hotline and case management reports, in addition to the foregoing, the following may also be captured: o facts reported by a reporter about a suspected violation, including how and where the suspected violation occurred and how the reporter learned about the suspected violation; o identity, function and contact details of individuals allegedly involved in the suspected violation; and o identity, function and contact details of individuals who could provide information relating to the suspected violation. Given the nature of incident management services, our customers, reporters, or authorized users of the services may submit sensitive categories of data to their case management systems. We recommend our customers have strict policies around the management of such report data in their use of the services, in accordance with the laws subject to them.
11.	What is the format of the personal data to be transferred?	NAVEX Global employs encryption at rest using either full-disk encryption or within the database using TDE. Data at rest will be encrypted using AES 256 or better, data in flight will be accomplished using TLS 1.2 or higher on public untrusted networks. When access is provided to NAVEX Global personnel in the U.S. for the purposes described in this TRA, customer data must be accessible in the clear to provide the requisite support or service function.
12.	What is the storage location of the data transferred?	The European Union.
13.	What are the sub-processing activities?	Please see details here:

#	Factor	Response
		https://www.navexglobal.com/en-us/service-hosting-providers. These are temporary and limited sub-processing activities. All requirements are flown down to each sub-processor.
Importer's exposure to government surveillance and practical application of Section 702 FISA		
14.	Is the data importer's sector or business directly subject to such laws in its jurisdiction that permit government access to personal data, or require the assistance of data importer to disclose personal data to public authorities, for surveillance and intelligence gathering purposes?	No. In our reasonable opinion upon internal and outside counsel review, we do not find NAVEX Global to be directly subject to such laws. As a practical matter based on the nature of NAVEX Global's services, the types of personal data processed, and the absence of any prior requests received in the past, NAVEX Global believes it is extremely unlikely to receive requests from U.S. government agencies to obtain customer data for national security purposes or to participate in the types of U.S. bulk surveillance programs scrutinized by the CJEU in its recent ruling on data transfer mechanisms.
	a. Specifically, what is data importer's analysis regarding Section 702 FISA under the SCCs and EDPB Guidance?	1) Data exporters may decide to proceed with the transfer without supplementary measures, if they consider there to be no reason to believe that the relevant and problematic legislation (those in the U.S. in this instance) will be applied, in practice, to the transferred data and/or NAVEX Global. a. In our reasonable opinion upon internal and outside counsel review, we do not find U.S. surveillance laws, including Section 702 FISA, to practically apply to these transfers. b. It is important to note that given the broad definitions of these laws, the vast majority of organizations are going to have to acknowledge their potential application. However, this does not mean they directly apply or practically apply in practice. c. We believe NAVEX Global is generally out of scope and that these laws are overall not going to apply to the services we provide, as the intent is for surveillance of certain telecom and internet service providers for targeted information. This typically involves to surveillance of real time emails, texts, and chat conversations. The foregoing is not what NAVEX Global provides and in order to obtain this sought for information, authorities would pursue those providers

#	Factor	Response
		directly as it would be impractical to make a request through NAVEX Global. 2) Data exporters may also take into consideration documented practical experience of data importer with relevant prior instances of requests for access received from public authorities in the U.S. a. ***To this point, NAVEX Global has never received a Section 702 FISA request or an EO 12.333 request or order. Please see our Public Authority Disclosure Request Policy for more details.** * b. The EDPB Guidance implies that the lack of requests received in the past plus no prohibition on providing information about such requests, could be sufficient to conclude Section 702 FISA does not apply in practice. Note there is no prohibition on NAVEX Global to provide information about these requests. 3) If you conclude Section 702 FISA does not apply in practice to the particular transfer, it is possible to proceed with the transfer without any supplementary measures. **a. While NAVEX Global takes the approach that Section 702 FISA does not apply in practice, we still have elected to provide for supplementary measures with regard to these transfers. Please see Section IV (D).**
15.	Within the last three (3) years, has the data importer received requests/demands from public authorities in its jurisdiction to disclose EU personal data pursuant to the SCCs?	No, not to the best of our knowledge.
	a. Approximately how many requests/demands from public authorities has the data importer received in that time period concerning EU personal data pursuant to the SCCs?	None, to the best of our knowledge.
	b. Approximately how many of these requests/demands are pursuant to criminal law procedure in the destination country? *[Regular court proceedings are not the issue under Schrems II, but intelligence programs are scrutinized.]*	While NAVEX Global has not received a Section 702 FISA request, an EO 12.333 request or order, or a public authority request specifically targeting EU personal data under the SCCs, we have received a limited number of formal requests or demands from U.S. government authorities concerning customer data. These requests have been made in the context of criminal and civil actions in the form of a subpoena issued to NAVEX Global as a third party, by a state or federal court. In each instance, we've notified the customer straight away and they have directed us to comply with

#	Factor	Response
		the subpoena. We've only fulfilled such requests with full customer clearance and direction on how to handle.
	c. Approximately how many of these requests/demands are pursuant to national security or intelligence agencies in the destination country?	None, to the best of our knowledge. The data importer can represent that it has not received requests/demands from intelligence agencies. NAVEX Global offers signed contracts, warranting it has not received such requests, via either a data processing addendum or amendment to data processing addendum.
	d. Has the data importer been able to contest/minimize such disclosure of EU personal data, where appropriate?	Not applicable
	e. What types of EU personal data has the data importer been required to disclose to public authorities in its jurisdiction?	Not applicable
16.	How likely is it that the data importer will receive bulk data surveillance requests to disclose EU personal data to public authorities in its jurisdiction in the future (e.g., based on factors such as the type of services provided and sector in which the data importer operates, its size, number of customers and reputation)?	Unlikely. As a practical matter based on the nature of NAVEX Global's services, the types of personal data processed, and the absence of any prior requests received in the past, NAVEX Global believes it is extremely unlikely to receive requests from U.S. government agencies to obtain customer data for national security purposes or to participate in the types of U.S. bulk surveillance programs scrutinized by the CJEU in its recent ruling on data transfer mechanisms. We have no reason to believe we may receive such requests in the future.
17.	Does the data importer maintain annual reports or statistics regarding requests/demands received from law enforcement or intelligence agencies (e.g., number/type of requests/demands, requesting authority, etc.)?	Not applicable. NAVEX Global has not received a Section 702 FISA request, an EO 12.333 request or order, or a public authority request specifically targeting EU personal data under the SCCs. As a result, if we get such requests in the future, we will provide such statistics and update our TRA process and Public Authority Disclosure Policy accordingly.
18.	Does the data importer maintain a written procedure(s) for: 1. Responding to or challenging requests/ demands of law enforcement or intelligence agencies that apply to EU personal data? 2. Informing customers of requests/demands from law enforcement or intelligence agencies where permitted by applicable law?	Yes, please see our Public Authority Disclosure Request Policy.
19.	Are the data importer's commitments enabling data subjects to exercise their rights as provided in the SCCs thwarted by the laws	NAVEX Global has never encountered a situation where it felt it could not enable data

#	Factor	Response
	and/or practices in the U.S. or can these rights be effectively applied in practice?	subject rights, including judicial redress. We do not believe the laws subject to us prevent us from enabling, supporting, and fulfilling data subject rights under the SCCs.
Onward transfers and exposure to government surveillance		
20.	Does the data importer share EU personal data further with sub-processors whose processing takes place in third countries?	Yes.
21.	What measures does the third-party data recipient take to ensure the protection of EU personal data transferred to it?	NAVEX Global enters into written agreements with sub-processors that include safeguards for EU personal data in accordance with the GDPR requirements.
22.	What assurances has the data importer received from third-party data recipients with respect to requests/demands for EU personal data from [U.S./other jurisdiction] public authorities?	NAVEX Global has updated, or is in the process of updating, all written agreements with sub-processors to include additional measures for the protection of EU personal data, where required.

Conclusion/Risk of transfers

Likely limited-risk data transfer

In particular, NAVEX Global identified the following factors (based on the assessment documented above and any additional information), that are likely to indicate a limited-risk transfer:

The data importer has never received requests/demands from intelligence services for disclosure of EU personal data.

The data importer has received limited requests/demands from public authorities for disclosure of EU personal data (such as for disclosure of employee data), but the requests related to regular criminal law procedure and did not go beyond what is necessary and proportionate to meet the purpose of the request.

The data importer has a process in place for handling and contesting public authority access requests, if received.

Based on the nature of its services and data processing activities, the data importer does not expect to be the target of requests/demands pursuant to national security or intelligence agencies for disclosure of EU personal data.

Such data transfers are not directly nor practically in scope of requests/demands from national security or intelligence agencies for disclosure of EU personal data.

D. Supplementary Measures

Notwithstanding the Conclusion set forth in the above TRA, NAVEX Global has also adopted the following supplemental measures. We believe that by implementing such supplemental measures, we are following best practices and are demonstrating our serious commitment to the protection of customer data.

Contractual safeguards	The SCCs themselves contain a number of contractual commitments by NAVEX Global and its customer, aimed at serving as safeguards for EU personal data.
	Supplementary contractual assurances are offered via our standard data processing addendum or an amendment to the data processing addendum. Please reach out to privacy@navexglobal.com in order to get this in place.
	NAVEX Global agrees to audit and monitor its obligations, and to support its customers auditing and monitoring obligations, regarding the level of government access to data.
	NAVEX Global provides a data processing agreement to support GDPR compliance, which includes the SCCs. As the data processor/importer, we process personal data strictly in accordance with your instructions and to provide the services. Our customers are the owners of the personal data within our service applications. NAVEX Global offers a Data Security Addendum, providing for contractual commitments to its information security program.
Organizational safeguards	NAVEX Global maintains written processes and procedures which provide for review of and limit the scope of EU personal data disclosed by NAVEX Global in response to requests from public authorities. Please see our Public Authority Disclosure Request Policy.
	NAVEX Global maintains internal record of requests made by public authorities concerning EU personal data.
	NAVEX Global takes steps to limit the volume of disclosed data, where possible.
	NAVEX Global would take data minimization measures such as redacting unnecessary identifiable personal data or personal data that may be of increased interest to intelligence agencies before complying with a request to disclosure EU personal data.
	NAVEX Global has developed a Standard Contractual Clauses Assurance Guide, which details our commitment to compliance with the SCCs. NAVEX Global remains a participant and has certified its compliance with the EU-U.S. Privacy Shield Framework and the Swiss- U.S. Privacy Shield Framework. NAVEX Global, Inc. is

	committed to subjecting all personal information received from the European Economic Area, United Kingdom, and Switzerland, respectively, in reliance on each Privacy Shield Framework, to the Frameworks' applicable Principles. To learn more about the Privacy Shield program, and to view our certification, please visit https://www.privacyshield.gov. NAVEX Global provides an independent recourse mechanism to EU individuals, currently TrustArc.
Technical safeguards	Encrypt personal data in transit.
	Encrypt personal data at rest.
	Appropriate access controls.
	Customers can implement data minimization (e.g., store the least amount of data necessary).
	Timespan for any access to personal data "in the clear" is limited to the specific function.
	Store personal data in the EU and enable only remote access.
	NAVEX Global equips its services with self-servicing functionality, allowing you to manage the personal data on your own through the use of the services. NAVEX Global engages a recognized, independent third party to conduct a Statement on Standards for Attestation Engagements No. 16, Service Organization Control 2, Type 2 ("SSAE 18 SOC 2 Type 2") audit (or its equivalent or successor) of its information security program and its administrative, technical, and physical safeguards for all facilities used to deliver the Services, which specifically includes privacy controls. NAVEX Global maintains an annual Standardized Information Gathering Questionnaire ("SIG"), which details our robust security program with supporting documentation.

Conclusion

Having regard to the level of risk of the data transfer (**limited risk**), NAVEX Global considers that the measures identified above are **sufficient and effective** in light of the circumstances of the transfers, in conjunction with the supplementary measures and safeguards provided by the SCCs, to allow the data importer to comply with its obligations under the SCCs and provide an appropriate level of protection for the transfer.

Hotline and Incident Management EU Hosted Sub-Processing Activity: Interpretations with Transatlantic Translations

NAVEX GLOBAL SUB-PROCESSING ACTIVITY

EU HOSTED HOTLINE AND INCIDENT MANAGEMENT – LIVE PHONE INTERPRETATION TRANSFER RISK ASSESSMENT

I. SCOPE

This TRA applies to NAVEX Global's EU Hosted Hotline customers. This TRA applies specifically to the live phone interpretations taking place as part of the Hotline services.

As part of NAVEX Global's Hotline service component, customers are provisioned with telephony for receiving reports submitted by individuals via telephone. When a call is received in the English language, no Interpreters are used. When a call is received in a language other than English, a sub-processor may be used to provide interpretation services. NAVEX Global outsources multi-lingual individuals and is therefore capable of processing calls received in languages other than English in some, but not all, instances. If NAVEX Global does not have any available agents capable of interpreting a call received in a particular language, NAVEX Global's sub-processor is contacted and the next available linguist who speaks the language needed is connected to the call ("Interpreter"), joining the reporter and a NAVEX Global contact centre agent. NAVEX Global does not have any discretion over who the Interpreter for a given call will be, or where they may be located, as there is no way to predict when a call will be received or what Interpreters will be available at that time. The individual Interpreters are located throughout the world to support growth in demand for non-English language services.

Once an Interpreter has been connected to the call, they will provide real-time interpretation services so that the NAVEX Global contact centre agent may collect the information from the reporter. The Interpreter does not record or maintain any report information and only makes a note of the date, the duration of the call, and the NAVEX Global billing ID to which the report pertains (for the purpose of billing NAVEX Global for the interpretation services).

II. TRANSFER ANALYSIS

In NAVEX Global's reasonable opinion, upon review with internal and outside counsel, it is unlikely that the interpretation services will be considered a transfer, as defined under the GDPR. There is a reasonable

argument, in the UK specifically, that a purely verbal disclosure of information to an interpreter does not trigger the GDPR's mandates, provided that the call (or a transcript of the call) is not recorded by the interpreter at any point in time.

Under UK decision *Scott v LGBT Foundation*, the court found that the information provided orally was not "recorded" and thus did not constitute "data" or "personal data", and accordingly, the (UK) Data Protection Act 1998 did not apply to that disclosure of information. The court also looked to the previous decision of the Court of Appeal in *Durant* v *Financial Services Authority* which confirms the need for information to be recorded in either electronic or manual form in order for it to constitute personal data. While the case was decided under the (UK) Data Protection Act 1998, the relevant provisions under the GDPR are analogous.

At no point is the information provided in the call recorded with the intention that it is processed in the future, but instead the interpretation happens "live", and no record is kept by the Interpreter. While this conclusion would need to be reviewed carefully across the Member States, the determination that live interpretation is not a transfer under the GDPR is reasonable considering the foregoing.

Nevertheless, NAVEX Global approaches its responsibilities with respect to privacy with utmost importance and considers it best practice to apply all the same compliance requirements to this sub-processing activity. As such, we have included interpretations as part of its TRA process.

III. ASSESSING THE ADEQUACY OF EU/UK DATA TRANSFERS – LIVE PHONE INTERPRETATION SERVICES

In assessing the adequacy of transfers of personal data from the EU/UK to NAVEX Global's sub-processor pursuant to the interpretation services provided by said sub-processor, we have taken the following steps:

1. **STEP 1:** Identified the relevant data transfers and the legal mechanism that NAVEX Global and sub-processor is relying on for such transfers (e.g., SCCs).

2. **STEP 2:** Conducted due diligence and collected information about the scope of the transfers, the exposure of the sub-processor to local law that may require disclosure of EU personal data about individuals, and any other relevant information.

3. **STEP 3:** Completed the "Transfer Risk Assessment" in **Section IV** to assess whether the SCCs is effective in light of all circumstances of the transfer.

4. **STEP 4:** Included additional "Supplementary Measures" as set forth in **Section IV (D)**.

5. **STEP 5:** Documented the assessment for accountability purposes. We encourage our customers to do the same.

6. **STEP 6:** NAVEX Global and its sub-processor is responsible for the periodic review of the assessment, which should take place at least annually, to ensure that the transfer of the EU personal data continues to be afforded an adequate level of protection.

IV. TRANSFER RISK ASSESSMENT

Name Of Data Importer: Transatlantic Translations Limited **(**NAVEX Global's sub-processor)
Completed By: NAVEX Global's Privacy Team and TTG's Vicki Crothall
Date: 25 September 2021

A. Type of Data Importer

Name of data importer: Transatlantic Translations Limited, on behalf of itself and Transatlantic Translations Company, LLC ("TTG"). The Processor to Processor SCCs between NAVEX Global and TTG is part of a master services agreement between NAVEX Global and TTG.

Does TTG provide the following services to NAVEX Global:

	Data Importer	
Telecommunications	☐ Yes	☒ No
Other electronic communications (such as an Internet Service Provider or a provider of email, text message, VoIP, remote desktop or VPN services)?	☐ Yes	☒ No
Remote computing services	☐ Yes	☒ No
Other communications service where there may be access to wire or electronic communications	☒ Yes	☐ No

TTG acknowledges that its services could be viewed as meeting the definition of a communication service.

B. Details of Data Transfers

Data transfer mechanism Appropriate Processor to Processor SCCs between TTG and NAVEX Global.
Scope of personal data covered by the data transfer mechanism in place The SCCs cover transfers of EU personal data from the EEA/UK to third countries, including the following categories of data subjects: • Employees of customer Data Controller • Clients, business partners and vendors of customer Data Controller (who are natural persons) • Employees or contact persons of customer Data Controllers' third-party suppliers, business partners and vendors • Customer Data Controller's users authorized by data exporter to use the relevant Service(s)

C. Transfer Risk Assessment

The table below aids identification and evaluation of risk factors in relation to the specific data transfer. The assessment of each risk factor is recorded in appropriate detail.

#	Factor	Response
Scope of the transfers		
1.	What is the type of transfer?	Live phone interpretation. There is no storage or remote access by TTG. The call is not recorded nor transcribed by the individual interpreters.
2.	Is the transfer necessary?	

#	Factor	Response
		Yes. The transfer is critical and necessary to provide the services to NAVEX Global, on behalf of NAVEX Global's customers. To intake reports from individuals on important ethics and compliance matters, we must be able the provide the best language support resources available, to allow these reporters effective whistle blowing capabilities.
3.	Is the transfer proportionate?	Yes. The transfer is strictly limited to interpreting the given reported information via the phone call only.
4.	Is the transfer occasional/non-routine or frequent/routine?	The transfer is occasional and non-routine to TTG interpreters on a per call basis.
5.	Will the transferred personal data be processed for a relatively long or short period of time?	Personal data transferred is processed for a relatively short period of time, in order to interpret the live phone call.
6.	Is the transferred data encrypted and/ or pseudonymized?	Yes. Encryption – when the call reaches NAVEX Global's platform (and thereafter, the Interpreters), the data is encrypted with 256 AES encryption both in transit and at rest. NAVEX Global and NAVEX Global's customer using the Interpreting services will ensure their own data encryption arrangements are in place.
Specific circumstances of the transfer		
7.	What are the purposes for which the data are transferred and processed?	To provide the best language interpretation support to hotline reporters.
8.	What are the types of entities involved in the processing?	TTG is a data sub-processor and a private company. NAVEX Global is a data processor and private company. NAVEX Global's customers are the data controllers and may consist of both private and public companies.
9.	In which sector does the transfer occur?	NAVEX Global provides risk and compliance management SaaS based software. ***This factor is especially important as the purposes of our services are to enable organizations to support their risk, ethics, and compliance programs. ***
10.	What are the categories of personal data transferred?	As instructed by NAVEX Global's customer, including but not limited to:

#	Factor	Response

		• name, job title, job position, location, employer, relationship with the organization, e-mail address, telephone number, log-in credentials, date of birth;
		• for whistle-blower hotline reports, in addition to the foregoing, the following may also be captured:
		  o facts reported by a reporter about a suspected violation, including how and where the suspected violation occurred and how the reporter learned about the suspected violation;
		  o identity, function and contact details of individuals allegedly involved in the suspected violation; and
		  o identity, function and contact details of individuals who could provide information relating to the suspected violation.
		
		Given the nature of hotline services, reporters may submit sensitive categories of data in a report. NAVEX Global recommends its customers have strict policies around the management of such report data in their use of the services, in accordance with the laws subject to them.

11.	What is the format of the personal data to be transferred?	When access is provided to an individual interpreter for the purposes described in this TRA, personal data must be accessible in the clear to provide the interpretation. The data is encrypted in transit and at rest as detailed above.
12.	What is the storage location of the data transferred?	The European Union via NAVEX Global's secure data centres.
13.	What are the sub-sub-processing activities?	Please see details here: https://www.navexglobal.com/en-us/service-hosting-providers. For the interpretation services, TTG engages Language Services Associates for additional interpreter resources. This processing activity is still limited to the interpretation of a phone call and subject to all the same compliance requirements.
Importer's exposure to government surveillance and practical application of Section 702 FISA		
14.	Is the data importer's sector or business	

#	Factor	Response
	directly subject to such laws in its jurisdiction that permit government access to personal data, or require the assistance of data importer to disclose personal data to public authorities, for surveillance and intelligence gathering purposes?	No, TTG's business is currently not directly subject to such laws.
	a. Specifically, what is data importer's analysis regarding third country surveillance laws, especially Section 702 FISA, under the SCCs and EDPB Guidance?	1) Data exporters may decide to proceed with the transfer without supplementary measures, if they consider there to be no reason to believe that the relevant and problematic legislation (for example, those in the U.S.) will be applied, in practice, to the transferred data and/or TTG. a. In our reasonable opinion upon internal and outside counsel review, we do not find third country surveillance laws, including Section 702 FISA from the U.S., to practically apply to these transfers. b. It is important to note that given the broad definitions of these laws, the vast majority of organizations are going to have to acknowledge their potential application. However, this does not mean they directly apply or practically apply in practice. c. We believe TTG is generally out of scope and that these laws are overall not going to apply to the services we provide, as the intent is for surveillance of certain telecom and internet service providers for targeted information. This typically involves surveillance of real time emails, texts, and chat conversations. The foregoing is not what NAVEX Global nor TTG provides and in order to obtain this sought for information, authorities would pursue those providers directly as it would be impractical to make a request through TTG. 2) Data exporters may also take into consideration documented practical experience of data importer with relevant prior instances of requests for access received from public authorities, including those in the U.S. a. ***To this point, TTG has never received a Section 702 FISA**

#	Factor	Response
		request, an EO 12.333 request or order, or any other country access request. * b. The EDPB Guidance implies that the lack of requests received in the past plus no prohibition on providing information about such requests, could be sufficient to conclude Section 702 FISA does not apply in practice. Note there is no prohibition on TTG to provide information about these requests. 3) If you conclude Section 702 FISA, or any other potential similar types of surveillance law, does not apply in practice to the particular transfer, it is possible to proceed with the transfer without any supplementary measures. **While NAVEX Global and TTG take the approach that Section 702 FISA does not apply in practice, we still have elected to provide for supplementary measures with regard to these transfers. Please see Section IV (D).**
15.	Within the last three (3) years, has the data importer received requests/demands from public authorities in its jurisdiction to disclose EU personal data?	Based on available information, TTG's entities in the U.S. do not receive requests/demands for disclosure of, or access to, EU personal data.
	a. Approximately how many requests/demands from public authorities has the data importer received in that time period concerning EU personal data?	None, to the best of our knowledge.
	b. Approximately how many of these requests/demands are pursuant to criminal law procedure in the destination country? *[Regular court proceedings are not the issue under Schrems II, but intelligence programs are scrutinized.]*	None, to the best of our knowledge.
	c. Approximately how many of these requests/demands are pursuant to national security or intelligence agencies in the destination country?	None, to the best of our knowledge. TTG can represent that it has not received requests/demands from intelligence agencies.
	d. Has the data importer been able to contest/minimize such disclosure of EU personal data, where appropriate?	Not applicable.
	e. What types of EU personal data has the data importer been required to disclose to public authorities in its jurisdiction?	Not applicable.
16.	How likely is it that the data importer will receive bulk data surveillance requests to	Unlikely. TTG's entities in the U.S. do not

#	Factor	Response
	disclose EU personal data to public authorities in its jurisdiction in the future (e.g., based on factors such as the type of services provided and sector in which the data importer operates, its size, number of customers and reputation)?	receive requests/demands by public authorities for disclosure of, or access to, EU personal data, and have no reason to believe that they might receive such in the future.
17.	Does the data importer maintain annual reports or statistics regarding requests/demands received from law enforcement or intelligence agencies (e.g., number/type of requests/demands, requesting authority, etc.)?	Not applicable. TTG has not received requests from public authorities for EU personal data under the SCCs or otherwise. As a result, if TTG gets such requests in the future, it will notify NAVEX Global and this TRA will be updated accordingly.
18.	Does the data importer maintain a written procedure(s) for: 1. Responding to or challenging requests/ demands of law enforcement or intelligence agencies that apply to EU personal data? 2. Informing customers of requests/demands from law enforcement or intelligence agencies where permitted by applicable law?	Yes. While TTG has never received such requests, it does have a policy and procedure should the event ever happen. Included in the procedure, there will be a list of any and all such requests.
19.	Are the data importer's commitments enabling data subjects to exercise their rights as provided in the SCCs thwarted by the laws and/or practices in the U.S. and any other third countries involved, or can these rights be effectively applied in practice?	Data subjects' rights can be effectively applied in practice. TTG has never encountered a situation where it felt it could not enable data subject rights, including judicial redress. We do not believe the laws subject to us prevent us from enabling, supporting, and fulfilling data subject rights under the SCCs.
Onward transfers and exposure to government surveillance		
20.	Does the data importer share EU personal data further with third-party data recipients in [the U.S./other jurisdiction]?	Yes. TTG utilizes Language Services Associates (LSA) for additional interpretation resources.
21.	What measures does the third-party data recipient take to ensure the protection of EU personal data transferred to it?	Where TTG engages LSA to have access to EU personal data, TTG enters into written agreements with LSA that include safeguards for EU personal data in accordance with the GDPR requirements.
22.	What assurances has the data importer received from third-party data recipients with respect to requests/demands for EU personal data from [U.S./other jurisdiction] public authorities?	TTG has updated written agreements, or has ensured such updates are in progress, with LSA to include additional measures for the protection of EU personal data, where required.
23.	Is the vendor's (or its sub-processor's) sector or business directly subject to such laws in its jurisdiction that permit government access to personal data, or require the assistance of data importer to disclose personal data to	No, TTG does not believe in its reasonable opinion that it or its sub-processors are directly subject to such laws in their jurisdiction.

#	Factor	Response
	public authorities, for surveillance and intelligence gathering purposes?	

Conclusion/Risk of transfers

Very limited-risk data transfer

In particular, TTG and NAVEX Global identified the following factors (based on the assessment documented above and any additional information), that are likely to indicate a very limited-risk transfer:

No further processing outside of an interpretation of a live phone call takes place. As such, it is reasonable to determine that no transfer is taking place under the GDPR.

The data importer has never received requests/demands from intelligence services for disclosure of EU personal data.

The data importer has received limited requests/demands from public authorities for disclosure of EU personal data (such as for disclosure of employee data), but the requests related to regular criminal law procedure and did not go beyond what is necessary and proportionate to meet the purpose of the request.

The data importer has a process in place for handling and contesting public authority access requests, if received.

Based on the nature of its services and data processing activities, the data importer does not expect to be the target of requests/demands pursuant to national security or intelligence agencies for disclosure of EU personal data.

Such data transfers are not directly nor practically in scope of requests/demands from national security or intelligence agencies for disclosure of EU personal data.

D. Supplementary Measures

Notwithstanding the Conclusion set forth in the above TRA, TTG has also adopted the following supplemental measures. We believe that by implementing such supplemental measures, we are following best practices and are demonstrating our serious commitment to the protection of customer data.

Contractual safeguards	TTG and NAVEX Global have entered into supplementary contractual assurances as an amendment to the data processing addendum.
	The SCCs themselves contain a number of contractual commitments by TTG and NAVEX Global, aimed at serving as safeguards for EU personal data. We have also entered into a robust general data processing addendum.
	TTG is committed to implementing other transparency, audit and monitoring obligations regarding the level of government access to data, including, a policy and process to address any potential requests for disclosure to governmental agencies around the world. This is to include a legend of any such request received and actioned.

Organizational safeguards	TTG maintains written processes and procedures provide for review of and limit the scope of EU personal data disclosed by TTG in response to requests from public authorities.
	TTG would maintain internal record of requests made by public authorities concerning EU personal data.
	TTG takes steps to limit the volume of disclosed data, where possible.
	TTG would take data minimization measures such as redacting unnecessary identifiable personal data or personal data that may be of increased interest to intelligence agencies before complying with a request to disclosure EU personal data.
Technical safeguards	Encrypt personal data in transit, as detailed above
	Encrypt personal data at rest, as detailed above.
	Appropriate access controls.
	Calls are not recorded, ensuring the limit timespan for processing personal data "in the clear" (i.e., in identifiable form).

Conclusion

Having regard to the level of risk of the data transfer (**very limited risk**), TTG and NAVEX Global consider that the measures identified above are **sufficient and effective** in light of the circumstances of the transfers, in conjunction with the supplementary measures and safeguards provided by the SCCs, to allow the data importer to comply with its obligations under the SCCs and provide an appropriate level of protection for the transfer.

Hotline and Incident Management EU Hosted Sub-Processing Activity: Translations with Transatlantic Translations

NAVEX GLOBAL SUB-PROCESSING ACTIVITY

EU HOSTED HOTLINE AND INCIDENT MANAGEMENT – WEB REPORT TRANSLATIONS TRANSFER RISK ASSESSMENT

I. SCOPE

This TRA applies to NAVEX Global's EU Hosted Incident Management customers. This TRA applies specifically to the web report translation services taking place as part of the Incident Management services.

As part of NAVEX Global's Incident Management service component, customers are provided with a web intake site to receive reports submitted via the web. When a report is received via the website in a language other than English, an electronic copy of the report is sent, in its original language, to a secure web-portal (the "Translation Management System") managed by Transatlantic Translations. A translator, who may be located in various countries throughout the world, then logs into the Translation Management System, performs the translation, and sends the report back through the Translation Management System for the NAVEX Global communication specialist to retrieve. The Translation Management System for Transatlantic Translation resides on servers owned by Wordbee S.A. in Amsterdam---via Microsoft Azure. Once the translation is complete and returned to NAVEX Global, the report is deleted permanently within the Translation Management System.

II. ASSESSING THE ADEQUACY OF EU/UK DATA TRANSFERS – WEB REPORT TRANSLATION SERVICES

In assessing the adequacy of transfers of personal data from the EU/UK to NAVEX Global's sub-processor pursuant to the web report translation services provided by said sub-processor, we have taken the following steps:

1. **STEP 1:** Identified the relevant data transfers and the legal mechanism that NAVEX Global and sub-processor is relying on for such transfers (e.g., SCCs).

2. **STEP 2:** Conducted due diligence and collected information about the scope of the transfers, the exposure of the sub-processor to local law that may require disclosure of EU personal data about individuals, and any other relevant information.

3. **STEP 3:** Completed the "Transfer Risk Assessment" in **Section IV** to assess whether the SCCs is effective in light of all circumstances of the transfer.

4. **STEP 4:** Included additional "Supplementary Measures" as set forth in **Section IV (D)**.

5. **STEP 5:** Documented the assessment for accountability purposes. We encourage our customers to do the same.

6. **STEP 6:** NAVEX Global and its sub-processor is responsible for the periodic review of the assessment, which should take place at least annually, to ensure that the transfer of the EU personal data continues to be afforded an adequate level of protection.

III. TRANSFER RISK ASSESSMENT

Name Of Data Importer: Transatlantic Translations Limited **(**NAVEX Global's sub-processor)
Completed By: NAVEX Global's Privacy Team and Vicki Crothall
Date: 25 September 2021

A. Type of Data Importer

Name of data importer: Transatlantic Translations Limited, on behalf of itself and Transatlantic Translations Company, LLC ("TTG"). The Processor to Processor SCCs between NAVEX Global and TTG is part of a master services agreement between NAVEX Global and TTG.

Does TTG provide the following services to NAVEX Global:

	Data Importer

Telecommunications	☐ Yes	☒ No
Other electronic communications (such as an Internet Service Provider or a provider of email, text message, VoIP, remote desktop or VPN services)?	☐ Yes	☒ No
Remote computing services	☐ Yes	☒ No
Other communications service where there may be access to wire or electronic communications	☒ Yes	☐ No

TTG acknowledges that its services could be viewed as meeting the definition of a communication service.

B. Details of Data Transfers

Data transfer mechanism Appropriate Processor to Processor SCCs between TTG and NAVEX Global.
Scope of personal data covered by the data transfer mechanism in place The SCCs cover transfers of EU personal data from the EEA/UK to third countries, including the following categories of data subjects: • Employees of customer Data Controller • Clients, business partners and vendors of customer Data Controller (who are natural persons) • Employees or contact persons of customer Data Controllers' third-party suppliers, business partners and vendors • Customer Data Controller's users authorized by data exporter to use the relevant Service(s)

C. Transfer Risk Assessment

The table below aids identification and evaluation of risk factors in relation to the specific data transfer. The assessment of each risk factor is recorded in appropriate detail.

#	Factor	Response
Scope of the transfers		
1.	What is the type of transfer?	Web report translation services. There is no persistent storage or access by TTG. The processing by the individual translators is limited to the performance of the translation of the given web report.
2.	Is the transfer necessary?	Yes. The transfer is critical and necessary to provide the services to NAVEX Global, on behalf of NAVEX Global's customers. To intake reports from individuals on important ethics and compliance matters, we have to be able the

#	Factor	Response
		provide the best language support resources available, to allow these reporters effective whistle blowing capabilities.
3.	Is the transfer proportionate?	Yes. The transfer is strictly limited to translating the reported information submitted via the website.
4.	Is the transfer occasional/non-routine or frequent/routine?	The transfer is occasional and non-routine to TTG translators on a per report basis.
5.	Will the transferred personal data be processed for a relatively long or short period of time?	Personal data transferred is processed for a relatively short period of time, in order to translate the report.
6.	Is the transferred data encrypted and/ or pseudonymized?	Yes. Encryption - all data, including all files uploaded to the Wordbee Translation Management System, all translated data, translation memories, projects, jobs, users, and companies, etc.—is encrypted at transfer time and while at rest. The encryption technologies that Wordbee uses, for the Translation Management System, meet industry security standards for preventing malicious attacks and data theft and for ensuring that data is protected.
Specific circumstances of the transfer		
7.	What are the purposes for which the data are transferred and processed?	To provide the best language translation support to web reporters.
8.	What are the types of entities involved in the processing?	TTG is a data sub-processor and a private company. NAVEX Global is a data processor and private company. NAVEX Global's customers are the data controllers and may consist of both private and public companies.
9.	In which sector does the transfer occur?	NAVEX Global provides risk and compliance management SaaS based software. ***This factor is especially important as the purposes of our services are to enable organizations to support their risk, ethics, and compliance programs. ***
10.	What are the categories of personal data transferred?	As instructed by NAVEX Global's customer, including but not limited to: • name, job title, job position, location,

#	Factor	Response
		employer, relationship with the organization, e-mail address, telephone number, log-in credentials, date of birth; • for whistle-blower hotline and case management reports, in addition to the foregoing, the following may also be captured: o facts reported by a reporter about a suspected violation, including how and where the suspected violation occurred and how the reporter learned about the suspected violation; o identity, function and contact details of individuals allegedly involved in the suspected violation; and o identity, function and contact details of individuals who could provide information relating to the suspected violation. Given the nature of incident management services, reporters may submit sensitive categories of data in a report. NAVEX Global recommends its customers have strict policies around the management of such report data in their use of the services, in accordance with the laws subject to them.
11.	What is the format of the personal data to be transferred?	When access is provided to an individual translator for the purposes described in this TRA, personal data must be accessible in the clear to provide the translation. The data is encrypted as detailed above.
12.	What is the storage location of the data transferred?	The European Union via the Wordbee Translator and ultimately via NAVEX Global's secure data centres.
13.	What are the sub-sub-processing activities?	Please see details here: https://www.navexglobal.com/en-us/service-hosting-providers. For the translation services, TTG engages Wordbee for the secure hosting of the translation management system. Wordbee utilizes the secure environment of Microsoft Azure. Storage and hosting as part of these sub-sub-processing activities is located within the European Union.
Importer's exposure to government surveillance and practical application of Section 702 FISA		
14.	Is the data importer's sector or business directly subject to such laws in its jurisdiction	No, TTG's business is currently not directly

#	Factor	Response
	that permit government access to personal data, or require the assistance of data importer to disclose personal data to public authorities, for surveillance and intelligence gathering purposes?	subject to such laws.
	a. Specifically, what is data importer's analysis regarding third country surveillance laws, especially Section 702 FISA, under the SCCs and EDPB Guidance?	4) Data exporters may decide to proceed with the transfer without supplementary measures, if they consider there to be no reason to believe that the relevant and problematic legislation (for example, those in the U.S.) will be applied, in practice, to the transferred data and/or TTG. a. In our reasonable opinion upon internal and outside counsel review, we do not find third country surveillance laws, including Section 702 FISA from the U.S., to practically apply to these transfers. b. It is important to note that given the broad definitions of these laws, the vast majority of organizations are going to have to acknowledge their potential application. However, this does not mean they directly apply or practically apply in practice. c. We believe TTG is generally out of scope and that these laws are overall not going to apply to the services we provide, as the intent is for surveillance of certain telecom and internet service providers for targeted information. This typically involves surveillance of real time emails, texts, and chat conversations. The foregoing is not what NAVEX Global nor TTG provides and in order to obtain this sought for information, authorities would pursue those providers directly as it would be impractical to make a request through TTG. 5) Data exporters may also take into consideration documented practical experience of data importer with relevant prior instances of requests for access received from public authorities, including those in the U.S. c. *** To this point, TTG has never received a Section 702 FISA request, an EO 12.333 request or**

#	Factor	Response
		order, or any other country access request. * d. The EDPB Guidance implies that the lack of requests received in the past plus no prohibition on providing information about such requests, could be sufficient to conclude Section 702 FISA does not apply in practice. Note there is no prohibition on TTG to provide information about these requests. 6) If you conclude Section 702 FISA, or any other potential similar types of surveillance law, does not apply in practice to the particular transfer, it is possible to proceed with the transfer without any supplementary measures. **While NAVEX Global and TTG take the approach that Section 702 FISA does not apply in practice, we still have elected to provide for supplementary measures with regard to these transfers. Please see Section IV (D).**
15.	Within the last three (3) years, has the data importer received requests/demands from public authorities in its jurisdiction to disclose EU personal data?	Based on available information, TTG entities in the U.S. do not receive requests/demands for disclosure of, or access to, EU personal data.
	a. Approximately how many requests/demands from public authorities has the data importer received in that time period concerning EU personal data?	None, to the best of our knowledge.
	b. Approximately how many of these requests/demands are pursuant to criminal law procedure in the destination country? *[Regular court proceedings are not the issue under Schrems II, but intelligence programs are scrutinized.]*	None, to the best of our knowledge.
	c. Approximately how many of these requests/demands are pursuant to national security or intelligence agencies in the destination country?	None, to the best of our knowledge. The data importer can represent that it has not received requests/demands from intelligence agencies.
	d. Has the data importer been able to contest/minimize such disclosure of EU personal data, where appropriate?	Not applicable.
	e. What types of EU personal data has the data importer been required to disclose to public authorities in its jurisdiction?	Not applicable.
16.	How likely is it that the data importer will receive bulk data surveillance requests to disclose EU personal data to public	Unlikely. TTG's entities in the U.S. do not receive requests/demands by public authorities

#	Factor	Response
	authorities in its jurisdiction in the future (e.g., based on factors such as the type of services provided and sector in which the data importer operates, its size, number of customers and reputation)?	for disclosure of, or access to, EU personal data, and have no reason to believe that they might receive such in the future.
17.	Does the data importer maintain annual reports or statistics regarding requests/demands received from law enforcement or intelligence agencies (e.g., number/type of requests/demands, requesting authority, etc.)?	Not applicable. TTG has not received requests from public authorities for EU personal data under the SCCs or otherwise. As a result, if TTG gets such requests in the future, it will notify NAVEX Global and this TRA will be updated accordingly.
18.	Does the data importer maintain a written procedure(s) for: 1. Responding to or challenging requests/ demands of law enforcement or intelligence agencies that apply to EU personal data? 3. Informing customers of requests/demands from law enforcement or intelligence agencies where permitted by applicable law?	Yes. While TTG has never received such requests, it does have a policy and procedure should the event ever happen. Included in the procedure, there will be a list of any and all such requests.
19.	Are the data importer's commitments enabling data subjects to exercise their rights as provided in the SCCs thwarted by the laws and/or practices in the U.S. and any other third countries involved, or can these rights be effectively applied in practice?	Data subjects' rights can be effectively applied in practice. TTG has never encountered a situation where it felt it could not enable data subject rights, including judicial redress. We do not believe the laws subject to us prevent us from enabling, supporting, and fulfilling data subject rights under the SCCs.
Onward transfers and exposure to government surveillance		
20.	Does the data importer share EU personal data further with third-party data recipients in [the U.S./other jurisdiction]?	Yes. TTG utilizes Wordbee specifically for their Translation Management System for the processing of all Translation requests. Only TTG Secure Linguists complete the actual translation work.
21.	What measures does the third-party data recipient take to ensure the protection of EU personal data transferred to it?	Where TTG engages Wordbee that have access to EU personal data, TTG enters into written agreements with Wordbee that include safeguards for EU personal data in accordance with the GDPR requirements.
22.	What assurances has the data importer received from third-party data recipients with respect to requests/demands for EU personal data from [U.S./other jurisdiction] public authorities?	TTG has updated written agreements, or has ensured such updates are in progress, with Wordbee to include additional measures for the protection of EU personal data, where required.
23.	Is the vendor's (or its sub-processor's) sector or business directly subject to such laws in its jurisdiction that permit government access to	No, TTG does not believe in its reasonable

#	Factor	Response
	personal data, or require the assistance of data importer to disclose personal data to public authorities, for surveillance and intelligence gathering purposes?	opinion that it or its sub-processors are directly subject to such laws in their jurisdiction.

Conclusion/Risk of transfers

Very limited-risk data transfer

In particular, TTG and NAVEX Global identified the following factors (based on the assessment documented above and any additional information), that are likely to indicate a very limited-risk transfer:

No further processing outside of translation of a given web report takes place.

The data importer has never received requests/demands from intelligence services for disclosure of EU personal data.

The data importer has received limited requests/demands from public authorities for disclosure of EU personal data (such as for disclosure of employee data), but the requests related to regular criminal law procedure and did not go beyond what is necessary and proportionate to meet the purpose of the request.

The data importer has a process in place for handling and contesting public authority access requests, if received.

Based on the nature of its services and data processing activities, the data importer does not expect to be the target of requests/demands pursuant to national security or intelligence agencies for disclosure of EU personal data.

Such data transfers are not directly nor practically in scope of requests/demands from national security or intelligence agencies for disclosure of EU personal data.

D. Supplementary Measures

Notwithstanding the Conclusion set forth in the above TRA, TTG has also adopted the following supplemental measures. We believe that by implementing such supplemental measures, we are following best practices and are demonstrating our serious commitment to the protection of customer data.

Contractual safeguards	TTG and NAVEX Global have entered into supplementary contractual assurances as an amendment to the data processing addendum.
	The SCCs themselves contain a number of contractual commitments by TTG and NAVEX Global, aimed at serving as safeguards for EU personal data. We have also entered into a robust general data processing addendum.
	TTG is committed to implementing other transparency, audit and monitoring obligations regarding the level of government access to data, including, a policy and process to address any potential requests for disclosure to governmental agencies around the world. This is to include a legend of any such request received and

	actioned.
Organizational safeguards	TTG maintains written processes and procedures provide for review of and limit the scope of EU personal data disclosed by TTG in response to requests from public authorities.
	TTG would maintain internal record of requests made by public authorities concerning EU personal data.
	TTG takes steps to limit the volume of disclosed data, where possible.
	TTG would take data minimization measures such as redacting unnecessary identifiable personal data or personal data that may be of increased interest to intelligence agencies before complying with a request to disclosure EU personal data.
Technical safeguards	Encrypt personal data in transit, as detailed above.
	Encrypt personal data at rest, as detailed above.
	Translation Management System encryption key kept in the EU.
	Appropriate access controls.
	Limit timespan is ensured for using personal data "in the clear" (i.e., in identifiable form).
	Store personal data in the EU and enable only remote access or view-only access.

Conclusion

Having regard to the level of risk of the data transfer (**very limited risk**), TTG and NAVEX Global consider that the measures identified above are **sufficient and effective** in light of the circumstances of the transfers, in conjunction with the supplementary measures and safeguards provided by the SCCs, to allow the data importer to comply with its obligations under the SCCs and provide an appropriate level of protection for the transfer.

PolicyTech: EU Hosted

NAVEX GLOBAL

EU HOSTED POLICYTECH - EU/UK DATA TRANSFER RISK ASSESSMENTS

I. INTRODUCTION

NAVEX Global must conduct Transfer Risk Assessments ("TRA" or "TRAs") for transfers of personal data from the European Economic Area ("EEA")[2] or the United Kingdom ("UK") (collectively "EU personal data") to third countries that are not deemed to provide an adequate level of data protection.

II. SCOPE

These TRAs apply to NAVEX Global's EU Hosted PolicyTech customers.

This TRA process applies to personal data transferred to NAVEX Global pursuant to the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council. This TRA is specifically designed to address Clause 14 of the foregoing set of Standard Contractual Clauses. Personal data from the UK is also in scope and shall be assessed pursuant to the European Commission's decision (C(2010)593) of 5 February 2010 on Standard Contractual Clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection. We collectively refer to the sets of Standard Contractual Clauses as the "SCCs." NAVEX Global agrees and acknowledges the UK will be issuing its own set of standard contractual clauses and related Schrems II guidance. We will update this TRA on an ongoing basis as needed.

This TRA process takes into account the European Data Protection Board's Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data adopted on 18 June 2021 (the "EDPB Guidance").

This TRA is not intended for transfers (i) within the EEA, (ii) between the EEA and the UK, or (iii) from the EEA or UK to a country recognized by the European Commission or UK law as adequate at this time (i.e., Andorra, Argentina, Canada (commercial organizations subject to PIPEDA), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, UK, and Uruguay).

The TRA is completed by the NAVEX Global Privacy Team, which consists of the Data Privacy Officer & Senior Counsel, Deputy Data Privacy Officer & Senior Counsel, and Privacy Counsel.

III. ASSESSING THE ADEQUACY OF EU/UK DATA TRANSFERS – TO NAVEX GLOBAL IN THE U.S.

In assessing the adequacy of transfers of personal data from the EU/UK to NAVEX Global in the U.S. we have taken the following steps:

1. **STEP 1:** Identified the relevant data transfers and the legal mechanism that NAVEX Global is relying on for such transfers (e.g., SCCs).

2. **STEP 2:** Conducted due diligence and collected information about the scope of the transfers, the exposure of NAVEX Global to local law that may require disclosure of EU personal data about individuals, and any other relevant information.

3. **STEP 3:** Completed the "Transfer Risk Assessment" in **Section IV** to assess whether the SCCs is effective in light of all circumstances of the transfer.

4. **STEP 4:** Included additional "Supplementary Measures" as set forth in **Section IV (D)**.

[2] The European Economic Area consists of the Member States of the EU (Austria, Belgium, Bulgaria, Croatia, Cyprus, Czechia, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain and Sweden), plus Iceland, Liechtenstein and Norway.

5. **STEP 5:** Documented the assessment for accountability purposes. We encourage our customers to do the same.

6. **STEP 6:** NAVEX Global is responsible for the periodic review of the assessment, which should take place at least annually, to ensure that the transfer of the EU personal data continues to be afforded an adequate level of protection.

IV. TRANSFER RISK ASSESSMENT

Name Of Data Importer: NAVEX Global
Scope of TRA: Transfers to NAVEX Global's affiliates in the United States as part of the PolicyTech services provided to EU Hosted Customers
Completed By: NAVEX Global's Privacy Team
Date: 25 September 2021

A. Type of Data Importer

Name of data importer: NAVEX Global. The SCCs between customer and NAVEX Global is part of a master services agreement between customer and NAVEX Global UK Limited (registered in the UK) or GCS Compliance Services Europe Unlimited Company trading as NAVEX Global (registered in Ireland), both with their principal places of business at Vantage West – 4th floor, Great West Road, Brentford TW8 9AG, United Kingdom. Some EU Hosted customers elect to contract directly with our U.S. entity, NAVEX Global, Inc., a Delaware corporation with its principal place of business at 5500 Meadows Road, Suite 500, Lake Oswego, OR 97035.

Upon reviewing the broad definitions set forth within U.S. surveillance laws under scrutiny pursuant to the CJEU ruling in the Schrems II case, NAVEX Global identifies itself as follows:

NAVEX Global does not consider itself a "telecommunications carrier" as defined in 47 U.S.C. 152.

NAVEX Global acknowledges that certain of its services could be viewed by U.S. government authorities as an "electronic communication service" as defined in 18 U.S.C. 2510.

NAVEX Global acknowledges that certain of its services could be viewed by U.S. government authorities as a "remote computing service" as defined in 18 U.S.C. 2711.

NAVEX Global acknowledges that certain of its services could be viewed by U.S. government authorities as other communication services where there may be access to wire or electronic communications.

B. Details of Data Transfers

Data transfer mechanism Appropriate Controller to Processor SCCs between customer and NAVEX Global.
Scope of personal data covered by the data transfer mechanism in place The SCCs cover transfers of EU personal data from the EEA/UK to the U.S., including the following categories of data subjects: • Employees of data exporter • Clients, business partners and vendors of data exporter (who are natural persons) • Employees or contact persons of data exporters' third-party suppliers, business partners and vendors

- Data exporter's users authorized by data exporter to use the relevant Service(s)

C. Transfer Risk Assessment

The table below aids identification and evaluation of risk factors in relation to the specific data transfer. The assessment of each risk factor is recorded in appropriate detail.

#	Factor	Response
Scope of the transfers		
1.	What is the type of transfer?	Remote access only by direct NAVEX Global personnel located in the U.S. to personal data stored in the EU. Personal data is not stored in the U.S. as part of this transfer.
2.	Is the transfer necessary?	Yes. NAVEX Global has critical resources located in the U.S., requiring access to the EU hosted database for the following purposes: • Support. General support cases that are submitted, depending on the case, may require access to customer data to address the issue at hand. To meet our service level commitments, U.S. support may be involved accordingly. This is mainly due to certain resource limitations based on location, an overflow of support cases, and time zone challenges. • Administrative Service Functions. There is certain work, for example setting up the landing page, that does not necessarily require a deep level access, but for which can result in a transfer of personal data to the U.S. depending on the service need. • Technical Work. Many of our technical resources are in the U.S. which requires access to customer data. Examples include certain data extract services, certain data migration services, integration services, user setups instances, and hosting installations. again, depending on the task, we need the option to leverage those resources which involves a certain level of access. • IT/Hosting. Select members of the hosting and information security group must have access for maintenance and

#	Factor	Response
		troubleshooting. Without the above, our service level commitments would greatly suffer, and the overall maintenance and security of our service would be put at great risk.
3.	Is the transfer proportionate?	Yes. Access is not provided to personnel in the U.S. in a general sense. Access is provided to those personnel in the U.S. on a strict need to know basis to perform their given job function.
4.	Is the transfer occasional/non-routine or frequent/routine?	The transfer is non-routine to NAVEX Global personnel in the U.S. for the purposes detailed in Factor #2 above.
5.	Will the transferred personal data be processed for a relatively long or short period of time?	Personal data transferred to the U.S. in this context is processed for a relatively short period of time to provide the applicable service support.
6.	Is the transferred data encrypted and/ or pseudonymized?	Yes. NAVEX Global employs encryption at rest using either full-disk encryption or within the database using TDE. Data at rest will be encrypted using AES 256 or better, data in flight will be accomplished using TLS 1.2 or higher on public untrusted networks. Upon reviewing pseudonymization in the context of this transfer, it is inapplicable to the services we need to support.
Specific circumstances of the transfer		
7.	What are the purposes for which the data are transferred and processed?	To provide the best support, maintenance, and services as committed to in our agreements with our customers.
8.	What are the types of entities involved in the processing?	NAVEX Global is a data processor and a private company. Our customers are the data controllers and may consist of both private and public companies.
9.	In which sector does the transfer occur?	NAVEX Global provides risk and compliance management SaaS based software. ***This factor is especially important as the**

#	Factor	Response
		purposes of our services is to enable organizations support their risk, ethics, and compliance programs. *
10.	What are the categories of personal data transferred?	As instructed by NAVEX Global's customer, including but not limited to: • Name (first and last), email address, job site, job title, department, supervisor, log-in credentials, completion status, time and date of policies. ****No sensitive data, as defined under the GDPR, is transferred as part of the PolicyTech services.****
11.	What is the format of the personal data to be transferred?	NAVEX Global employs encryption at rest using either full-disk encryption or within the database using TDE. Data at rest will be encrypted using AES 256 or better, data in flight will be accomplished using TLS 1.2 or higher on public untrusted networks. When access is provided to NAVEX Global personnel in the U.S. for the purposes described in this TRA, customer data must be accessible in the clear to provide the requisite support or service function.
12.	What is the storage location of the data transferred?	The European Union.
13.	What are the sub-processing activities?	Please see details here: https://www.navexglobal.com/en-us/service-hosting-providers. Outside of affiliate access in scope of this TRA, there are no transfers outside the EU/UK via sub-sub-processors.
Importer's exposure to government surveillance and practical application of Section 702 FISA		
14.	Is the data importer's sector or business directly subject to such laws in its jurisdiction that permit government access to personal data, or require the assistance of data importer to disclose personal data to public authorities, for surveillance and intelligence gathering purposes?	No. In our reasonable opinion upon internal and outside counsel review, we do not find NAVEX Global to be directly subject to such laws. As a practical matter based on the nature of NAVEX Global's services, the types of personal data processed, and the absence of any prior requests received in the past, NAVEX Global believes it is extremely unlikely to receive requests from U.S. government agencies to obtain customer data for national security purposes or to participate in the types of U.S. bulk surveillance programs scrutinized by the

#	Factor	Response
		CJEU in its recent ruling on data transfer mechanisms.
	a. Specifically, what is data importer's analysis regarding Section 702 FISA under the SCCs and EDPB Guidance?	1) Data exporters may decide to proceed with the transfer without supplementary measures, if they consider there to be no reason to believe that the relevant and problematic legislation (those in the U.S. in this instance) will be applied, in practice, to the transferred data and/or NAVEX Global. a. In our reasonable opinion upon internal and outside counsel review, we do not find U.S. surveillance laws, including Section 702 FISA, to practically apply to these transfers. b. It is important to note that given the broad definitions of these laws, the vast majority of organizations are going to have to acknowledge their potential application. However, this does not mean they directly apply or practically apply in practice. c. We believe NAVEX Global is generally out of scope and that these laws are overall not going to apply to the services we provide, as the intent is for surveillance of certain telecom and internet service providers for targeted information. This typically involves to surveillance of real time emails, texts, and chat conversations. The foregoing is not what NAVEX Global provides and in order to obtain this sought for information, authorities would pursue those providers directly as it would be impractical to make a request through NAVEX Global. 2) Data exporters may also take into consideration documented practical experience of data importer with relevant prior instances of requests for access received from public authorities in the U.S. e. ***To this point, NAVEX Global has never received a Section 702 FISA request or an EO 12.333 request or order. Please see our Public Authority Disclosure Request Policy for more details.** * f. The EDPB Guidance implies that the lack of requests received in the past plus no prohibition on providing information about such requests, could be sufficient to conclude Section 702 FISA does not apply in

#	Factor	Response
		practice. Note there is no prohibition on NAVEX Global to provide information about these requests. 3) If you conclude Section 702 FISA does not apply in practice to the particular transfer, it is possible to proceed with the transfer without any supplementary measures. **a. While NAVEX Global takes the approach that Section 702 FISA does not apply in practice, we still have elected to provide for supplementary measures with regard to these transfers. Please see Section IV (D).**
15.	Within the last three (3) years, has the data importer received requests/demands from public authorities in its jurisdiction to disclose EU personal data pursuant to the SCCs?	No, not to the best of our knowledge.
	a. Approximately how many requests/demands from public authorities has the data importer received in that time period concerning EU personal data pursuant to the SCCs?	None, to the best of our knowledge.
	b. Approximately how many of these requests/demands are pursuant to criminal law procedure in the destination country? *[Regular court proceedings are not the issue under Schrems II, but intelligence programs are scrutinized.]*	While NAVEX Global has not received a Section 702 FISA request, an EO 12.333 request or order, or a public authority request specifically targeting EU personal data under the SCCs, we have received a limited number of formal requests or demands from U.S. government authorities concerning customer data. These requests have been made in the context of criminal and civil actions in the form of a subpoena issued to NAVEX Global as a third party, by a state or federal court. In each instance, we've notified the customer straight away and they have directed us to comply with the subpoena. We've only fulfilled such requests with full customer clearance and direction on how to handle.
	c. Approximately how many of these requests/demands are pursuant to national security or intelligence agencies in the destination country?	None, to the best of our knowledge. The data importer can represent that it has not received requests/demands from intelligence agencies. NAVEX Global offers signed contracts, warranting it has not received such requests, via either a data processing addendum or amendment to data processing addendum.
	d. Has the data importer been able to contest/minimize such disclosure of EU personal data, where appropriate?	Not applicable
	e. What types of EU personal data has the data importer been required to disclose to public authorities in its jurisdiction?	Not applicable
16.	How likely is it that the data importer will	

#	Factor	Response
	receive bulk data surveillance requests to disclose EU personal data to public authorities in its jurisdiction in the future (e.g., based on factors such as the type of services provided and sector in which the data importer operates, its size, number of customers and reputation)?	Unlikely. As a practical matter based on the nature of NAVEX Global's services, the types of personal data processed, and the absence of any prior requests received in the past, NAVEX Global believes it is extremely unlikely to receive requests from U.S. government agencies to obtain customer data for national security purposes or to participate in the types of U.S. bulk surveillance programs scrutinized by the CJEU in its recent ruling on data transfer mechanisms. We have no reason to believe we may receive such requests in the future.
17.	Does the data importer maintain annual reports or statistics regarding requests/demands received from law enforcement or intelligence agencies (e.g., number/type of requests/demands, requesting authority, etc.)?	Not applicable. NAVEX Global has not received a Section 702 FISA request, an EO 12.333 request or order, or a public authority request specifically targeting EU personal data under the SCCs. As a result, if we get such requests in the future, we will provide such statistics and update our TRA process and Public Authority Disclosure Policy accordingly.
18.	Does the data importer maintain a written procedure(s) for: 1. Responding to or challenging requests/ demands of law enforcement or intelligence agencies that apply to EU personal data? 2. Informing customers of requests/demands from law enforcement or intelligence agencies where permitted by applicable law?	Yes, please see our Public Authority Disclosure Request Policy.
19.	Are the data importer's commitments enabling data subjects to exercise their rights as provided in the SCCs thwarted by the laws and/or practices in the U.S. or can these rights be effectively applied in practice?	NAVEX Global has never encountered a situation where it felt it could not enable data subject rights, including judicial redress. We do not believe the laws subject to us prevent us from enabling, supporting, and fulfilling data subject rights under the SCCs.
Onward transfers and exposure to government surveillance		
20.	Does the data importer share EU personal data further with sub-processors whose processing takes place in third countries?	Yes. Only to its US affiliate.
21.	What measures does the third-party data recipient take to ensure the protection of EU personal data transferred to it?	NAVEX Global enters into written agreements with sub-processors that include safeguards for EU personal data in accordance with the GDPR requirements.
22.	What assurances has the data importer received from third-party data recipients with respect to requests/demands for EU personal data from [U.S./other jurisdiction] public	NAVEX Global has updated all written agreements with sub-processors to include additional measures for the protection of EU

#	Factor	Response
	authorities?	personal data, where required.

Conclusion/Risk of transfers

Likely limited-risk data transfer

In particular, NAVEX Global identified the following factors (based on the assessment documented above and any additional information), that are likely to indicate a limited-risk transfer:

The data importer has never received requests/demands from intelligence services for disclosure of EU personal data.

The data importer has received limited requests/demands from public authorities for disclosure of EU personal data (such as for disclosure of employee data), but the requests related to regular criminal law procedure and did not go beyond what is necessary and proportionate to meet the purpose of the request.

The data importer has a process in place for handling and contesting public authority access requests, if received.

Based on the nature of its services and data processing activities, the data importer does not expect to be the target of requests/demands pursuant to national security or intelligence agencies for disclosure of EU personal data.

Such data transfers are not directly nor practically in scope of requests/demands from national security or intelligence agencies for disclosure of EU personal data.

D. Supplementary Measures

Notwithstanding the Conclusion set forth in the above TRA, NAVEX Global has also adopted the following supplemental measures. We believe that by implementing such supplemental measures, we are following best practices and are demonstrating our serious commitment to the protection of customer data.

Contractual safeguards	The SCCs themselves contain a number of contractual commitments by NAVEX Global and its customer, aimed at serving as safeguards for EU personal data.
	Supplementary contractual assurances are offered via our standard data processing addendum or an amendment to the data processing addendum. Please reach out to privacy@navexglobal.com in order to get this in place.
	NAVEX Global agrees to audit and monitor its obligations, and to support its customers auditing and monitoring obligations, regarding the level of government access to data.

	NAVEX Global provides a data processing agreement to support GDPR compliance, which includes the SCCs. As the data processor/importer, we process personal data strictly in accordance with your instructions and to provide the services. Our customers are the owners of the personal data within our service applications. NAVEX Global offers a Data Security Addendum, providing for contractual commitments to its information security program.
Organizational safeguards	NAVEX Global maintains written processes and procedures which provide for review of and limit the scope of EU personal data disclosed by NAVEX Global in response to requests from public authorities. Please see our Public Authority Disclosure Request Policy.
	NAVEX Global maintains internal record of requests made by public authorities concerning EU personal data.
	NAVEX Global takes steps to limit the volume of disclosed data, where possible.
	NAVEX Global would take data minimization measures such as redacting unnecessary identifiable personal data or personal data that may be of increased interest to intelligence agencies before complying with a request to disclosure EU personal data.
	NAVEX Global has developed the attached Standard Contractual Clauses Assurance Guide, which details our commitment to compliance with the SCCs. NAVEX Global remains a participant and has certified its compliance with the EU-U.S. Privacy Shield Framework and the Swiss- U.S. Privacy Shield Framework. NAVEX Global, Inc. is committed to subjecting all personal information received from the European Economic Area, United Kingdom, and Switzerland, respectively, in reliance on each Privacy Shield Framework, to the Frameworks' applicable Principles. To learn more about the Privacy Shield program, and to view our certification, please visit https://www.privacyshield.gov. NAVEX Global provides an independent recourse mechanism to EU individuals, currently TrustArc.
Technical safeguards	Encrypt personal data in transit.

	Encrypt personal data at rest.
	Appropriate access controls.
	Customers can implement data minimization (e.g., store the least amount of data necessary).
	Timespan for any access to personal data “in the clear” is limited to the specific function.
	Store personal data in the EU and enable only remote access.
	NAVEX Global equips its services with self-servicing functionality, allowing you to manage the personal data on your own through the use of the services. NAVEX Global engages a recognized, independent third party to conduct a Statement on Standards for Attestation Engagements No. 16, Service Organization Control 2, Type 2 (“SSAE 18 SOC 2 Type 2”) audit (or its equivalent or successor) of its information security program and its administrative, technical, and physical safeguards for all facilities used to deliver the Services, which specifically includes privacy controls. NAVEX Global maintains an annual Standardized Information Gathering Questionnaire (“SIG”), which details our robust security program with supporting documentation.

Conclusion

Having regard to the level of risk of the data transfer (**limited risk**), NAVEX Global considers that the measures identified above are **sufficient and effective** in light of the circumstances of the transfers, in conjunction with the supplementary measures and safeguards provided by the SCCs, to allow the data importer to comply with its obligations under the SCCs and provide an appropriate level of protection for the transfer.

NAVEXEngage: EU Hosted

EU HOSTED NAVEXENGAGE - EU/UK DATA TRANSFER RISK ASSESSMENTS

I. INTRODUCTION

NAVEX Global must conduct Transfer Risk Assessments ("TRA" or "TRAs") for transfers of personal data from the European Economic Area ("EEA")[3] or the United Kingdom ("UK") (collectively "EU personal data") to third countries that are not deemed to provide an adequate level of data protection.

II. SCOPE

These TRAs apply to NAVEX Global's EU Hosted NAVEXEngage customers.

This TRA process applies to personal data transferred to NAVEX Global pursuant to the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council. This TRA is specifically designed to address Clause 14 of the foregoing set of Standard Contractual Clauses. Personal data from the UK is also in scope and shall be assessed pursuant to the European Commission's decision (C(2010)593) of 5 February 2010 on Standard Contractual Clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection. We collectively refer to the sets of Standard Contractual Clauses as the "SCCs." NAVEX Global agrees and acknowledges the UK will be issuing its own set of standard contractual clauses and related Schrems II guidance. We will update this TRA on an ongoing basis as needed.

This TRA process takes into account the European Data Protection Board's Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data adopted on 18 June 2021 (the "EDPB Guidance").

This TRA is not intended for transfers (i) within the EEA, (ii) between the EEA and the UK, or (iii) from the EEA or UK to a country recognized by the European Commission or UK law as adequate at this time (i.e., Andorra, Argentina, Canada (commercial organizations subject to PIPEDA), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, UK, and Uruguay).

The TRA is completed by the NAVEX Global Privacy Team, which consists of the Data Privacy Officer & Senior Counsel, Deputy Data Privacy Officer & Senior Counsel, and Privacy Counsel.

III. ASSESSING THE ADEQUACY OF EU/UK DATA TRANSFERS – TO NAVEX GLOBAL IN THE U.S.

In assessing the adequacy of transfers of personal data from the EU/UK to NAVEX Global in the U.S. we have taken the following steps:

1. **STEP 1:** Identified the relevant data transfers and the legal mechanism that NAVEX Global is relying on for such transfers (e.g., SCCs).

2. **STEP 2:** Conducted due diligence and collected information about the scope of the transfers, the exposure of NAVEX Global to local law that may require disclosure of EU personal data about individuals, and any other relevant information.

3. **STEP 3:** Completed the "Transfer Risk Assessment" in **Section IV** to assess whether the SCCs is effective in light of all circumstances of the transfer.

4. **STEP 4:** Included additional "Supplementary Measures" as set forth in **Section IV (D)**.

[3] The European Economic Area consists of the Member States of the EU (Austria, Belgium, Bulgaria, Croatia, Cyprus, Czechia, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain and Sweden), plus Iceland, Liechtenstein and Norway.

5. **STEP 5:** Documented the assessment for accountability purposes. We encourage our customers to do the same.

6. **STEP 6:** NAVEX Global is responsible for the periodic review of the assessment, which should take place at least annually, to ensure that the transfer of the EU personal data continues to be afforded an adequate level of protection.

IV. TRANSFER RISK ASSESSMENT

Name Of Data Importer: NAVEX Global
Scope of TRA: Transfers to NAVEX Global's affiliates in the United States as part of the NAVEXEngage services provided to EU Hosted Customers
Completed By: NAVEX Global's Privacy Team
Date: 25 September 2021

A. Type of Data Importer

Name of data importer: NAVEX Global. The SCCs between customer and NAVEX Global is part of a master services agreement between customer and NAVEX Global UK Limited (registered in the UK) or GCS Compliance Services Europe Unlimited Company trading as NAVEX Global (registered in Ireland), both with their principal places of business at Vantage West – 4th floor, Great West Road, Brentford TW8 9AG, United Kingdom. Some EU Hosted customers elect to contract directly with our U.S. entity, NAVEX Global, Inc., a Delaware corporation with its principal place of business at 5500 Meadows Road, Suite 500, Lake Oswego, OR 97035.

Upon reviewing the broad definitions set forth within U.S. surveillance laws under scrutiny pursuant to the CJEU ruling in the Schrems II case, NAVEX Global identifies itself as follows:

NAVEX Global does not consider itself a "telecommunications carrier" as defined in 47 U.S.C. 152.

NAVEX Global acknowledges that certain of its services could be viewed by U.S. government authorities as an "electronic communication service" as defined in 18 U.S.C. 2510.

NAVEX Global acknowledges that certain of its services could be viewed by U.S. government authorities as a "remote computing service" as defined in 18 U.S.C. 2711.

NAVEX Global acknowledges that certain of its services could be viewed by U.S. government authorities as other communication services where there may be access to wire or electronic communications.

B. Details of Data Transfers

Data transfer mechanism Appropriate Controller to Processor SCCs between customer and NAVEX Global.
Scope of personal data covered by the data transfer mechanism in place The SCCs cover transfers of EU personal data from the EEA/UK to the U.S., including the following categories of data subjects: • Employees of data exporter • Clients, business partners and vendors of data exporter (who are natural persons) • Employees or contact persons of data exporters' third-party suppliers, business partners and vendors

- Data exporter's users authorized by data exporter to use the relevant Service(s)

C. Transfer Risk Assessment

The table below aids identification and evaluation of risk factors in relation to the specific data transfer. The assessment of each risk factor is recorded in appropriate detail.

#	Factor	Response
Scope of the transfers		
1.	What is the type of transfer?	Remote access only by direct NAVEX Global personnel located in the U.S. to personal data stored in the EU. Personal data is not stored in the U.S. as part of this transfer.
2.	Is the transfer necessary?	Yes. NAVEX Global has critical resources located in the U.S., requiring access to the EU hosted database for the following purposes: • Support. General support cases that are submitted, depending on the case, may require access to customer data to address the issue at hand. To meet our service level commitments, U.S. support may be involved accordingly. This is mainly due to certain resource limitations based on location, an overflow of support cases, and time zone challenges. • Administrative Service Functions. There is certain work, for example setting up the landing page, that does not necessarily require a deep level access, but for which can result in a transfer of personal data to the U.S. depending on the service need. • Technical Work. Many of our technical resources are in the U.S. which requires access to customer data. Examples include certain data extract services, certain data migration services, integration services, user setups instances, and hosting installations. again, depending on the task, we need the option to leverage those resources which involves a certain level of access. • IT/Hosting. Select members of the hosting and information security group must have access for maintenance and

#	Factor	Response
		troubleshooting. Without the above, our service level commitments would greatly suffer, and the overall maintenance and security of our service would be put at great risk.
3.	Is the transfer proportionate?	Yes. Access is not provided to personnel in the U.S. in a general sense. Access is provided to those personnel in the U.S. on a strict need to know basis to perform their given job function.
4.	Is the transfer occasional/non-routine or frequent/routine?	The transfer is non-routine to NAVEX Global personnel in the U.S. for the purposes detailed in Factor #2 above.
5.	Will the transferred personal data be processed for a relatively long or short period of time?	Personal data transferred to the U.S. in this context is processed for a relatively short period of time to provide the applicable service support.
6.	Is the transferred data encrypted and/ or pseudonymized?	Yes. NAVEX Global employs encryption at rest using either full-disk encryption or within the database using TDE. Data at rest will be encrypted using AES 256 or better, data in flight will be accomplished using TLS 1.2 or higher on public untrusted networks. Upon reviewing pseudonymization in the context of this transfer, it is inapplicable to the services we need to support.
Specific circumstances of the transfer		
7.	What are the purposes for which the data are transferred and processed?	To provide the best support, maintenance, and services as committed to in our agreements with our customers.
8.	What are the types of entities involved in the processing?	NAVEX Global is a data processor and a private company. Our customers are the data controllers and may consist of both private and public companies.
9.	In which sector does the transfer occur?	NAVEX Global provides risk and compliance management SaaS based software. ***This factor is especially important as the**

#	Factor	Response
		purposes of our services is to enable organizations support their risk, ethics, and compliance programs. *
10.	What are the categories of personal data transferred?	• Name (first and last), email address, job site, job title, department, supervisor, log-in credentials, completion status, time and date of training media. ****No sensitive data, as defined under the GDPR, is transferred as part of the NAVEXEngage services.****
11.	What is the format of the personal data to be transferred?	NAVEX Global employs encryption at rest using either full-disk encryption or within the database using TDE. Data at rest will be encrypted using AES 256 or better, data in flight will be accomplished using TLS 1.2 or higher on public untrusted networks. When access is provided to NAVEX Global personnel in the U.S. for the purposes described in this TRA, customer data must be accessible in the clear to provide the requisite support or service function.
12.	What is the storage location of the data transferred?	The European Union.
13.	What are the sub-processing activities?	Please see details here: https://www.navexglobal.com/en-us/service-hosting-providers. Outside of affiliate access in scope of this TRA, there are no transfers outside the EU/UK via sub-sub-processors.
Importer's exposure to government surveillance and practical application of Section 702 FISA		
14.	Is the data importer's sector or business directly subject to such laws in its jurisdiction that permit government access to personal data, or require the assistance of data importer to disclose personal data to public authorities, for surveillance and intelligence gathering purposes?	No. In our reasonable opinion upon internal and outside counsel review, we do not find NAVEX Global to be directly subject to such laws. As a practical matter based on the nature of NAVEX Global's services, the types of personal data processed, and the absence of any prior requests received in the past, NAVEX Global believes it is extremely unlikely to receive requests from U.S. government agencies to obtain customer data for national security purposes or to participate in the types of U.S. bulk surveillance programs scrutinized by the CJEU in its recent ruling on data transfer mechanisms.

#	Factor	Response
	a. Specifically, what is data importer's analysis regarding Section 702 FISA under the SCCs and EDPB Guidance?	1) Data exporters may decide to proceed with the transfer without supplementary measures, if they consider there to be no reason to believe that the relevant and problematic legislation (those in the U.S. in this instance) will be applied, in practice, to the transferred data and/or NAVEX Global. a. In our reasonable opinion upon internal and outside counsel review, we do not find U.S. surveillance laws, including Section 702 FISA, to practically apply to these transfers. b. It is important to note that given the broad definitions of these laws, the vast majority of organizations are going to have to acknowledge their potential application. However, this does not mean they directly apply or practically apply in practice. c. We believe NAVEX Global is generally out of scope and that these laws are overall not going to apply to the services we provide, as the intent is for surveillance of certain telecom and internet service providers for targeted information. This typically involves to surveillance of real time emails, texts, and chat conversations. The foregoing is not what NAVEX Global provides and in order to obtain this sought for information, authorities would pursue those providers directly as it would be impractical to make a request through NAVEX Global. 2) Data exporters may also take into consideration documented practical experience of data importer with relevant prior instances of requests for access received from public authorities in the U.S. g. ***To this point, NAVEX Global has never received a Section 702 FISA request or an EO 12.333 request or order. Please see our Public Authority Disclosure Request Policy for more details.** * h. The EDPB Guidance implies that the lack of requests received in the past plus no prohibition on providing information about such requests, could be sufficient to conclude Section 702 FISA does not apply in practice. Note there is no prohibition on NAVEX Global to provide information about these requests.

#	Factor	Response
		3) If you conclude Section 702 FISA does not apply in practice to the particular transfer, it is possible to proceed with the transfer without any supplementary measures. **a. While NAVEX Global takes the approach that Section 702 FISA does not apply in practice, we still have elected to provide for supplementary measures with regard to these transfers. Please see Section IV (D).**
15.	Within the last three (3) years, has the data importer received requests/demands from public authorities in its jurisdiction to disclose EU personal data pursuant to the SCCs?	No, not to the best of our knowledge.
	a. Approximately how many requests/demands from public authorities has the data importer received in that time period concerning EU personal data pursuant to the SCCs?	None, to the best of our knowledge.
	b. Approximately how many of these requests/demands are pursuant to criminal law procedure in the destination country? *[Regular court proceedings are not the issue under Schrems II, but intelligence programs are scrutinized.]*	While NAVEX Global has not received a Section 702 FISA request, an EO 12.333 request or order, or a public authority request specifically targeting EU personal data under the SCCs, we have received a limited number of formal requests or demands from U.S. government authorities concerning customer data. These requests have been made in the context of criminal and civil actions in the form of a subpoena issued to NAVEX Global as a third party, by a state or federal court. In each instance, we've notified the customer straight away and they have directed us to comply with the subpoena. We've only fulfilled such requests with full customer clearance and direction on how to handle.
	c. Approximately how many of these requests/demands are pursuant to national security or intelligence agencies in the destination country?	None, to the best of our knowledge. The data importer can represent that it has not received requests/demands from intelligence agencies. NAVEX Global offers signed contracts, warranting it has not received such requests, via either a data processing addendum or amendment to data processing addendum.
	d. Has the data importer been able to contest/minimize such disclosure of EU personal data, where appropriate?	Not applicable
	e. What types of EU personal data has the data importer been required to disclose to public authorities in its jurisdiction?	Not applicable
16.	How likely is it that the data importer will receive bulk data surveillance requests to disclose EU personal data to public authorities in its jurisdiction in the future (e.g.,	Unlikely. As a practical matter based on the nature of NAVEX Global's services, the types of personal data processed, and the absence of

#	Factor	Response
	based on factors such as the type of services provided and sector in which the data importer operates, its size, number of customers and reputation)?	any prior requests received in the past, NAVEX Global believes it is extremely unlikely to receive requests from U.S. government agencies to obtain customer data for national security purposes or to participate in the types of U.S. bulk surveillance programs scrutinized by the CJEU in its recent ruling on data transfer mechanisms. We have no reason to believe we may receive such requests in the future.
17.	Does the data importer maintain annual reports or statistics regarding requests/demands received from law enforcement or intelligence agencies (e.g., number/type of requests/demands, requesting authority, etc.)?	Not applicable. NAVEX Global has not received a Section 702 FISA request, an EO 12.333 request or order, or a public authority request specifically targeting EU personal data under the SCCs. As a result, if we get such requests in the future, we will provide such statistics and update our TRA process and Public Authority Disclosure Policy accordingly.
18.	Does the data importer maintain a written procedure(s) for: 1. Responding to or challenging requests/ demands of law enforcement or intelligence agencies that apply to EU personal data? 3. Informing customers of requests/demands from law enforcement or intelligence agencies where permitted by applicable law?	Yes, please see our Public Authority Disclosure Request Policy.
19.	Are the data importer's commitments enabling data subjects to exercise their rights as provided in the SCCs thwarted by the laws and/or practices in the U.S. or can these rights be effectively applied in practice?	NAVEX Global has never encountered a situation where it felt it could not enable data subject rights, including judicial redress. We do not believe the laws subject to us prevent us from enabling, supporting, and fulfilling data subject rights under the SCCs.
Onward transfers and exposure to government surveillance		
20.	Does the data importer share EU personal data further with sub-processors whose processing takes place in third countries?	Yes. Only to its US affiliate.
21.	What measures does the third-party data recipient take to ensure the protection of EU personal data transferred to it?	NAVEX Global enters into written agreements with sub-processors that include safeguards for EU personal data in accordance with the GDPR requirements.
22.	What assurances has the data importer received from third-party data recipients with respect to requests/demands for EU personal data from [U.S./other jurisdiction] public authorities?	NAVEX Global has updated all written agreements with sub-processors to include additional measures for the protection of EU personal data, where required.

#	Factor	Response
	Conclusion/Risk of transfers **Likely limited-risk data transfer** **In particular, NAVEX Global identified the following factors (based on the assessment documented above and any additional information), that are likely to indicate a limited-risk transfer:** The data importer has never received requests/demands from intelligence services for disclosure of EU personal data. The data importer has received limited requests/demands from public authorities for disclosure of EU personal data (such as for disclosure of employee data), but the requests related to regular criminal law procedure and did not go beyond what is necessary and proportionate to meet the purpose of the request. The data importer has a process in place for handling and contesting public authority access requests, if received. Based on the nature of its services and data processing activities, the data importer does not expect to be the target of requests/demands pursuant to national security or intelligence agencies for disclosure of EU personal data. Such data transfers are not directly nor practically in scope of requests/demands from national security or intelligence agencies for disclosure of EU personal data.	

D. Supplementary Measures

Notwithstanding the Conclusion set forth in the above TRA, NAVEX Global has also adopted the following supplemental measures. We believe that by implementing such supplemental measures, we are following best practices and are demonstrating our serious commitment to the protection of customer data.

Contractual safeguards	The SCCs themselves contain a number of contractual commitments by NAVEX Global and its customer, aimed at serving as safeguards for EU personal data.
	Supplementary contractual assurances are offered via our standard data processing addendum or an amendment to the data processing addendum. Please reach out to privacy@navexglobal.com in order to get this in place.
	NAVEX Global agrees to audit and monitor its obligations, and to support its customers auditing and monitoring obligations, regarding the level of government access to data.
	NAVEX Global provides a data processing agreement to support

	GDPR compliance, which includes the SCCs. As the data processor/importer, we process personal data strictly in accordance with your instructions and to provide the services. Our customers are the owners of the personal data within our service applications. NAVEX Global offers a Data Security Addendum, providing for contractual commitments to its information security program.
Organizational safeguards	NAVEX Global maintains written processes and procedures which provide for review of and limit the scope of EU personal data disclosed by NAVEX Global in response to requests from public authorities. Please see our Public Authority Disclosure Request Policy.
	NAVEX Global maintains internal record of requests made by public authorities concerning EU personal data.
	NAVEX Global takes steps to limit the volume of disclosed data, where possible.
	NAVEX Global would take data minimization measures such as redacting unnecessary identifiable personal data or personal data that may be of increased interest to intelligence agencies before complying with a request to disclosure EU personal data.
	NAVEX Global has developed the attached Standard Contractual Clauses Assurance Guide, which details our commitment to compliance with the SCCs. NAVEX Global remains a participant and has certified its compliance with the EU-U.S. Privacy Shield Framework and the Swiss- U.S. Privacy Shield Framework. NAVEX Global, Inc. is committed to subjecting all personal information received from the European Economic Area, United Kingdom, and Switzerland, respectively, in reliance on each Privacy Shield Framework, to the Frameworks' applicable Principles. To learn more about the Privacy Shield program, and to view our certification, please visit https://www.privacyshield.gov. NAVEX Global provides an independent recourse mechanism to EU individuals, currently TrustArc.
Technical safeguards	Encrypt personal data in transit.
	Encrypt personal data at rest.

	Appropriate access controls.
	Customers can implement data minimization (e.g., store the least amount of data necessary).
	Timespan for any access to personal data “in the clear” is limited to the specific function.
	Store personal data in the EU and enable only remote access.
	NAVEX Global equips its services with self-servicing functionality, allowing you to manage the personal data on your own through the use of the services. NAVEX Global engages a recognized, independent third party to conduct a Statement on Standards for Attestation Engagements No. 16, Service Organization Control 2, Type 2 (“SSAE 18 SOC 2 Type 2”) audit (or its equivalent or successor) of its information security program and its administrative, technical, and physical safeguards for all facilities used to deliver the Services, which specifically includes privacy controls. NAVEX Global maintains an annual Standardized Information Gathering Questionnaire (“SIG”), which details our robust security program with supporting documentation.

Conclusion

Having regard to the level of risk of the data transfer (**limited risk**), NAVEX Global considers that the measures identified above are **sufficient and effective** in light of the circumstances of the transfers, in conjunction with the supplementary measures and safeguards provided by the SCCs, to allow the data importer to comply with its obligations under the SCCs and provide an appropriate level of protection for the transfer.

RiskRate: EU Hosted

NAVEX GLOBAL

EU HOSTED RISKRATE- EU/UK DATA TRANSFER RISK ASSESSMENTS

I. INTRODUCTION

NAVEX Global must conduct Transfer Risk Assessments ("TRA" or "TRAs") for transfers of personal data from the European Economic Area ("EEA")[4] or the United Kingdom ("UK") (collectively "EU personal data") to third countries that are not deemed to provide an adequate level of data protection.

II. SCOPE

These TRAs apply to NAVEX Global's EU Hosted RiskRate customers.

This TRA process applies to personal data transferred to NAVEX Global pursuant to the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council. This TRA is specifically designed to address Clause 14 of the foregoing set of Standard Contractual Clauses. Personal data from the UK is also in scope and shall be assessed pursuant to the European Commission's decision (C(2010)593) of 5 February 2010 on Standard Contractual Clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection. We collectively refer to the sets of Standard Contractual Clauses as the "SCCs." NAVEX Global agrees and acknowledges the UK will be issuing its own set of standard contractual clauses and related Schrems II guidance. We will update this TRA on an ongoing basis as needed.

This TRA process takes into account the European Data Protection Board's Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data adopted on 18 June 2021 (the "EDPB Guidance").

NAVEX Global has separate TRAs for its non-affiliate sub-processing activities, where NAVEX Global utilizes such sub-processors for the processing of personal data who receive customer EU personal data in third countries that have not been deemed adequate by the European Commission. These are available as part of our compliance documentation and on request.

This TRA is not intended for transfers (i) within the EEA, (ii) between the EEA and the UK, or (iii) from the EEA or UK to a country recognized by the European Commission or UK law as adequate at this time (i.e., Andorra, Argentina, Canada (commercial organizations subject to PIPEDA), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, UK, and Uruguay).

The TRA is completed by the NAVEX Global Privacy Team, which consists of the Data Privacy Officer & Senior Counsel, Senior Privacy Counsel, and Privacy Counsel.

III. ASSESSING THE ADEQUACY OF EU/UK DATA TRANSFERS – TO NAVEX GLOBAL IN THE U.S.

In assessing the adequacy of transfers of personal data from the EU/UK to NAVEX Global in the U.S. we have taken the following steps:

1. **STEP 1:** Identified the relevant data transfers and the legal mechanism that NAVEX Global is relying on for such transfers (e.g., SCCs).

[4] The European Economic Area consists of the Member States of the EU (Austria, Belgium, Bulgaria, Croatia, Cyprus, Czechia, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain and Sweden), plus Iceland, Liechtenstein and Norway.

2. **STEP 2:** Conducted due diligence and collected information about the scope of the transfers, the exposure of NAVEX Global to local law that may require disclosure of EU personal data about individuals, and any other relevant information.

3. **STEP 3:** Completed the "Transfer Risk Assessment" in **Section IV** to assess whether the SCCs is effective in light of all circumstances of the transfer.

4. **STEP 4:** Included additional "Supplementary Measures" as set forth in **Section IV (D)**.

5. **STEP 5:** Documented the assessment for accountability purposes. We encourage our customers to do the same.

6. **STEP 6:** NAVEX Global is responsible for the periodic review of the assessment, which should take place at least annually, to ensure that the transfer of the EU personal data continues to be afforded an adequate level of protection.

IV. TRANSFER RISK ASSESSMENT

Name Of Data Importer: NAVEX Global

Scope of TRA: Transfers to NAVEX Global's affiliates in the United States as part of the RiskRate Services provided to EU Hosted Customers

Completed By: NAVEX Global's Privacy Team

Date: 25 September 2021

A. Type of Data Importer

Name of data importer: NAVEX Global. The SCCs between customer and NAVEX Global is part of a master services agreement between customer and NAVEX Global UK Limited (registered in the UK) or GCS Compliance Services Europe Unlimited Company trading as NAVEX Global (registered in Ireland), both with their principal places of business at Vantage West – 4th floor, Great West Road, Brentford TW8 9AG, United Kingdom. Some EU Hosted customers elect to contract directly with our U.S. entity, NAVEX Global, Inc., a Delaware corporation with its principal place of business at 5500 Meadows Road, Suite 500, Lake Oswego, OR 97035.

Upon reviewing the broad definitions set forth within U.S. surveillance laws under scrutiny pursuant to the CJEU ruling in the Schrems II case, NAVEX Global identifies itself as follows:

NAVEX Global does not consider itself a "telecommunications carrier" as defined in 47 U.S.C. 152.

NAVEX Global acknowledges that certain of its services could be viewed by U.S. government authorities as an "electronic communication service" as defined in 18 U.S.C. 2510.

NAVEX Global acknowledges that certain of its services could be viewed by U.S. government authorities as a "remote computing service" as defined in 18 U.S.C. 2711.

NAVEX Global acknowledges that certain of its services could be viewed by U.S. government authorities as other communication services where there may be access to wire or electronic communications.

B. Details of Data Transfers

Data transfer mechanism Appropriate Controller to Processor SCCs between customer and NAVEX Global.
Scope of personal data covered by the data transfer mechanism in place The SCCs cover transfers of EU personal data from the EEA/UK to the U.S., including the following categories of data subjects: • Employees of data exporter • Clients, business partners and vendors of data exporter (who are natural persons) • Employees or contact persons of data exporters' third-party suppliers, business partners and vendors • Data exporter's users authorized by data exporter to use the relevant Service(s)

C. Transfer Risk Assessment

The table below aids identification and evaluation of risk factors in relation to the specific data transfer. The assessment of each risk factor is recorded in appropriate detail.

#	Factor	Response
Scope of the transfers		
1.	What is the type of transfer?	Remote access only by direct NAVEX Global personnel located in the U.S. to personal data stored in the EU. Personal data is not stored in the U.S. as part of this transfer.
2.	Is the transfer necessary?	Yes. NAVEX Global has critical resources located in the U.S., requiring access to the EU hosted database for the following purposes: • Support. General support cases that are submitted, depending on the case, may require access to customer data to address the issue at hand. To meet our service level commitments, U.S. support may be involved accordingly. This is mainly due to certain resource limitations based on location, an overflow of support cases, and time zone challenges. • Administrative Service Functions. There is certain work, for example setting up the RiskRate web pages, that does not necessarily require a deep level access, but for which can result in a transfer of personal data to the U.S. depending on the service need. • Technical Work and Product Management. Many of our technical and product specific resources are in the U.S. which requires access to customer data. Examples include certain data extract services, implementation and professional services, certain data migration services, integration services, user setups instances, and hosting installations. Again, depending on the task, we need the option to leverage

#	Factor	Response
		those resources which involves a certain level of access. • IT/Hosting. Select members of the hosting and information security group must have access for maintenance and troubleshooting. Without the above, our service level commitments would greatly suffer, and the overall maintenance and security of our service would be put at great risk.
3.	Is the transfer proportionate?	Yes. Access is not provided to personnel in the U.S. in a general sense. Access is provided to those personnel in the U.S. on a strict need to know basis to perform their given job function.
4.	Is the transfer occasional/non-routine or frequent/routine?	The transfer is non-routine to NAVEX Global personnel in the U.S. for the purposes detailed in Factor #2 above.
5.	Will the transferred personal data be processed for a relatively long or short period of time?	Personal data transferred to the U.S. in this context is processed for a relatively short period of time to provide the applicable service support.
6.	Is the transferred data encrypted and/ or pseudonymized?	Yes. NAVEX Global employs encryption at rest using either full-disk encryption or within the database using TDE. Data at rest will be encrypted using AES 256 or better, data in flight will be accomplished using TLS 1.2 or higher on public untrusted networks. Upon reviewing pseudonymization in the context of this transfer, it is inapplicable to the services we need to support.
Specific circumstances of the transfer		
7.	What are the purposes for which the data are transferred and processed?	To provide the best support, maintenance, and services as committed to in our agreements with our customers.
8.	What are the types of entities involved in the processing?	NAVEX Global is a data processor and a private company. Our customers are the data controllers and may consist of both private and public companies.

#	Factor	Response
9.	In which sector does the transfer occur?	NAVEX Global provides risk and compliance management SaaS based software. ***This factor is especially important as the purposes of our services is to enable organizations support their risk, ethics, and compliance programs.*** * Many of our customers are required by law to conduct appropriate due diligence on third parties. As such, our customers request certain data to be screened and provided back to them, to allow them to conduct this due diligence.
10.	What are the categories of personal data transferred?	Generally, the RiskRate services implicate the following categories of personal data, as requested by the customer to perform the screening: • name, job title, job position, location, employer, relationship with the organization, e-mail address, telephone number, address, date of birth, manager, director, officer and affiliated or organization information Depending on the scope of the customer request, additional categories of personal data may be sent back to the customer for processing as part of their due diligence: • nationality, shareholder ID #, percentage of ownership, picture, ID # (passport, social security number, or national ID) ***No sensitive data, as defined under the GDPR, is transferred from data exporter to the RiskRate services. ***
11.	What is the format of the personal data to be transferred?	NAVEX Global employs encryption at rest using either full-disk encryption or within the database using TDE. Data at rest will be encrypted using AES 256 or better, data in flight will be accomplished using TLS 1.2 or higher on public untrusted networks. When access is provided to NAVEX Global personnel in the U.S. for the purposes described in this TRA, customer data must be accessible in the clear to provide the requisite support or service function.

#	Factor	Response
12.	What is the storage location of the data transferred?	The European Union.
13.	What are the sub-processing activities?	Please see details here: https://www.navexglobal.com/en-us/service-hosting-providers. These are temporary and limited sub-processing activities. All requirements are flown down to each sub-processor.
Importer's exposure to government surveillance and practical application of Section 702 FISA		
14.	Is the data importer's sector or business directly subject to such laws in its jurisdiction that permit government access to personal data, or require the assistance of data importer to disclose personal data to public authorities, for surveillance and intelligence gathering purposes?	No. In our reasonable opinion upon internal and outside counsel review, we do not find NAVEX Global to be directly subject to such laws. As a practical matter based on the nature of NAVEX Global's services, the types of personal data processed, and the absence of any prior requests received in the past, NAVEX Global believes it is extremely unlikely to receive requests from U.S. government agencies to obtain customer data for national security purposes or to participate in the types of U.S. bulk surveillance programs scrutinized by the CJEU in its recent ruling on data transfer mechanisms. ***NAVEX Global has never received <u>ANY</u> requests for data pertaining to its RiskRate services. ***
	a. Specifically, what is data importer's analysis regarding Section 702 FISA under the SCCs and EDPB Guidance?	1) Data exporters may decide to proceed with the transfer without supplementary measures, if they consider there to be no reason to believe that the relevant and problematic legislation (those in the U.S. in this instance) will be applied, in practice, to the transferred data and/or NAVEX Global. a. In our reasonable opinion upon internal and outside counsel review, we do not find U.S. surveillance laws, including Section 702 FISA, to practically apply to these transfers. b. It is important to note that given the broad definitions of these laws, the vast majority of organizations are going to have to acknowledge their potential application. However, this does not mean they directly apply or practically apply in practice. c. We believe NAVEX Global is generally out of scope and that these laws are overall not going to apply to the services we provide, as the intent is for surveillance of certain telecom and internet service

#	Factor	Response
		providers for targeted information. This typically involves to surveillance of real time emails, texts, and chat conversations. The foregoing is not what NAVEX Global provides and to obtain this sought for information, authorities would pursue those providers directly as it would be impractical to make a request through NAVEX Global. 2) Data exporters may also take into consideration documented practical experience of data importer with relevant prior instances of requests for access received from public authorities in the U.S. a. ***To this point, NAVEX Global has never received a Section 702 FISA request or an EO 12.333 request or order. Please see our Public Authority Disclosure Request Policy for more details.** * **b. **NAVEX Global has never received <u>ANY</u> requests for data pertaining to its RiskRate services. *** c. The EDPB Guidance implies that the lack of requests received in the past plus no prohibition on providing information about such requests, could be sufficient to conclude Section 702 FISA does not apply in practice. Note there is no prohibition on NAVEX Global to provide information about these requests. 3) If you conclude Section 702 FISA does not apply in practice to the particular transfer, it is possible to proceed with the transfer without any supplementary measures. **a. While NAVEX Global takes the approach that Section 702 FISA does not apply in practice, we still have elected to provide for supplementary measures with regard to these transfers. Please see Section IV (D).**
15.	Within the last three (3) years, has the data importer received requests/demands from public authorities in its jurisdiction to disclose EU personal data pursuant to the SCCs?	No.
	a. Approximately how many requests/demands from public authorities has the data importer received in that time period concerning EU personal data pursuant to the SCCs?	None.
	b. Approximately how many of these requests/demands are pursuant to criminal law procedure in the destination	****NAVEX Global has never received <u>ANY</u> requests for data pertaining to its RiskRate**

#	Factor	Response
	country? *[Regular court proceedings are not the issue under Schrems II, but intelligence programs are scrutinized.]*	**services. *** While NAVEX Global has not received requests from public authorities for EU personal data under the SCCs or otherwise, we have received a limited number of formal requests or demands from U.S. government **authorities concerning customer data pertaining to its hotline and incident management services**. These requests have been made in the context of criminal and civil actions in the form of a subpoena issued to NAVEX Global as a third party, by a state or federal court. In each instance, we've notified the customer straight away and they have directed us to comply with the subpoena. We've only fulfilled such requests with full customer clearance and direction on how to handle.
	c. Approximately how many of these requests/demands are pursuant to national security or intelligence agencies in the destination country?	None. The data importer can represent that it has not received requests/demands from intelligence agencies. NAVEX Global offers signed contracts, warranting it has not received such requests, via either a data processing addendum or amendment to data processing addendum.
	d. Has the data importer been able to contest/minimize such disclosure of EU personal data, where appropriate?	Not applicable
	e. What types of EU personal data has the data importer been required to disclose to public authorities in its jurisdiction?	Not applicable
16.	How likely is it that the data importer will receive bulk data surveillance requests to disclose EU personal data to public authorities in its jurisdiction in the future (e.g., based on factors such as the type of services provided and sector in which the data importer operates, its size, number of customers and reputation)?	Unlikely. As a practical matter based on the nature of NAVEX Global's services, the types of personal data processed, and the absence of any prior requests received in the past, NAVEX Global believes it is extremely unlikely to receive requests from U.S. government agencies to obtain customer data for national security purposes or to participate in the types of U.S. bulk surveillance programs scrutinized by the CJEU in its recent ruling on data transfer mechanisms. We have no reason to believe we may receive such requests in the future.
17.	Does the data importer maintain annual reports or statistics regarding requests/demands received from law enforcement or intelligence agencies (e.g., number/type of requests/demands, requesting authority, etc.)?	Not applicable. NAVEX Global has not received requests from public authorities for EU personal data under the SCCs or otherwise. As a result, if we get such requests in the future, we will provide such statistics and update our TRA process and Public Authority Disclosure Policy accordingly.

#	Factor	Response
18.	Does the data importer maintain a written procedure(s) for: 1. Responding to or challenging requests/demands of law enforcement or intelligence agencies that apply to EU personal data? 4. Informing customers of requests/demands from law enforcement or intelligence agencies where permitted by applicable law?	Yes, please see our Public Authority Disclosure Request Policy.
19.	Are the data importer's commitments enabling data subjects to exercise their rights as provided in the SCCs thwarted by the laws and/or practices in the U.S. or can these rights be effectively applied in practice?	NAVEX Global has never encountered a situation where it felt it could not enable data subject rights, including judicial redress. We do not believe the laws subject to us prevent us from enabling, supporting, and fulfilling data subject rights under the SCCs.
Onward transfers and exposure to government surveillance		
20.	Does the data importer share EU personal data further with sub-processors whose processing takes place in third countries?	Yes.
21.	What measures does the third-party data recipient take to ensure the protection of EU personal data transferred to it?	NAVEX Global enters into written agreements with sub-processors that include safeguards for EU personal data in accordance with the GDPR requirements.
22.	What assurances has the data importer received from third-party data recipients with respect to requests/demands for EU personal data from [U.S./other jurisdiction] public authorities?	NAVEX Global has updated, or is in the process of updating, all written agreements with sub-processors to include additional measures for the protection of EU personal data, where required.

Conclusion/Risk of transfers

Likely limited-risk data transfer

In particular, NAVEX Global identified the following factors (based on the assessment documented above and any additional information), that are likely to indicate a limited-risk transfer:

The data importer has never received requests/demands from intelligence services for disclosure of EU personal data.

The data importer has received limited requests/demands from public authorities for disclosure of EU personal data (such as for disclosure of employee data), but the requests related to regular criminal law procedure and did not go beyond what is necessary and proportionate to meet the purpose of the request.

#	Factor	Response
		The data importer has a process in place for handling and contesting public authority access requests, if received. Based on the nature of its services and data processing activities, the data importer does not expect to be the target of requests/demands pursuant to national security or intelligence agencies for disclosure of EU personal data. Such data transfers are not directly nor practically in scope of requests/demands from national security or intelligence agencies for disclosure of EU personal data.

D. Supplementary Measures

Notwithstanding the Conclusion set forth in the above TRA, NAVEX Global has also adopted the following supplemental measures. We believe that by implementing such supplemental measures, we are following best practices and are demonstrating our serious commitment to the protection of customer data.

Contractual safeguards	The SCCs themselves contain a number of contractual commitments by NAVEX Global and its customer, aimed at serving as safeguards for EU personal data.
	Supplementary contractual assurances are offered via our standard data processing addendum or an amendment to the data processing addendum. Please reach out to privacy@navexglobal.com in order to get this in place.
	NAVEX Global agrees to audit and monitor its obligations, and to support its customers auditing and monitoring obligations, regarding the level of government access to data.
	NAVEX Global provides a data processing agreement to support GDPR compliance, which includes the SCCs. As the data processor/importer, we process personal data strictly in accordance with your instructions and to provide the services. Our customers are the owners of the personal data within our service applications. NAVEX Global offers a Data Security Addendum, providing for contractual commitments to its information security program.
Organizational safeguards	NAVEX Global maintains written processes and procedures which provide for review of and limit the scope of EU personal data disclosed by NAVEX Global in response to requests from public authorities. Please see our Public Authority Disclosure Request Policy.

	NAVEX Global maintains internal record of requests made by public authorities concerning EU personal data.
	NAVEX Global takes steps to limit the volume of disclosed data, where possible.
	NAVEX Global would take data minimization measures such as redacting unnecessary identifiable personal data or personal data that may be of increased interest to intelligence agencies before complying with a request to disclosure EU personal data.
	NAVEX Global has developed the attached Standard Contractual Clauses Assurance Guide, which details our commitment to compliance with the SCCs. NAVEX Global remains a participant and has certified its compliance with the EU-U.S. Privacy Shield Framework and the Swiss- U.S. Privacy Shield Framework. NAVEX Global, Inc. is committed to subjecting all personal information received from the European Economic Area, United Kingdom, and Switzerland, respectively, in reliance on each Privacy Shield Framework, to the Frameworks' applicable Principles. To learn more about the Privacy Shield program, and to view our certification, please visit https://www.privacyshield.gov. NAVEX Global provides an independent recourse mechanism to EU individuals, currently TrustArc.
Technical safeguards	Encrypt personal data in transit.
	Encrypt personal data at rest.
	Appropriate access controls.
	Customers can implement data minimization (e.g., store the least amount of data necessary).
	Timespan for any access to personal data "in the clear" is limited to the specific function.
	Store personal data in the EU and enable only remote access.
	NAVEX Global equips its services with self-servicing functionality, allowing you to manage the personal data on your own through the use of the services.

	NAVEX Global engages a recognized, independent third party to conduct a Statement on Standards for Attestation Engagements No. 16, Service Organization Control 2, Type 2 ("SSAE 18 SOC 2 Type 2") audit (or its equivalent or successor) of its information security program and its administrative, technical, and physical safeguards for all facilities used to deliver the Services, which specifically includes privacy controls. NAVEX Global maintains an annual Standardized Information Gathering Questionnaire ("SIG"), which details our robust security program with supporting documentation.

Conclusion

Having regard to the level of risk of the data transfer (**limited risk**), NAVEX Global considers that the measures identified above are **sufficient and effective** in light of the circumstances of the transfers, in conjunction with the supplementary measures and safeguards provided by the SCCs, to allow the data importer to comply with its obligations under the SCCs and provide an appropriate level of protection for the transfer.

RiskRate EU Hosted Sub-processing Activity: Due Diligence with Regulatory DataCorp

NAVEX GLOBAL SUB-PROCESSING ACTIVITY

EU HOSTED RISKRATE- REGULATORY DATACORP TRANSFER RISK ASSESSMENT

I. SCOPE

This TRA applies to NAVEX Global's EU Hosted RiskRate customers. This TRA applies specifically to the services provided by NAVEX Global's sub-processor, Regulatory DataCorp, Inc. (RDC).

As part of NAVEX Global's RiskRate services, our customers provide certain personal data in NAVEX Global's systems to be received and processed by RDC as part of the due diligence screenings. For NAVEX Global's EU Hosted customers, RDC utilizes servers located in the EU for the applicable hosting.

RDC personnel access to customer personal data is limited to only a select group of RDC staff members through RDC's VPN and to limited and vetted sub-processors (applicable for Analyst Review only). The relevant RDC staff members are located in the United States, the United Kingdom, and Singapore. The analyst review manager for inquiries sent to NAVEX Global's EU servers is located in the UK. The sub-processors are located in the US, Romania, India and Bangladesh.

II. ASSESSING THE ADEQUACY OF EU/UK DATA TRANSFERS – RDC SERVICES

In assessing the adequacy of transfers of personal data from the EU/UK to NAVEX Global's sub-processor pursuant to the RDC services, we have taken the following steps:

1. **STEP 1:** Identified the relevant data transfers and the legal mechanism that NAVEX Global and sub-processor is relying on for such transfers (e.g., SCCs).

2. **STEP 2:** Conducted due diligence and collected information about the scope of the transfers, the exposure of the sub-processor to local law that may require disclosure of EU personal data about individuals, and any other relevant information.

3. **STEP 3:** Completed the "Transfer Risk Assessment" in **Section IV** to assess whether the SCCs is effective in light of all circumstances of the transfer.

4. **STEP 4:** Included additional "Supplementary Measures" as set forth in **Section IV (D)**.

5. **STEP 5:** Documented the assessment for accountability purposes. We encourage our customers to do the same.

6. **STEP 6:** NAVEX Global and its sub-processor is responsible for the periodic review of the assessment, which should take place at least annually, to ensure that the transfer of the EU personal data continues to be afforded an adequate level of protection.

III. TRANSFER RISK ASSESSMENT

Name Of Data Importer: Regulatory DataCorp, Inc. (NAVEX Global's sub-processor)

Completed By: NAVEX Global's Privacy Team and Moody's Privacy Team on behalf of RDC

Date: 25 September 2021

A. Type of Data Importer

Name of data importer: Regulatory DataCorp, Inc. ("RDC"). The Processor to Processor SCCs between NAVEX Global and RDC is part of a master services agreement between NAVEX Global and RDC.

B. Does RDC provide the following services to NAVEX Global:

	Data Importer	
Telecommunications	☐ Yes	☒ No
Other electronic communications (such as an Internet Service Provider or a provider of email, text message, VoIP, remote desktop or VPN services)?	☐ Yes	☒ No
Remote computing services	☐ Yes	☒ No
Other communications service where there may be access to wire or electronic communications	☐ Yes	☒ No

If no, please specify the nature of the services provided to NAVEX Global by the data importer: Provision of regulatory screening services GRID, Client Review, AI Review and Analyst Review.

C. Details of Data Transfers

Data transfer mechanism

Appropriate Processor to Processor SCCs between RDC and NAVEX Global.

Scope of personal data covered by the data transfer mechanism in place

The SCCs cover transfers of EU personal data from the EEA/UK to third countries, including the following categories of data subjects:

- Clients, business partners and vendors of customer Data Controller (who are natural persons)
- Employees or contact persons of customer Data Controller's third-party suppliers, business partners and vendors

D. Transfer Risk Assessment

The table below aids identification and evaluation of risk factors in relation to the specific data transfer. The assessment of each risk factor is recorded in appropriate detail.

#	Factor	Response
Scope of the transfers		
1.	What is the type of transfer?	NAVEX Global's customer submits certain personal data within the RiskRate system which is provided to RDC to utilize in its due diligence screening and ongoing monitoring. The processing by RDC is limited to the performance of the given screen or monitoring request.
2.	Is the transfer necessary?	Yes. The transfer is critical and necessary to provide the services to NAVEX Global, on behalf of NAVEX Global's customers.
3.	Is the transfer proportionate?	Yes. The transfer is strictly limited to screening and monitoring the information provided from the customer.
4.	Is the transfer occasional/non-routine or frequent/routine?	The transfer is non-routine to RDC on a per request basis.
5.	Will the transferred personal data be processed for a relatively long or short period of time?	Personal data is processed for a relatively short period of time to support the applicable due diligence requests.
6.	Is the transferred data encrypted and/or pseudonymized?	Yes, both Encryption in transit and at rest and Obfuscation as follows: In storage, the data is contained within unique database tables assigned to each "firm" in the application, Firm identifiers are not client name but rather a unique two alphabetical character + a 6-character alphanumeric string. Clients can set this firm ID. In processing there is anonymization between RDC and its sub processors, i.e. it is never disclosed to offshore analysts which client submitted inquiry data for which they review, this is done through role based views within he analytics application.

#	Factor	Response
Specific circumstances of the transfer		
7.	What are the purposes for which the data are transferred and processed?	To provide the best publicly available information regarding adverse media alerts, sanctions watchlists, and politically exposed alerts.
8.	What are the types of entities involved in the processing?	RDC is a data sub-processor and a private company. NAVEX Global's customers are the data controllers and may consist of both private and public companies.
9.	In which sector does the transfer occur?	NAVEX Global provides risk and compliance management SaaS based software. ***This factor is especially important as the purposes of our services is to enable organizations support their risk, ethics, and compliance programs.** * Many of our customers are required by law to conduct appropriate due diligence on third parties. As such, our customers request certain data to be screened and provided back to them, to allow them to conduct this due diligence.
10.	What are the categories of personal data transferred?	Customers can send the following categories of data to RDC via NAVEX Global's RiskRate services: • name, address information (street, city, state/province, country, zip code), date of birth ***No sensitive data, as defined under the GDPR, is sent to RDC from customer to the RiskRate services. ***
11.	What is the format of the personal data to be transferred?	When personal data is provided to RDC for the purposes described in this TRA, such personal data must be accessible in the clear to fulfill the request.
12.	What is the storage location of the data transferred?	The European Union for NAVEX Global's EU hosted customers.
13.	What are the sub-sub-processing activities?	AWS: cloud hosting. Europe (specifically Ireland as Primary and Frankfurt as Secondary for NAVEX Global customers who elect EU hosting) WNS: Remote customer support (all Review

#	Factor	Response
		products); Analyst review (applicable for Analyst Review only). SEBPO: Analyst review (applicable for Analyst Review only).
Importer's exposure to government surveillance and practical application of Section 702 FISA		
14.	Is the data importer's sector or business directly subject to such laws in its jurisdiction that permit government access to personal data, or require the assistance of data importer to disclose personal data to public authorities, for surveillance and intelligence gathering purposes?	No, RDC's business is currently not directly subject to such laws.
	a. What is data importer's analysis regarding applicable third country surveillance and intelligence laws under the SCCs and EDPB Guidance?	NAVEX Global and RDC have conducted an analysis and the risk is very low, given the nature of our business. The same conclusions as set forth in this TRA apply to any transfers in non-U.S. countries.
	b. Specifically, what is data importer's analysis regarding third country surveillance laws, especially Section 702 FISA, under the SCCs and EDPB Guidance?	1) Data exporters may decide to proceed with the transfer without supplementary measures, if they consider there to be no reason to believe that the relevant and problematic legislation (for example, those in the U.S.) will be applied, in practice, to the transferred data and/or RDC. a. In our reasonable opinion upon internal and outside counsel review, we do not find third country surveillance laws, including Section 702 FISA from the U.S., to practically apply to these transfers. b. It is important to note that given the broad definitions of these laws, the vast majority of organizations are going to have to acknowledge their potential application. However, this does not mean they directly apply or practically apply in practice. c. We believe RDC is generally out of scope and that these laws are overall not going to apply to the services we provide, as the intent is for surveillance of certain telecom and internet service providers for targeted information. This typically involves to surveillance of real time emails, texts, and chat conversations. The foregoing is not what RDC nor NAVEX Global provides and to obtain this sought for information, authorities would pursue those providers directly as it would be

#	Factor	Response
		impractical to make a request through RDC. 2) Data exporters may also take into consideration documented practical experience of data importer with relevant prior instances of requests for access received from public authorities, including those in the U.S. c. ***To this point, RDC has never received a Section 702 FISA request, an EO 12.333 request or order, or any other country access request.** * d. The EDPB Guidance implies that the lack of requests received in the past plus no prohibition on providing information about such requests, could be sufficient to conclude Section 702 FISA does not apply in practice. Note there is no prohibition on RDC to provide information about these requests. 3) If you conclude Section 702 FISA, or any other potential similar types of surveillance laws, does not apply in practice to the particular transfer, it is possible to proceed with the transfer without any supplementary measures. **a. While NAVEX Global and RDC take the approach that Section 702 FISA does not apply in practice, we still have elected to provide for supplementary measures with regard to these transfers. Please see Section IV (D).**
15	Within the last three (3) years, has the data importer received requests/demands from public authorities in its jurisdiction to disclose EU personal data?	Based on available information, RDC does not receive requests/demands for disclosure of, or access to, EU personal data.
	a. Approximately how many requests/demands from public authorities has the data importer received in that time period concerning EU personal data?	None, to the best of our knowledge.
	b. Approximately how many of these requests/demands are pursuant to criminal law procedure in the destination country? *[Regular court proceedings are not the issue under Schrems II, but intelligence programs are scrutinized.]*	None, to the best of our knowledge.
	c. Approximately how many of these requests/demands are pursuant to national security or intelligence agencies in the destination country?	None, to the best of our knowledge. The data importer can represent that it has not received requests/demands from intelligence agencies.

#	Factor	Response
	d. Has the data importer been able to contest/minimize such disclosure of EU personal data, where appropriate?	Not applicable.
	e. What types of EU personal data has the data importer been required to disclose to public authorities in its jurisdiction?	Not applicable
16	How likely is it that the data importer will receive bulk data surveillance requests to disclose EU personal data to public authorities in its jurisdiction in the future (e.g., based on factors such as the type of services provided and sector in which the data importer operates, its size, number of customers and reputation)?	Unlikely. RDC's entities do not receive requests/demands by public authorities for disclosure of, or access to, EU personal data, and have no reason to believe that they might receive such in the future.
17	Does the data importer maintain annual reports or statistics regarding requests/demands received from law enforcement or intelligence agencies (e.g., number/type of requests/demands, requesting authority, etc.)?	Not applicable. RDC has not received requests from public authorities for EU personal data under the SCCs or otherwise. As a result, if RDC gets such requests in the future, it will notify NAVEX Global and this TRA will be updated accordingly.
18	Does the data importer maintain a written procedure(s) for: 1. Responding to or challenging requests/demands of law enforcement or intelligence agencies that apply to EU personal data? 3. Informing customers of requests/demands from law enforcement or intelligence agencies where permitted by applicable law?	RDC does not maintain a written policy because no requests have ever been received. However, in the event of any request, these would be reviewed by the Privacy Team within Legal and NAVEX Global will be duly notified where required. RDC and NAVEX Global entered into a contractual agreement requiring RDC to cooperate and mutually agree on any appropriate actions, to notify NAVEX Global of any requests unless explicitly required otherwise under applicable law, to put any access request on hold, and to use reasonable efforts to obtain the right to waive any notice prohibitions and oppose any such request and contest its legal validity where possible and permitted. The contract additionally ensures RDC will not make any disclosures that are determined to be massive, disproportionate, and indiscriminate in a manner that would go beyond what is necessary in a democratic society. RDC is obliged to document and demonstrate to the assessments made and the actions taken. RDC undertakes to regularly review, assess, and continuously monitor the scope of the access to personal data by public authorities in the countries where RDC is processing personal data, as well as the safeguards and recourses in place to protect data subjects, and to immediately inform NAVEX Global in the case of a change in applicable law that would materially impact such access by public authorities or recourses available to data subjects.

#	Factor	Response
19	Are the data importer's commitments enabling data subjects to exercise their rights as provided in the SCCs thwarted by the laws and/or practices in the U.S. and any other third countries involved, or can these rights be effectively applied in practice?	No. Data subjects' rights can be effectively applied in practice. RDC has never encountered a situation where it felt it could not enable data subject rights, including judicial redress. We do not believe the laws subject to us prevent us from enabling, supporting, and fulfilling data subject rights under the SCCs.
Onward transfers and exposure to government surveillance		
20	Does the data importer share EU personal data further with third-party data recipients in [the U.S./other jurisdiction]?	Yes, RDC utilizes AWS: cloud hosting. Europe (specifically Ireland as Primary and Frankfurt as Secondary for NAVEX Global customers who elect EU hosting) WNS: Analyst review (applicable for Analyst Review only). SEBPO: Analyst review (applicable for Analyst Review only).
21	What measures does the third-party data recipient take to ensure the protection of EU personal data transferred to it?	Where RDC engages sub-processors that have access to EU personal data, RDC enters into written agreements with sub-processors that include safeguards for EU personal data in accordance with the GDPR requirements.
22	What assurances has the data importer received from third-party data recipients with respect to requests/demands for EU personal data from [U.S./other jurisdiction] public authorities?	RDC will update written agreements with sub-processorsto include additional measures for the protection of EU personal data, where required. Existing data processing addendums are in place under applicable law.
23	Is the vendor's (or its sub-processor's) sector or business directly subject to such laws in its jurisdiction that permit government access to personal data, or require the assistance of data importer to disclose personal data to public authorities, for surveillance and intelligence gathering purposes?	No, RDC does not believe in its reasonable opinion that it or its sub-processors are directly subject to such laws in their jurisdiction.
Conclusion/Risk of transfers **Very limited-risk data transfer** **In particular, RDC and NAVEX Global identified the following factors (based on the assessment documented above and any additional information), that are likely to indicate a limited-risk transfer:** No further processing outside of a given screen and/or monitoring request takes place. The data importer has never received requests/demands from intelligence services for disclosure of EU		

personal data. The data importer has received limited requests/demands from public authorities for disclosure of EU personal data (such as for disclosure of employee data), but the requests related to regular criminal law procedure and did not go beyond what is necessary and proportionate to meet the purpose of the request. The data importer has a process in place for handling and contesting public authority access requests, if received. Based on the nature of its services and data processing activities, the data importer does not expect to be the target of requests/demands pursuant to national security or intelligence agencies for disclosure of EU personal data. Such data transfers are not directly nor practically in scope of requests/demands from national security or intelligence agencies for disclosure of EU personal data.

E. Supplementary Measures

Notwithstanding the Conclusion set forth in the above TRA, RDC has also adopted the following supplemental measures. We believe that by implementing such supplemental measures, we are following best practices and are demonstrating our serious commitment to the protection of customer data.

Contractual safeguards	RDC and NAVEX Global have entered into supplementary contractual assurances as an amendment to the data processing addendum.
	The SCCs themselves contain a number of contractual commitments by RDC and NAVEX Global, aimed at serving as safeguards for EU personal data. We have also entered into a robust general data processing addendum.
Organizational safeguards	RDC would maintain internal record of requests made by public authorities concerning EU personal data.
	RDC would take steps to limit the volume of disclosed data, where possible and applicable.
	RDC would take data minimization measures such as redacting unnecessary identifiable personal data or personal data that may be of increased interest to intelligence agencies before complying with a request to disclosure EU personal data.
Technical safeguards	Encrypt personal data in transit.

	Encrypt personal data at rest.
	Encryption key kept in the EU for data hosted in the EU.
	Appropriate access controls.
	Enhance data minimization (e.g., store the least amount of data necessary).
	Limit timespan for using personal data "in the clear" (i.e., in identifiable form).
	Obfuscate stored personal data.
	Store personal data in the EU and enable only remote access or view-only access.

Conclusion

Having regard to the level of risk of the data transfer (**limited risk**), RDC and NAVEX Global considers that the measures identified above are **sufficient and effective** in light of the circumstances of the transfers, in conjunction with the supplementary measures and safeguards provided by the SCCs, to allow the data importer to comply with its obligations under the SCCs and provide an appropriate level of protection for the transfer.

RiskRate EU Hosted Sub-processing Activity: Due Diligence with Pacific Strategies & Assessments

NAVEX GLOBAL SUB-PROCESSING ACTIVITY

EU HOSTED RISKRATE- PACIFIC STRATEGIES & ASSESSMENTS TRANSFER RISK ASSESSMENT

I. SCOPE

This TRA applies to NAVEX Global's EU Hosted RiskRate customers. This TRA applies specifically to the services provided by NAVEX Global's sub-processor, Pacific Strategies & Assessments Limited (PSA).

As part of NAVEX Global's RiskRate services, our customers provide certain personal data in NAVEX Global's systems to be received and processed by PSA as part of the enhanced due diligence screenings. PSA's network

is located in the Philippines. PSA logs into NAVEX Global's RiskRate services, hosted in the EU, to view the customer's request. During this viewing, PSA personnel extract relevant details including the level of research required, jurisdiction of research, and names of designated subject entities. An analyst in the Philippines will be assigned to process the provided information. In addition to the Philippines, material relating to a NAVEX Global customer RiskRate request may be processed by PSA staff located in China, the UAE and occasionally, in the Czech Republic. The information required for these offices to process the case element will be sent by internal email to ensure data security is maintained. The staff will conduct the local language or other research required and on completion will return the result over the same secure internal email system.

II. ASSESSING THE ADEQUACY OF EU/UK DATA TRANSFERS –

In assessing the adequacy of transfers of personal data from the EU/UK to NAVEX Global's sub-processor pursuant to the PSA services, we have taken the following steps:

1. **STEP 1:** Identified the relevant data transfers and the legal mechanism that NAVEX Global and sub-processor is relying on for such transfers (e.g., SCCs).

2. **STEP 2:** Conducted due diligence and collected information about the scope of the transfers, the exposure of the sub-processor to local law that may require disclosure of EU personal data about individuals, and any other relevant information.

3. **STEP 3:** Completed the "Transfer Risk Assessment" in **Section IV** to assess whether the SCCs is effective in light of all circumstances of the transfer.

4. **STEP 4:** Included additional "Supplementary Measures" as set forth in **Section IV (D)**.

5. **STEP 5:** Documented the assessment for accountability purposes. We encourage our customers to do the same.

6. **STEP 6:** NAVEX Global and its sub-processor is responsible for the periodic review of the assessment, which should take place at least annually, to ensure that the transfer of the EU personal data continues to be afforded an adequate level of protection.

III. TRANSFER RISK ASSESSMENT

Name Of Data Importer: Pacific Strategies & Assessments Limited ("PSA") (NAVEX Global's sub-processor)

Completed By: NAVEX Global's Privacy Team and PSA's Privacy Team

Date: 25 September 2021

The Processor to Processor SCCs between NAVEX Global and PSA is part of a master services agreement between NAVEX Global and PSA.

A. Does PSA provide the following services to NAVEX Global:

	Data Importer	
Telecommunications	☐ Yes	☒ No
Other electronic communications (such as an Internet Service Provider or a provider of email, text message, VoIP, remote desktop or VPN services)?	☐ Yes	☒ No
Remote computing services	☐ Yes	☒ No
Other communications service where there may be access to wire or electronic communications	☐ Yes	☒ No

If no, please specify the nature of the services provided to NAVEX Global by the data importer: PSA provide Due Dilligence reports uploaded at the customer Data Controller's request into the NAVEX Global service portal.

B. Details of Data Transfers

Data transfer mechanism

Appropriate Processor to Processor SCCs between PSA and NAVEX Global.

Scope of personal data covered by the data transfer mechanism in place

The SCCs cover transfers of EU personal data from the EEA/UK to third countries, including the following categories of data subjects:

- Clients, business partners and vendors of customer Data Controller (who are natural persons)
- Employees or contact persons of customer Data Controller's third-party suppliers, business partners and vendors

C. Transfer Risk Assessment

The table below aids identification and evaluation of risk factors in relation to the specific data transfer. The assessment of each risk factor is recorded in appropriate detail.

#	Factor	Response
Scope of the transfers		
1.	What is the type of transfer?	NAVEX Global's customer submits certain personal data within the RiskRate system which is provided to PSA to utilize for the enhanced due diligence request. The processing by PSA is limited to the performance of the given request.
2.	Is the transfer necessary?	Yes. The transfer is critical and necessary to provide the services to NAVEX Global, on behalf of NAVEX Global's customers.
3.	Is the transfer proportionate?	Yes. The transfer is strictly limited to the due diligence request information provided from the customer.
4.	Is the transfer occasional/non-routine or frequent/routine?	The transfer is non-routine to PSA on a per request basis.
5.	Will the transferred personal data be processed for a relatively long or short period of time?	Personal data is processed for a relatively short period of time to support the applicable due diligence requests.
6.	Is the transferred data encrypted, pseudonymized or otherwise processed in an unintelligible form??	Yes, encryption in transit and at rest during all stages of processing.
Specific circumstances of the transfer		
7.	What are the purposes for which the data are transferred and processed?	The data is directly used to construct an Enhanced Due Diligence report and so contains information in the request including who the report is on, and any supporting details needed to carry out the report.
8.	What are the types of entities involved in the processing?	PSA is a data sub-processor and a private company. NAVEX Global's customers are the data controllers and may consist of both private

#	Factor	Response
		and public companies.
9.	In which sector does the transfer occur?	NAVEX Global provides risk and compliance management SaaS based software. ***This factor is especially important as the purposes of our services is to enable organizations support their risk, ethics, and compliance programs. *** Many of our customers are required by law to conduct appropriate due diligence on third parties. As such, our customers request certain data to be screened and provided back to them, to allow them to conduct this due diligence.
10.	What are the categories of personal data transferred?	Customers can send various categories of data to PSA for processing using NAVEX Global's RiskRate services. This can include company name and details used to identify a company or individual as required by the scope of the work. ***No sensitive data, as defined under the GDPR, is transferred from the customer Data Controller to NAVEX Global nor PSA as part of the RiskRate services. ***
11.	What is the format of the personal data to be transferred?	When personal data is provided to PSA for the purposes described in this TRA, such personal data must be accessible in the clear to fulfill the request.
12.	What is the storage location of the data transferred?	The European Union via NAVEX Global's secure servers.
13.	What are the sub-sub-processing activities?	Only where it is essential based on the requirements of the customer request/task (for example where a physical site visit or attendance at court in a separate country is required) will PSA take some of the relevant information and provide it to a sub-sub-processor to complete this section of the tasking. This information is provided through encrypted email, password protected excel sheet or password protected zip folder. All sub-sub-processors agree to and are subject to PSA's data protection and retention policies. Sub-sub-processors agree to delete all record of

#	Factor	Response
		the matter from their system within 60 days of completion of their tasking under the secondary sub processor allocation.
Importer's exposure to government surveillance and practical application of such laws		
14.	Is the data importer's sector or business directly subject to such laws in its jurisdiction that permit government access to personal data, or require the assistance of data importer to disclose personal data to public authorities, for surveillance and intelligence gathering purposes?	No, in our reasonable opinion, PSA's business is currently not directly subject to such laws. As a Philippines registered business PSA must comply with all relevant laws, for example the Expanded Anti-Trafficking in Persons Act of 2012, the Anti-Child Pornography Act of 2009, the Cybercrime Prevention Act of 2012, and the Anti-Terrorism Act of 2020 which may require data access, however, our business sector is not directly subject to these laws.
	a. What is data importer's analysis regarding applicable third country surveillance and intelligence laws under the SCCs and EDPB Guidance?	1) Data exporters may decide to proceed with the transfer without supplementary measures, if they consider there to be no reason to believe that the relevant and problematic legislation will be applied, in practice, to the transferred data and/or PSA. a. Philippines law mandates a court order for surveillance or data access to support an active investigation and supports the international laws on data privacy however in practice we do not believe that the laws are focused on our industry or sector, and so do not apply to these transfers between PSA and NAVEX Global in practice. b. It is important to note that given the broad definitions of these laws, the vast majority of organizations are going to have to acknowledge their potential application. However, this does not mean they directly apply or practically apply in practice. c. We believe PSA is generally out of scope and that these laws are overall not going to apply to the services provided, as the intent is for surveillance of certain telecom and internet service providers for targeted information. This typically involves to surveillance of real time emails, texts, and chat conversations. The foregoing is not what PSA nor NAVEX Global provides and to obtain this sought

#	Factor	Response
		for information, authorities would pursue those providers directly as it would be impractical to make a request through PSA. 2) Data exporters may also take into consideration documented practical experience of data importer with relevant prior instances of requests for access received from public authorities. a. **To this point, PSA has never received a public authority access request.*** b. The EDPB Guidance implies that the lack of requests received in the past plus no prohibition on providing information about such requests, could be sufficient to conclude relevant problematic legislation does not apply in practice. Note there is no prohibition on PSA to provide information about these requests. 3) If you conclude such surveillance laws do not apply in practice to the particular transfer, it is possible to proceed with the transfer without any supplementary measures. **While NAVEX Global and PSA take the approach that such laws don't apply in practice, we still have elected to provide for supplementary measures with regard to these transfers. Please see Section IV (D).**
15.	Within the last three (3) years, has the data importer received requests/demands from public authorities in its jurisdiction to disclose EU personal data?	PSA has not received requests/demands for disclosure of, or access to, EU personal data in the last 3 years.
	a. Approximately how many requests/demands from public authorities has the data importer received in that time period concerning EU personal data?	None, to the best of our knowledge.
	b. Approximately how many of these requests/demands are pursuant to criminal law procedure in the destination country? *[Regular court proceedings are not the issue under Schrems II, but intelligence programs are scrutinized.]*	None, to the best of our knowledge.
	c. Approximately how many of these requests/demands are pursuant to national security or intelligence agencies	None, to the best of our knowledge. The data importer can represent that it has not received

#	Factor	Response
	in the destination country?	requests/demands from intelligence agencies.
	d. Has the data importer been able to contest/minimize such disclosure of EU personal data, where appropriate?	Not applicable.
	e. What types of EU personal data has the data importer been required to disclose to public authorities in its jurisdiction?	Not applicable.
16.	How likely is it that the data importer will receive bulk data surveillance requests to disclose EU personal data to public authorities in its jurisdiction in the future (e.g., based on factors such as the type of services provided and sector in which the data importer operates, its size, number of customers and reputation)?	Unlikely. PSA does not store bulk data on individuals nor provide resources that law enforcement would not be able to get internally without going through PSA.
17.	Does the data importer maintain annual reports or statistics regarding requests/demands received from law enforcement or intelligence agencies (e.g., number/type of requests/demands, requesting authority, etc.)?	Yes. Collected by relevant personnel and reported directly to the management team. Records kept for reporting and review by management team in a dedicated log.
18.	Does the data importer maintain a written procedure(s) for: 1. Responding to or challenging requests/ demands of law enforcement or intelligence agencies that apply to EU personal data? 5. Informing customers of requests/demands from law enforcement or intelligence agencies where permitted by applicable law?	Yes. Covered by "Data Request Policy". Inform customers within 24 hours of receiving authenticated request where possible within the law.
19.	Are the data importer's commitments enabling data subjects to exercise their rights as provided in the SCCs thwarted by the laws and/or practices in the U.S. and any other third countries involved, or can these rights be effectively applied in practice?	PSA has not yet encountered a situation where it felt it could not enable data subject rights, including judicial redress. We do not believe the laws we are subject to prevent us from enabling, supporting, and fulfilling data subject rights under the SCCs.
Onward transfers and exposure to government surveillance		
20.	Does the data importer share EU personal data further with third-party data recipients in [the U.S./other jurisdiction]?	Yes, only where it is essential based on the requirements of the customer request/task (for example where a physical site visit or attendance at court in a separate country is required) will PSA take some of the relevant information and provide it to a sub-sub-processor to complete this section of the tasking. This information is provided through encrypted email, password protected excel sheet or password protected zip folder.

#	Factor	Response
		All sub-sub-processors agree to and are subject to PSA's data protection and retention policies. Sub-sub-processors agree to delete all record of the matter from their system within 60 days of completion of their tasking under the secondary sub processor allocation.
21.	What measures does the third-party data recipient take to ensure the protection of EU personal data transferred to it?	Where PSA engages sub-processors that have access to EU personal data, PSA enters into written agreements with sub-processors that include safeguards for EU personal data in accordance with the GDPR requirements. These include strict requirements on how data can be transferred, and on how long data can be kept before mandatory deletion.
22.	What assurances has the data importer received from third-party data recipients with respect to requests/demands for EU personal data from [U.S./other jurisdiction] public authorities?	PSA has signed policies in place with sub-sub-processors to ensure their compliance and regularly carries out audits to ensure compliance. No sub-sub-party holds significant amounts of data and is obligated to inform PSA in the event of any data request where possible by law so that PSA can inform the relevant parties.
23.	Is the vendor's (or its sub-processor's) sector or business directly subject to such laws in its jurisdiction that permit government access to personal data, or require the assistance of data importer to disclose personal data to public authorities, for surveillance and intelligence gathering purposes?	No. As a Philippines registered business we must comply with all relevant laws, for example the Expanded Anti-Trafficking in Persons Act of 2012, the Anti-Child Pornography Act of 2009, the Cybercrime Prevention Act of 2012, and the Anti-Terrorism Act of 2020 which may require data access however our business sector is not directly subject to these laws and would not fall under any known surveillance or intelligence gathering assistance requests.

Conclusion/Risk of transfers

Very limited-risk data transfer

In particular, PSA and NAVEX Global identified the following factors (based on the assessment documented above and any additional information), that are likely to indicate a limited-risk transfer:

No further processing outside of a given enhanced due diligence request takes place.

The data importer has never received requests/demands from intelligence services for disclosure of EU personal data.

The data importer has received limited requests/demands from public authorities for disclosure of EU

#	Factor	Response
		personal data (such as for disclosure of employee data), but the requests related to regular criminal law procedure and did not go beyond what is necessary and proportionate to meet the purpose of the request. The data importer has a process in place for handling and contesting public authority access requests, if received. Based on the nature of its services and data processing activities, the data importer does not expect to be the target of requests/demands pursuant to national security or intelligence agencies for disclosure of EU personal data. Such data transfers are not directly nor practically in scope of requests/demands from national security or intelligence agencies for disclosure of EU personal data.

D. Supplementary Measures

Notwithstanding the Conclusion set forth in the above TRA, PSA has also adopted the following supplemental measures. We believe that by implementing such supplemental measures, we are following best practices and are demonstrating our serious commitment to the protection of customer data.

Contractual safeguards	PSA and NAVEX Global have entered into supplementary contractual assurances as an amendment to the data processing addendum.
	The SCCs themselves contain a number of contractual commitments by PSA and NAVEX Global, aimed at serving as safeguards for EU personal data. We have also entered into a robust general data processing addendum.
	PSA agrees to audit and monitor its obligations, and to support its customers auditing and monitoring obligations, regarding the level of government access to data.
Organizational safeguards	PSA maintains written processes and procedures to provide for review of and limit the scope of EU personal data disclosed by PSA in response to requests from public authorities.
	PSA maintains internal record of requests made by public authorities concerning EU personal data.
	PSA takes steps to limit the volume of disclosed data, where possible.

	PSA would take data minimization measures such as redacting unnecessary identifiable personal data or personal data that may be of increased interest to intelligence agencies before complying with a request to disclosure EU personal data.
Technical safeguards	PSA ensures that any personal data must be encrypted in transit and at rest with at least AES-128bit encryption.
	Logging of all access with unique identifiers for all actors to ensure audit trails and data confidentiality.
	PSA enforces appropriate strong access controls including 'minimum necessary access' for all work, ensuring that no more access is granted than is necessary to complete the work.
	PSA Implements data minimization (e.g., store the least amount of data necessary including using an alias to refer to projects where possible to ensure data subjects are kept 'need to know'.
	Timespan for any access to personal data "in the clear" is limited to the specific function.
	Personal data is ultimately stored in the EU via NAVEX Global's secure data centre.
	Data kept in PSA is held only long enough to collate, present and transfer the requested data, once the transfer is confirmed all copies are wiped from PSA systems. This provides considerably security and reduces any risks or responsibilities brought on by storing the data in PSA systems.

Conclusion

Having regard to the level of risk of the data transfer (**very limited risk**), PSA and NAVEX Global considers that the measures identified above are **sufficient and effective** in light of the circumstances of the transfers, in conjunction with the supplementary measures and safeguards provided by the SCCs, to allow the data importer to comply with its obligations under the SCCs and provide an appropriate level of protection for the transfer.

Disclosures: EU Hosted

EU HOSTED COI DISCLOSURES - EU/UK DATA TRANSFER RISK ASSESSMENTS

I. INTRODUCTION

NAVEX Global must conduct Transfer Risk Assessments ("TRA" or "TRAs") for transfers of personal data from the European Economic Area ("EEA")[5] or the United Kingdom ("UK") (collectively "EU personal data") to third countries that are not deemed to provide an adequate level of data protection.

II. SCOPE

These TRAs apply to NAVEX Global's EU Hosted Disclosures customers.

This TRA process applies to personal data transferred to NAVEX Global pursuant to the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council. This TRA is specifically designed to address Clause 14 of the foregoing set of Standard Contractual Clauses. Personal data from the UK is also in scope and shall be assessed pursuant to the European Commission's decision (C(2010)593) of 5 February 2010 on Standard Contractual Clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection. We collectively refer to the sets of Standard Contractual Clauses as the "SCCs." NAVEX Global agrees and acknowledges the UK will be issuing its own set of standard contractual clauses and related Schrems II guidance. We will update this TRA on an ongoing basis as needed.

This TRA process takes into account the European Data Protection Board's Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data adopted on 18 June 2021 (the "EDPB Guidance").

This TRA is not intended for transfers (i) within the EEA, (ii) between the EEA and the UK, or (iii) from the EEA or UK to a country recognized by the European Commission or UK law as adequate at this time (i.e., Andorra, Argentina, Canada (commercial organizations subject to PIPEDA), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, UK, and Uruguay).

The TRA is completed by the NAVEX Global Privacy Team, which consists of the Data Privacy Officer & Senior Counsel, Deputy Data Privacy Officer & Senior Counsel, and Privacy Counsel.

III. ASSESSING THE ADEQUACY OF EU/UK DATA TRANSFERS – TO NAVEX GLOBAL IN THE U.S.

In assessing the adequacy of transfers of personal data from the EU/UK to NAVEX Global in the U.S. we have taken the following steps:

1. **STEP 1:** Identified the relevant data transfers and the legal mechanism that NAVEX Global is relying on for such transfers (e.g., SCCs).

2. **STEP 2:** Conducted due diligence and collected information about the scope of the transfers, the exposure of NAVEX Global to local law that may require disclosure of EU personal data about individuals, and any other relevant information.

3. **STEP 3:** Completed the "Transfer Risk Assessment" in **Section IV** to assess whether the SCCs is effective in light of all circumstances of the transfer.

4. **STEP 4:** Included additional "Supplementary Measures" as set forth in **Section IV (D)**.

[5] The European Economic Area consists of the Member States of the EU (Austria, Belgium, Bulgaria, Croatia, Cyprus, Czechia, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain and Sweden), plus Iceland, Liechtenstein and Norway.

5. **STEP 5:** Documented the assessment for accountability purposes. We encourage our customers to do the same.

6. **STEP 6:** NAVEX Global is responsible for the periodic review of the assessment, which should take place at least annually, to ensure that the transfer of the EU personal data continues to be afforded an adequate level of protection.

IV. TRANSFER RISK ASSESSMENT

Name Of Data Importer: NAVEX Global
Scope of TRA: Transfers to NAVEX Global's affiliates in the United States as part of the Disclosure services provided to EU Hosted Customers
Completed By: NAVEX Global's Privacy Team
Date: 25 September 2021

A. Type of Data Importer

Name of data importer: NAVEX Global. The SCCs between customer and NAVEX Global is part of a master services agreement between customer and NAVEX Global UK Limited (registered in the UK) or GCS Compliance Services Europe Unlimited Company trading as NAVEX Global (registered in Ireland), both with their principal places of business at Vantage West – 4th floor, Great West Road, Brentford TW8 9AG, United Kingdom. Some EU Hosted customers elect to contract directly with our U.S. entity, NAVEX Global, Inc., a Delaware corporation with its principal place of business at 5500 Meadows Road, Suite 500, Lake Oswego, OR 97035.

Upon reviewing the broad definitions set forth within U.S. surveillance laws under scrutiny pursuant to the CJEU ruling in the Schrems II case, NAVEX Global identifies itself as follows:

NAVEX Global does not consider itself a "telecommunications carrier" as defined in 47 U.S.C. 152.

NAVEX Global acknowledges that certain of its services could be viewed by U.S. government authorities as an "electronic communication service" as defined in 18 U.S.C. 2510.

NAVEX Global acknowledges that certain of its services could be viewed by U.S. government authorities as a "remote computing service" as defined in 18 U.S.C. 2711.

NAVEX Global acknowledges that certain of its services could be viewed by U.S. government authorities as other communication services where there may be access to wire or electronic communications.

B. Details of Data Transfers

Data transfer mechanism Appropriate Controller to Processor SCCs between customer and NAVEX Global.
Scope of personal data covered by the data transfer mechanism in place The SCCs cover transfers of EU personal data from the EEA/UK to the U.S., including the following categories of data subjects: • Employees of data exporter • Clients, business partners and vendors of data exporter (who are natural persons) • Employees or contact persons of data exporters' third-party suppliers, business partners and vendors

- Data exporter's users authorized by data exporter to use the relevant Service(s)

C. Transfer Risk Assessment

The table below aids identification and evaluation of risk factors in relation to the specific data transfer. The assessment of each risk factor is recorded in appropriate detail.

#	Factor	Response
Scope of the transfers		
1.	What is the type of transfer?	Remote access only by direct NAVEX Global personnel located in the U.S. to personal data stored in the EU. Personal data is not stored in the U.S. as part of this transfer.
2.	Is the transfer necessary?	Yes. NAVEX Global has critical resources located in the U.S., requiring access to the EU hosted database for the following purposes: • Support. General support cases that are submitted, depending on the case, may require access to customer data to address the issue at hand. To meet our service level commitments, U.S. support may be involved accordingly. This is mainly due to certain resource limitations based on location, an overflow of support cases, and time zone challenges. • Administrative Service Functions. There is certain work, for example setting up the landing page, that does not necessarily require a deep level access, but for which can result in a transfer of personal data to the U.S. depending on the service need. • Technical Work. Many of our technical resources are in the U.S. which requires access to customer data. Examples include certain data extract services, certain data migration services, integration services, user setups instances, and hosting installations. again, depending on the task, we need the option to leverage those resources which involves a certain level of access. • IT/Hosting. Select members of the hosting and information security group must have access for maintenance and

#	Factor	Response
		troubleshooting. Without the above, our service level commitments would greatly suffer, and the overall maintenance and security of our service would be put at great risk.
3.	Is the transfer proportionate?	Yes. Access is not provided to personnel in the U.S. in a general sense. Access is provided to those personnel in the U.S. on a strict need to know basis to perform their given job function.
4.	Is the transfer occasional/non-routine or frequent/routine?	The transfer is non-routine to NAVEX Global personnel in the U.S. for the purposes detailed in Factor #2 above.
5.	Will the transferred personal data be processed for a relatively long or short period of time?	Personal data transferred to the U.S. in this context is processed for a relatively short period of time to provide the applicable service support.
6.	Is the transferred data encrypted and/ or pseudonymized?	Yes. NAVEX Global employs encryption at rest using either full-disk encryption or within the database using TDE. Data at rest will be encrypted using AES 256 or better, data in flight will be accomplished using TLS 1.2 or higher on public untrusted networks. Upon reviewing pseudonymization in the context of this transfer, it is inapplicable to the services we need to support.
Specific circumstances of the transfer		
7.	What are the purposes for which the data are transferred and processed?	To provide the best support, maintenance, and services as committed to in our agreements with our customers.
8.	What are the types of entities involved in the processing?	NAVEX Global is a data processor and a private company. Our customers are the data controllers and may consist of both private and public companies.
9.	In which sector does the transfer occur?	NAVEX Global provides risk and compliance management SaaS based software. ***This factor is especially important as the**

#	Factor	Response
		purposes of our services is to enable organizations support their risk, ethics, and compliance programs. *
10.	What are the categories of personal data transferred?	• Name (first and last), email address, job site, job title, department, supervisor, log-in credentials, completion status, details about the reported conflicts, time and date of disclosure. ****No sensitive data, as defined under the GDPR, is transferred as part of the Disclosures services.****
11.	What is the format of the personal data to be transferred?	NAVEX Global employs encryption at rest using either full-disk encryption or within the database using TDE. Data at rest will be encrypted using AES 256 or better, data in flight will be accomplished using TLS 1.2 or higher on public untrusted networks. When access is provided to NAVEX Global personnel in the U.S. for the purposes described in this TRA, customer data must be accessible in the clear to provide the requisite support or service function.
12.	What is the storage location of the data transferred?	The European Union.
13.	What are the sub-processing activities?	Please see details here: https://www.navexglobal.com/en-us/service-hosting-providers. Outside of affiliate access in scope of this TRA, there are no transfers outside the EU/UK via sub-sub-processors.
Importer's exposure to government surveillance and practical application of Section 702 FISA		
14.	Is the data importer's sector or business directly subject to such laws in its jurisdiction that permit government access to personal data, or require the assistance of data importer to disclose personal data to public authorities, for surveillance and intelligence gathering purposes?	No. In our reasonable opinion upon internal and outside counsel review, we do not find NAVEX Global to be directly subject to such laws. As a practical matter based on the nature of NAVEX Global's services, the types of personal data processed, and the absence of any prior requests received in the past, NAVEX Global believes it is extremely unlikely to receive requests from U.S. government agencies to obtain customer data for national security purposes or to participate in the types of U.S. bulk surveillance programs scrutinized by the CJEU in its recent ruling on data transfer mechanisms.

#	Factor	Response
	a. Specifically, what is data importer's analysis regarding Section 702 FISA under the SCCs and EDPB Guidance?	1) Data exporters may decide to proceed with the transfer without supplementary measures, if they consider there to be no reason to believe that the relevant and problematic legislation (those in the U.S. in this instance) will be applied, in practice, to the transferred data and/or NAVEX Global. a. In our reasonable opinion upon internal and outside counsel review, we do not find U.S. surveillance laws, including Section 702 FISA, to practically apply to these transfers. b. It is important to note that given the broad definitions of these laws, the vast majority of organizations are going to have to acknowledge their potential application. However, this does not mean they directly apply or practically apply in practice. c. We believe NAVEX Global is generally out of scope and that these laws are overall not going to apply to the services we provide, as the intent is for surveillance of certain telecom and internet service providers for targeted information. This typically involves to surveillance of real time emails, texts, and chat conversations. The foregoing is not what NAVEX Global provides and in order to obtain this sought for information, authorities would pursue those providers directly as it would be impractical to make a request through NAVEX Global. 2) Data exporters may also take into consideration documented practical experience of data importer with relevant prior instances of requests for access received from public authorities in the U.S. a. ***To this point, NAVEX Global has never received a Section 702 FISA request or an EO 12.333 request or order. Please see our Public Authority Disclosure Request Policy for more details.** * b. The EDPB Guidance implies that the lack of requests received in the past plus no prohibition on providing information about such requests, could be sufficient to conclude Section 702 FISA does not apply in practice. Note there is no prohibition on NAVEX Global to provide

#	Factor	Response
		information about these requests. 3) If you conclude Section 702 FISA does not apply in practice to the particular transfer, it is possible to proceed with the transfer without any supplementary measures. **a. While NAVEX Global takes the approach that Section 702 FISA does not apply in practice, we still have elected to provide for supplementary measures with regard to these transfers. Please see Section IV (D).**
15.	Within the last three (3) years, has the data importer received requests/demands from public authorities in its jurisdiction to disclose EU personal data pursuant to the SCCs?	No, not to the best of our knowledge.
	a. Approximately how many requests/demands from public authorities has the data importer received in that time period concerning EU personal data pursuant to the SCCs?	None, to the best of our knowledge.
	b. Approximately how many of these requests/demands are pursuant to criminal law procedure in the destination country? *[Regular court proceedings are not the issue under Schrems II, but intelligence programs are scrutinized.]*	While NAVEX Global has not received a Section 702 FISA request, an EO 12.333 request or order, or a public authority request specifically targeting EU personal data under the SCCs, we have received a limited number of formal requests or demands from U.S. government authorities concerning customer data. These requests have been made in the context of criminal and civil actions in the form of a subpoena issued to NAVEX Global as a third party, by a state or federal court. In each instance, we've notified the customer straight away and they have directed us to comply with the subpoena. We've only fulfilled such requests with full customer clearance and direction on how to handle.
	c. Approximately how many of these requests/demands are pursuant to national security or intelligence agencies in the destination country?	None, to the best of our knowledge. The data importer can represent that it has not received requests/demands from intelligence agencies. NAVEX Global offers signed contracts, warranting it has not received such requests, via either a data processing addendum or amendment to data processing addendum.
	d. Has the data importer been able to contest/minimize such disclosure of EU personal data, where appropriate?	Not applicable
	e. What types of EU personal data has the data importer been required to disclose to public authorities in its jurisdiction?	Not applicable
16.	How likely is it that the data importer will receive bulk data surveillance requests to disclose EU personal data to public	Unlikely. As a practical matter based on the nature of NAVEX Global's services, the types of

#	Factor	Response
	authorities in its jurisdiction in the future (e.g., based on factors such as the type of services provided and sector in which the data importer operates, its size, number of customers and reputation)?	personal data processed, and the absence of any prior requests received in the past, NAVEX Global believes it is extremely unlikely to receive requests from U.S. government agencies to obtain customer data for national security purposes or to participate in the types of U.S. bulk surveillance programs scrutinized by the CJEU in its recent ruling on data transfer mechanisms. We have no reason to believe we may receive such requests in the future.
17.	Does the data importer maintain annual reports or statistics regarding requests/demands received from law enforcement or intelligence agencies (e.g., number/type of requests/demands, requesting authority, etc.)?	Not applicable. NAVEX Global has not received a Section 702 FISA request, an EO 12.333 request or order, or a public authority request specifically targeting EU personal data under the SCCs. As a result, if we get such requests in the future, we will provide such statistics and update our TRA process and Public Authority Disclosure Policy accordingly.
18.	Does the data importer maintain a written procedure(s) for: 1. Responding to or challenging requests/ demands of law enforcement or intelligence agencies that apply to EU personal data? 4. Informing customers of requests/demands from law enforcement or intelligence agencies where permitted by applicable law?	Yes, please see our Public Authority Disclosure Request Policy.
19.	Are the data importer's commitments enabling data subjects to exercise their rights as provided in the SCCs thwarted by the laws and/or practices in the U.S. or can these rights be effectively applied in practice?	NAVEX Global has never encountered a situation where it felt it could not enable data subject rights, including judicial redress. We do not believe the laws subject to us prevent us from enabling, supporting, and fulfilling data subject rights under the SCCs.
Onward transfers and exposure to government surveillance		
20.	Does the data importer share EU personal data further with sub-processors whose processing takes place in third countries?	Yes. Only to its US affiliate.
21.	What measures does the third-party data recipient take to ensure the protection of EU personal data transferred to it?	NAVEX Global enters into written agreements with sub-processors that include safeguards for EU personal data in accordance with the GDPR requirements.
22.	What assurances has the data importer received from third-party data recipients with respect to requests/demands for EU personal data from [U.S./other jurisdiction] public authorities?	NAVEX Global has updated all written agreements with sub-processors to include additional measures for the protection of EU personal data, where required.

#	Factor	Response

Conclusion/Risk of transfers

Likely limited-risk data transfer

In particular, NAVEX Global identified the following factors (based on the assessment documented above and any additional information), that are likely to indicate a limited-risk transfer:

The data importer has never received requests/demands from intelligence services for disclosure of EU personal data.

The data importer has received limited requests/demands from public authorities for disclosure of EU personal data (such as for disclosure of employee data), but the requests related to regular criminal law procedure and did not go beyond what is necessary and proportionate to meet the purpose of the request.

The data importer has a process in place for handling and contesting public authority access requests, if received.

Based on the nature of its services and data processing activities, the data importer does not expect to be the target of requests/demands pursuant to national security or intelligence agencies for disclosure of EU personal data.

Such data transfers are not directly nor practically in scope of requests/demands from national security or intelligence agencies for disclosure of EU personal data.

D. Supplementary Measures

Notwithstanding the Conclusion set forth in the above TRA, NAVEX Global has also adopted the following supplemental measures. We believe that by implementing such supplemental measures, we are following best practices and are demonstrating our serious commitment to the protection of customer data.

Contractual safeguards	The SCCs themselves contain a number of contractual commitments by NAVEX Global and its customer, aimed at serving as safeguards for EU personal data.
	Supplementary contractual assurances are offered via our standard data processing addendum or an amendment to the data processing addendum. Please reach out to privacy@navexglobal.com in order to get this in place.
	NAVEX Global agrees to audit and monitor its obligations, and to support its customers auditing and monitoring obligations, regarding the level of government access to data.
	NAVEX Global provides a data processing agreement to support GDPR compliance, which includes the SCCs. As the data processor/importer, we process personal data strictly in accordance

	with your instructions and to provide the services. Our customers are the owners of the personal data within our service applications. NAVEX Global offers a Data Security Addendum, providing for contractual commitments to its information security program.
Organizational safeguards	NAVEX Global maintains written processes and procedures which provide for review of and limit the scope of EU personal data disclosed by NAVEX Global in response to requests from public authorities. Please see our Public Authority Disclosure Request Policy.
	NAVEX Global maintains internal record of requests made by public authorities concerning EU personal data.
	NAVEX Global takes steps to limit the volume of disclosed data, where possible.
	NAVEX Global would take data minimization measures such as redacting unnecessary identifiable personal data or personal data that may be of increased interest to intelligence agencies before complying with a request to disclosure EU personal data.
	NAVEX Global has developed the attached Standard Contractual Clauses Assurance Guide, which details our commitment to compliance with the SCCs. NAVEX Global remains a participant and has certified its compliance with the EU-U.S. Privacy Shield Framework and the Swiss- U.S. Privacy Shield Framework. NAVEX Global, Inc. is committed to subjecting all personal information received from the European Economic Area, United Kingdom, and Switzerland, respectively, in reliance on each Privacy Shield Framework, to the Frameworks' applicable Principles. To learn more about the Privacy Shield program, and to view our certification, please visit https://www.privacyshield.gov. NAVEX Global provides an independent recourse mechanism to EU individuals, currently TrustArc.
Technical safeguards	Encrypt personal data in transit.
	Encrypt personal data at rest.
	Appropriate access controls.

	Customers can implement data minimization (e.g., store the least amount of data necessary).
	Timespan for any access to personal data “in the clear” is limited to the specific function.
	Store personal data in the EU and enable only remote access.
	NAVEX Global equips its services with self-servicing functionality, allowing you to manage the personal data on your own through the use of the services. NAVEX Global engages a recognized, independent third party to conduct a Statement on Standards for Attestation Engagements No. 16, Service Organization Control 2, Type 2 (“SSAE 18 SOC 2 Type 2”) audit (or its equivalent or successor) of its information security program and its administrative, technical, and physical safeguards for all facilities used to deliver the Services, which specifically includes privacy controls. NAVEX Global maintains an annual Standardized Information Gathering Questionnaire (“SIG”), which details our robust security program with supporting documentation.

Conclusion

Having regard to the level of risk of the data transfer (**limited risk**), NAVEX Global considers that the measures identified above are **sufficient and effective** in light of the circumstances of the transfers, in conjunction with the supplementary measures and safeguards provided by the SCCs, to allow the data importer to comply with its obligations under the SCCs and provide an appropriate level of protection for the transfer.

Lockpath: EU Hosted

NAVEX GLOBAL

EU HOSTED LOCKPATH- EU/UK DATA TRANSFER RISK ASSESSMENTS

I. INTRODUCTION

NAVEX Global must conduct Transfer Risk Assessments ("TRA" or "TRAs") for transfers of personal data from the European Economic Area ("EEA")[6] or the United Kingdom ("UK") (collectively "EU personal data") to third countries that are not deemed to provide an adequate level of data protection.

II. SCOPE

These TRAs apply to NAVEX Global's EU Hosted Lockpath customers.

This TRA process applies to personal data transferred to NAVEX Global pursuant to the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council. This TRA is specifically designed to address Clause 14 of the foregoing set of Standard Contractual Clauses. Personal data from the UK is also in scope and shall be assessed pursuant to the European Commission's decision (C(2010)593) of 5 February 2010 on Standard Contractual Clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection. We collectively refer to the sets of Standard Contractual Clauses as the "SCCs." NAVEX Global agrees and acknowledges the UK will be issuing its own set of standard contractual clauses and related Schrems II guidance. We will update this TRA on an ongoing basis as needed.

This TRA process takes into account the European Data Protection Board's Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data adopted on 18 June 2021 (the "EDPB Guidance").

NAVEX Global has separate TRAs for its non-affiliate sub-processing activities, where NAVEX Global utilizes such sub-processors for the processing of personal data who receive customer EU personal data in third countries that have not been deemed adequate by the European Commission. These are available as part of our compliance documentation and on request.

This TRA is not intended for transfers (i) within the EEA, (ii) between the EEA and the UK, or (iii) from the EEA or UK to a country recognized by the European Commission or UK law as adequate at this time (i.e., Andorra, Argentina, Canada (commercial organizations subject to PIPEDA), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, UK, and Uruguay).

The TRA is completed by the NAVEX Global Privacy Team, which consists of the Data Privacy Officer & Senior Counsel, Senior Privacy Counsel, and Privacy Counsel.

III. ASSESSING THE ADEQUACY OF EU/UK DATA TRANSFERS – TO NAVEX GLOBAL IN THE U.S.

In assessing the adequacy of transfers of personal data from the EU/UK to NAVEX Global in the U.S. we have taken the following steps:

1. **STEP 1:** Identified the relevant data transfers and the legal mechanism that NAVEX Global is relying on for such transfers (e.g., SCCs).

2. **STEP 2:** Conducted due diligence and collected information about the scope of the transfers, the exposure of NAVEX Global to local law that may require disclosure of EU personal data about individuals, and any other relevant information.

[6] The European Economic Area consists of the Member States of the EU (Austria, Belgium, Bulgaria, Croatia, Cyprus, Czechia, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain and Sweden), plus Iceland, Liechtenstein and Norway.

3. **STEP 3:** Completed the "Transfer Risk Assessment" in **Section IV** to assess whether the SCCs is effective in light of all circumstances of the transfer.

4. **STEP 4:** Included additional "Supplementary Measures" as set forth in **Section IV (D)**.

5. **STEP 5:** Documented the assessment for accountability purposes. We encourage our customers to do the same.

6. **STEP 6:** NAVEX Global is responsible for the periodic review of the assessment, which should take place at least annually, to ensure that the transfer of the EU personal data continues to be afforded an adequate level of protection.

IV. TRANSFER RISK ASSESSMENT

Name Of Data Importer: NAVEX Global

Scope of TRA: Transfers to NAVEX Global's affiliates in the United States as part of the Lockpath Services provided to EU Hosted Customers

Completed By: NAVEX Global's Privacy Team

Date: 25 September 2021

A. Type of Data Importer

Name of data importer: NAVEX Global. The SCCs between customer and NAVEX Global is part of a master services agreement between customer and NAVEX Global UK Limited (registered in the UK) or GCS Compliance Services Europe Unlimited Company trading as NAVEX Global (registered in Ireland), both with their principal places of business at Vantage West – 4th floor, Great West Road, Brentford TW8 9AG, United Kingdom. Some EU Hosted customers elect to contract directly with our U.S. entity, NAVEX Global, Inc., a Delaware corporation with its principal place of business at 5500 Meadows Road, Suite 500, Lake Oswego, OR 97035.

Upon reviewing the broad definitions set forth within U.S. surveillance laws under scrutiny pursuant to the CJEU ruling in the Schrems II case, NAVEX Global identifies itself as follows:

NAVEX Global does not consider itself a "telecommunications carrier" as defined in 47 U.S.C. 152.

NAVEX Global acknowledges that certain of its services could be viewed by U.S. government authorities as an "electronic communication service" as defined in 18 U.S.C. 2510.

NAVEX Global acknowledges that certain of its services could be viewed by U.S. government authorities as a "remote computing service" as defined in 18 U.S.C. 2711.

NAVEX Global acknowledges that certain of its services could be viewed by U.S. government authorities as other communication services where there may be access to wire or electronic communications.

B. Details of Data Transfers

Data transfer mechanism Appropriate Controller to Processor SCCs between customer and NAVEX Global.
Scope of personal data covered by the data transfer mechanism in place The SCCs cover transfers of EU personal data from the EEA/UK to the U.S., including the following categories of data subjects: • Employees of data exporter • Clients, business partners and vendors of data exporter (who are natural persons) • Employees or contact persons of data exporters' third-party suppliers, business partners and vendors • Data exporter's users authorized by data exporter to use the relevant Service(s)

C. Transfer Risk Assessment

The table below aids identification and evaluation of risk factors in relation to the specific data transfer. The assessment of each risk factor is recorded in appropriate detail.

#	Factor	Response
Scope of the transfers		
1.	What is the type of transfer?	Remote access only by direct NAVEX Global personnel located in the U.S. to personal data stored in the EU. Personal data is not stored in the U.S. as part of this transfer.
2.	Is the transfer necessary?	Yes. NAVEX Global has critical resources located in the U.S., requiring access to the EU hosted database for the following purposes: • Support. General support cases that are submitted, depending on the case, may require access to customer data to address the issue at hand. To meet our service level commitments, U.S. support may be involved accordingly. This is mainly due to certain resource limitations based on location, an overflow of support cases, and time zone challenges. • Administrative Service Functions. There is certain work, for example setting up web pages, that does not necessarily require a deep level access, but for which can result in a transfer of personal data to the U.S. depending on the service need. • Technical Work and Product Management. Many of our technical and product specific resources are in the U.S. which requires access to customer data. Examples include certain data extract services, implementation and professional services, certain data migration services, integration services, user setups instances, and hosting installations. Again, depending on the task, we need the option to leverage

#	Factor	Response
		those resources which involves a certain level of access. • IT/Hosting. Select members of the hosting and information security group must have access for maintenance and troubleshooting. Without the above, our service level commitments would greatly suffer, and the overall maintenance and security of our service would be put at great risk.
3.	Is the transfer proportionate?	Yes. Access is not provided to personnel in the U.S. in a general sense. Access is provided to those personnel in the U.S. on a strict need to know basis to perform their given job function.
4.	Is the transfer occasional/non-routine or frequent/routine?	The transfer is non-routine to NAVEX Global personnel in the U.S. for the purposes detailed in Factor #2 above.
5.	Will the transferred personal data be processed for a relatively long or short period of time?	Personal data transferred to the U.S. in this context is processed for a relatively short period of time to provide the applicable service support.
6.	Is the transferred data encrypted and/ or pseudonymized?	Yes. NAVEX Global employs encryption at rest using either full-disk encryption or within the database using TDE. Data at rest will be encrypted using AES 256 or better, data in flight will be accomplished using TLS 1.2 or higher on public untrusted networks. Upon reviewing pseudonymization in the context of this transfer, it is inapplicable to the services we need to support.
Specific circumstances of the transfer		
7.	What are the purposes for which the data are transferred and processed?	To provide the best support, maintenance, and services as committed to in our agreements with our customers.
8.	What are the types of entities involved in the processing?	NAVEX Global is a data processor and a private company. Our customers are the data controllers and may consist of both private and public companies.

#	Factor	Response
9.	In which sector does the transfer occur?	NAVEX Global provides risk and compliance management SaaS based software. ***This factor is especially important as the purposes of our services is to enable organizations support their risk, ethics, and compliance programs. ***
10.	What are the categories of personal data transferred?	• Name (first and last), email address, log-in credentials, and other categories such as job title. ****No sensitive data, as defined under the GDPR, is transferred as part of the Lockpath services.****
11.	What is the format of the personal data to be transferred?	NAVEX Global employs encryption at rest using either full-disk encryption or within the database using TDE. Data at rest will be encrypted using AES 256 or better, data in flight will be accomplished using TLS 1.2 or higher on public untrusted networks. When access is provided to NAVEX Global personnel in the U.S. for the purposes described in this TRA, customer data must be accessible in the clear to provide the requisite support or service function.
12.	What is the storage location of the data transferred?	The European Union.
13.	What are the sub-processing activities?	Please see details here: https://www.navexglobal.com/en-us/service-hosting-providers. These are temporary and limited sub-processing activities. All requirements are flown down to each sub-processor.
Importer's exposure to government surveillance and practical application of Section 702 FISA		
14.	Is the data importer's sector or business directly subject to such laws in its jurisdiction that permit government access to personal data, or require the assistance of data importer to disclose personal data to public authorities, for surveillance and intelligence gathering purposes?	No. In our reasonable opinion upon internal and outside counsel review, we do not find NAVEX Global to be directly subject to such laws. As a practical matter based on the nature of NAVEX Global's services, the types of personal data processed, and the absence of any prior requests received in the past, NAVEX Global believes it is extremely unlikely to receive requests from U.S. government agencies to

#	Factor	Response
		obtain customer data for national security purposes or to participate in the types of U.S. bulk surveillance programs scrutinized by the CJEU in its recent ruling on data transfer mechanisms.
	a. Specifically, what is data importer's analysis regarding Section 702 FISA under the SCCs and EDPB Guidance?	1) Data exporters may decide to proceed with the transfer without supplementary measures, if they consider there to be no reason to believe that the relevant and problematic legislation (those in the U.S. in this instance) will be applied, in practice, to the transferred data and/or NAVEX Global. a. In our reasonable opinion upon internal and outside counsel review, we do not find U.S. surveillance laws, including Section 702 FISA, to practically apply to these transfers. b. It is important to note that given the broad definitions of these laws, the vast majority of organizations are going to have to acknowledge their potential application. However, this does not mean they directly apply or practically apply in practice. c. We believe NAVEX Global is generally out of scope and that these laws are overall not going to apply to the services we provide, as the intent is for surveillance of certain telecom and internet service providers for targeted information. This typically involves to surveillance of real time emails, texts, and chat conversations. The foregoing is not what NAVEX Global provides and to obtain this sought for information, authorities would pursue those providers directly as it would be impractical to make a request through NAVEX Global. 2) Data exporters may also take into consideration documented practical experience of data importer with relevant prior instances of requests for access received from public authorities in the U.S. a. ***To this point, NAVEX Global has never received a Section 702 FISA request or an EO 12.333 request or order. Please see our Public Authority Disclosure Request Policy for more details.** * b. The EDPB Guidance implies that the lack of requests received in the past plus no prohibition on providing

#	Factor	Response
		information about such requests, could be sufficient to conclude Section 702 FISA does not apply in practice. Note there is no prohibition on NAVEX Global to provide information about these requests. 3) If you conclude Section 702 FISA does not apply in practice to the particular transfer, it is possible to proceed with the transfer without any supplementary measures. **a. While NAVEX Global takes the approach that Section 702 FISA does not apply in practice, we still have elected to provide for supplementary measures with regard to these transfers. Please see Section IV (D).**
15.	Within the last three (3) years, has the data importer received requests/demands from public authorities in its jurisdiction to disclose EU personal data pursuant to the SCCs?	No.
	a. Approximately how many requests/demands from public authorities has the data importer received in that time period concerning EU personal data pursuant to the SCCs?	None.
	b. Approximately how many of these requests/demands are pursuant to criminal law procedure in the destination country? *[Regular court proceedings are not the issue under Schrems II, but intelligence programs are scrutinized.]*	****NAVEX Global has never received <u>ANY</u> requests for data pertaining to its Lockpath services. *** While NAVEX Global has not received requests from public authorities for EU personal data under the SCCs or otherwise, we have received a limited number of formal requests or demands from U.S. government **authorities concerning customer data pertaining to its hotline and incident management services**. These requests have been made in the context of criminal and civil actions in the form of a subpoena issued to NAVEX Global as a third party, by a state or federal court. In each instance, we've notified the customer straight away and they have directed us to comply with the subpoena. We've only fulfilled such requests with full customer clearance and direction on how to handle.
	c. Approximately how many of these requests/demands are pursuant to national security or intelligence agencies in the destination country?	None. The data importer can represent that it has not received requests/demands from intelligence agencies. NAVEX Global offers signed contracts, warranting it has not received such requests, via either a data processing addendum or amendment to data processing addendum.

#	Factor	Response
	d. Has the data importer been able to contest/minimize such disclosure of EU personal data, where appropriate?	Not applicable
	e. What types of EU personal data has the data importer been required to disclose to public authorities in its jurisdiction?	Not applicable
16.	How likely is it that the data importer will receive bulk data surveillance requests to disclose EU personal data to public authorities in its jurisdiction in the future (e.g., based on factors such as the type of services provided and sector in which the data importer operates, its size, number of customers and reputation)?	Unlikely. As a practical matter based on the nature of NAVEX Global's services, the types of personal data processed, and the absence of any prior requests received in the past, NAVEX Global believes it is extremely unlikely to receive requests from U.S. government agencies to obtain customer data for national security purposes or to participate in the types of U.S. bulk surveillance programs scrutinized by the CJEU in its recent ruling on data transfer mechanisms. We have no reason to believe we may receive such requests in the future.
17.	Does the data importer maintain annual reports or statistics regarding requests/demands received from law enforcement or intelligence agencies (e.g., number/type of requests/demands, requesting authority, etc.)?	Not applicable. NAVEX Global has not received requests from public authorities for EU personal data under the SCCs or otherwise. As a result, if we get such requests in the future, we will provide such statistics and update our TRA process and Public Authority Disclosure Policy accordingly.
18.	Does the data importer maintain a written procedure(s) for: 1. Responding to or challenging requests/demands of law enforcement or intelligence agencies that apply to EU personal data? 6. Informing customers of requests/demands from law enforcement or intelligence agencies where permitted by applicable law?	Yes, please see our Public Authority Disclosure Request Policy.
19.	Are the data importer's commitments enabling data subjects to exercise their rights as provided in the SCCs thwarted by the laws and/or practices in the U.S. or can these rights be effectively applied in practice?	NAVEX Global has never encountered a situation where it felt it could not enable data subject rights, including judicial redress. We do not believe the laws subject to us prevent us from enabling, supporting, and fulfilling data subject rights under the SCCs.
Onward transfers and exposure to government surveillance		
20.	Does the data importer share EU personal data further with sub-processors whose processing takes place in third countries?	Yes.
21.	What measures does the third-party data	

#	Factor	Response
	recipient take to ensure the protection of EU personal data transferred to it?	NAVEX Global enters into written agreements with sub-processors that include safeguards for EU personal data in accordance with the GDPR requirements.
22.	What assurances has the data importer received from third-party data recipients with respect to requests/demands for EU personal data from [U.S./other jurisdiction] public authorities?	NAVEX Global has updated, or is in the process of updating, all written agreements with sub-processors to include additional measures for the protection of EU personal data, where required.

Conclusion/Risk of transfers

Likely limited-risk data transfer

In particular, NAVEX Global identified the following factors (based on the assessment documented above and any additional information), that are likely to indicate a limited-risk transfer:

The data importer has never received requests/demands from intelligence services for disclosure of EU personal data.

The data importer has received limited requests/demands from public authorities for disclosure of EU personal data (such as for disclosure of employee data), but the requests related to regular criminal law procedure and did not go beyond what is necessary and proportionate to meet the purpose of the request.

The data importer has a process in place for handling and contesting public authority access requests, if received.

Based on the nature of its services and data processing activities, the data importer does not expect to be the target of requests/demands pursuant to national security or intelligence agencies for disclosure of EU personal data.

Such data transfers are not directly nor practically in scope of requests/demands from national security or intelligence agencies for disclosure of EU personal data.

D. Supplementary Measures

Notwithstanding the Conclusion set forth in the above TRA, NAVEX Global has also adopted the following supplemental measures. We believe that by implementing such supplemental measures, we are following best practices and are demonstrating our serious commitment to the protection of customer data.

Contractual safeguards	The SCCs themselves contain a number of contractual commitments by NAVEX Global and its customer, aimed at serving as safeguards for EU personal data.

	Supplementary contractual assurances are offered via our standard data processing addendum or an amendment to the data processing addendum. Please reach out to privacy@navexglobal.com in order to get this in place.
	NAVEX Global agrees to audit and monitor its obligations, and to support its customers auditing and monitoring obligations, regarding the level of government access to data.
	NAVEX Global provides a data processing agreement to support GDPR compliance, which includes the SCCs. As the data processor/importer, we process personal data strictly in accordance with your instructions and to provide the services. Our customers are the owners of the personal data within our service applications. NAVEX Global offers a Data Security Addendum, providing for contractual commitments to its information security program.
Organizational safeguards	NAVEX Global maintains written processes and procedures which provide for review of and limit the scope of EU personal data disclosed by NAVEX Global in response to requests from public authorities. Please see our Public Authority Disclosure Request Policy.
	NAVEX Global maintains internal record of requests made by public authorities concerning EU personal data.
	NAVEX Global takes steps to limit the volume of disclosed data, where possible.
	NAVEX Global would take data minimization measures such as redacting unnecessary identifiable personal data or personal data that may be of increased interest to intelligence agencies before complying with a request to disclosure EU personal data.
	NAVEX Global has developed the attached Standard Contractual Clauses Assurance Guide, which details our commitment to compliance with the SCCs. NAVEX Global remains a participant and has certified its compliance with the EU-U.S. Privacy Shield Framework and the Swiss- U.S. Privacy Shield Framework. NAVEX Global, Inc. is committed to subjecting all personal information received from the European Economic Area, United Kingdom, and Switzerland, respectively, in reliance on each Privacy Shield Framework, to the Frameworks' applicable Principles. To learn more about the Privacy Shield program, and to view our certification, please visit https://www.privacyshield.gov.

	NAVEX Global provides an independent recourse mechanism to EU individuals, currently TrustArc.
Technical safeguards	Encrypt personal data in transit.
	Encrypt personal data at rest.
	Appropriate access controls.
	Customers can implement data minimization (e.g., store the least amount of data necessary).
	Timespan for any access to personal data "in the clear" is limited to the specific function.
	Store personal data in the EU and enable only remote access.
	NAVEX Global equips its services with self-servicing functionality, allowing you to manage the personal data on your own through the use of the services. NAVEX Global engages a recognized, independent third party to conduct a Statement on Standards for Attestation Engagements No. 16, Service Organization Control 2, Type 2 ("SSAE 18 SOC 2 Type 2") audit (or its equivalent or successor) of its information security program and its administrative, technical, and physical safeguards for all facilities used to deliver the Services, which specifically includes privacy controls. NAVEX Global maintains an annual Standardized Information Gathering Questionnaire ("SIG"), which details our robust security program with supporting documentation.

Conclusion

Having regard to the level of risk of the data transfer (**limited risk**), NAVEX Global considers that the measures identified above are **sufficient and effective** in light of the circumstances of the transfers, in conjunction with the supplementary measures and safeguards provided by the SCCs, to allow the data importer to comply with its obligations under the SCCs and provide an appropriate level of protection for the transfer.

Lockpath EU Hosted Sub-processing Activity: IPaaS Connector Services with Workato

NAVEX GLOBAL SUB-PROCESSING ACTIVITY

EU HOSTED LOCKPATH SERVICES – WORKATO SERVICES

I. SCOPE

This TRA applies to NAVEX Global's EU Hosted Lockpath customers. This TRA applies specifically to the services provided by Workato.

As part of NAVEX Global's Lockpath services, Workato provides software products and services relating to enterprise integration platforms to integrate and automate tasks across on-premise, cloud apps and databases.

Workato's capabilities and functions are more fully described at docs.workato.com and specifically include:

1. A low-code/no-code online editor for visually designing and editing integration processes ("recipes").
2. Connection facilities to a wide range of 3rd-party applications, systems and services.
3. The ability to execute recipes and thus enable data flow between applications.
4. Monitoring and management facilities including a history of jobs processed on the platform.
5. Management facilities for controlling user access and permissions.
6. The ability to embed Workato functionality within data exporter's own applications.

II. ASSESSING THE ADEQUACY OF EU/UK DATA TRANSFERS – WORKATO SERVICES

In assessing the adequacy of transfers of personal data from the EU/UK to NAVEX Global's sub-processor pursuant to the services provided by said sub-processor, we have taken the following steps:

1. **STEP 1:** Identified the relevant data transfers and the legal mechanism that NAVEX Global and sub-processor is relying on for such transfers (e.g., SCCs).

2. **STEP 2:** Conducted due diligence and collected information about the scope of the transfers, the exposure of the sub-processor to local law that may require disclosure of EU personal data about individuals, and any other relevant information.

3. **STEP 3:** Completed the "Transfer Risk Assessment" in **Section IV** to assess whether the SCCs is effective in light of all circumstances of the transfer.

4. **STEP 4:** Included additional "Supplementary Measures" as set forth in **Section IV (D)**.

5. **STEP 5:** Documented the assessment for accountability purposes. We encourage our customers to do the same.

6. **STEP 6:** NAVEX Global and its sub-processor is responsible for the periodic review of the assessment, which should take place at least annually, to ensure that the transfer of the EU personal data continues to be afforded an adequate level of protection.

III. TRANSFER RISK ASSESSMENT

Name Of Data Importer: Workato, Inc. **(**NAVEX Global's sub-processor)
Completed By: NAVEX Global's Privacy Team and Workato's Chief Information Security Officer
Date: 25 September 2021

A. Type of Data Importer

Name of data importer: Workato, Inc. ("Workato"). The Processor to Processor SCCs between NAVEX Global and Workato is part of a master services agreement between NAVEX Global and Workato.

Does Workato provide the following services to NAVEX Global:

	Data Importer	
Telecommunications	☐ Yes	☒ No
Other electronic communications (such as an Internet Service Provider or a provider of email, text message, VoIP, remote desktop or VPN services)?	☐ Yes	☒ No
Remote computing services	☒ Yes	☐ No
Other communications service where there may be access to wire or electronic communications	☐ Yes	☒ No

B. Details of Data Transfers

Data transfer mechanism

Appropriate Processor to Processor SCCs between Workato and NAVEX Global.

Scope of personal data covered by the data transfer mechanism in place

The SCCs cover transfers of EU personal data from the EEA/UK to the U.S., including the following categories of data subjects:

- Employees of customer Data Controller
- Clients, business partners and vendors of customer Data Controller (who are natural persons)
- Employees or contact persons of customer Data Controllers' third-party suppliers, business partners and vendors
- Customer Data Controller's users authorized to use the relevant Service(s)

C. Transfer Risk Assessment

The table below aids identification and evaluation of risk factors in relation to the specific data transfer. The assessment of each risk factor is recorded in appropriate detail.

#	Factor	Response
Scope of the transfers		
1.	What is the type of transfer?	Data is processed in accordance with the Data exporter's or controller's instructions, generally delivered via online configuration options and APIs provided to authorized users of the Data importer's platform.
2.	Is the transfer necessary?	Yes, in order to deliver the services requested by the customer Data Controller.
3.	Is the transfer proportionate?	Yes, data is transferred and processed solely for the specified service and in accordance with Processor's instructions.
4.	Is the transfer occasional/non-routine or frequent/routine?	This is dependent upon the customer Data Controller's use of the services and for the term of the commercial agreement between Navex and Workato.
5.	Will the transferred personal data be processed for a relatively long or short period of time?	Retention is limited and under NAVEX Global and Data Controller control: 30 days default.
6.	Is the transferred data encrypted, pseudonymized or otherwise processed in an unintelligible form, during all stages of the processing (i.e., in transit, in rest and while in use)?	Yes, All data is encrypted both in transit and at rest using industry-standard encryption technologies. In addition, the data importer provides as an option the ability to mask sensitive data from display and to restrict its retention on the platform. Display masking is applied automatically to certain data including passwords and keys.
Specific circumstances of the transfer		
7.	What are the purposes for which the data are transferred and processed?	Workato provides a flexible business integration and automation service. Data submitted by NAVEX Global's customers may be transferred onwards to one or more business applications or systems, under the control of NAVEX Global and Data Controller.
8.	What are the types of entities involved in the processing?	Workato is a data sub-processor and a private company. NAVEX Global is a data processor and private company. NAVEX Global's customers are the data controllers and may consist of both private and public companies.

#	Factor	Response
9.	In which sector does the transfer occur?	NAVEX Global provides risk and compliance management SaaS based software. ***This factor is especially important as the purposes of our services is to enable organizations support their risk, ethics, and compliance programs. ***
10.	What are the categories of personal data transferred?	• name, job title, job position, location, employer, relationship with the organization, e-mail address, telephone number; • Third party application data provided at the customer Data Controller's election depending on the Services' use case, as detailed in an agreement between Data exporter and the customer Data Controller • Other categories of data may be processed at the customer Data Controller's election depending on the Services' use case, as detailed in an agreement between Data exporter and the customer Data Controller • In the event customer Data controller whistle-blower hotline and incident management report data is processed, strictly as elected by the customer Data Controller, the following may also be captured: o facts reported by a reporter about a suspected violation, including how and where the suspected violation occurred and how the reporter learned about the suspected violation; o identity, function and contact details of individuals allegedly involved in the suspected violation; and o identity, function and contact details of individuals who could provide information relating to the suspected violation. Given the nature of incident management services, reporters may submit sensitive categories of data in a report. NAVEX Global recommends its customers have strict policies around the management of such report data in their use of the services, in accordance with the laws subject to them.
11.	What is the format of the personal data to be transferred?	Under the control of the customer Data Controller and may be in various formats.

#	Factor	Response
12.	What is the storage location of the data transferred?	The United States via Workato temporarily. Ultimately stored in NAVEX Global's secure data centres in the European Union.
13.	What are the sub-sub-processing activities?	See https://www.workato.com/legal/sub-processors.
Importer's exposure to government surveillance and practical application of Section 702 FISA		
14.	Is the data importer's sector or business directly subject to such laws in its jurisdiction that permit government access to personal data, or require the assistance of data importer to disclose personal data to public authorities, for surveillance and intelligence gathering purposes?	No. Workato's business is currently not directly subject to such laws.
	a. Specifically, what is data importer's analysis regarding Section 702 FISA under the SCCs and EDPB Guidance?	1) Data exporters may decide to proceed with the transfer without supplementary measures, if they consider there to be no reason to believe that the relevant and problematic legislation (those in the U.S. in this instance) will be applied, in practice, to the transferred data and/or Workato. a. In our reasonable opinion upon internal and outside counsel review, we do not find U.S. surveillance laws, including Section 702 FISA, to practically apply to these transfers. b. It is important to note that given the broad definitions of these laws, the vast majority of organizations are going to have to acknowledge their potential application. However, this does not mean they directly apply or practically apply in practice. c. We believe Workato is generally out of scope and that these laws are overall not going to apply to the services we provide, as the intent is for surveillance of certain telecom and internet service providers for targeted information. This typically involves to surveillance of real time emails, texts, and chat conversations. The foregoing is not what Workato provides and in order to obtain this sought for information, authorities would pursue those providers directly as it would be impractical to make a request through Workato.

#	Factor	Response
		2) Data exporter may also take into consideration documented practical experience of data importer with relevant prior instances of requests for access received from public authorities in the U.S. a. To this point, Workato has never received a Section 702 FISA request or an EO 12.333 request or order. b. The EDPB Guidance implies that the lack of requests received in the past plus no prohibition on providing information about such requests, could be sufficient to conclude Section 702 FISA does not apply in practice. Note there is no prohibition on Workato to provide information about these requests. 3) If you conclude Section 702 FISA does not apply in practice to the particular transfer, it is possible to proceed with the transfer without any supplementary measures. While NAVEX Global and Workato take the approach that Section 702 FISA does not apply in practice, we still have elected to provide for supplementary measures with regard to these transfers. Please see Section IV (D).
15.	Within the last three (3) years, has the data importer received requests/demands from public authorities in its jurisdiction to disclose EU personal data?	Based on available information, Workato entities do not receive requests/demands for disclosure of, or access to, EU personal data in the US or elsewhere.
	a. Approximately how many requests/demands from public authorities has the data importer received in that time period concerning EU personal data?	None, to the best of our knowledge.
	b. Approximately how many of these requests/demands are pursuant to criminal law procedure in the destination country? *[Regular court proceedings are not the issue under Schrems II, but intelligence programs are scrutinized.]*	None, to the best of our knowledge.
	c. Approximately how many of these requests/demands are pursuant to national security or intelligence agencies in the destination country?	None, to the best of our knowledge. The data importer can represent that it has not received requests/demands from intelligence agencies.
	d. Has the data importer been able to contest/minimize such disclosure of EU personal data, where appropriate?	Not applicable

#	Factor	Response
	e. What types of EU personal data has the data importer been required to disclose to public authorities in its jurisdiction?	Not applicable
16.	How likely is it that the data importer will receive bulk data surveillance requests to disclose EU personal data to public authorities in its jurisdiction in the future (e.g., based on factors such as the type of services provided and sector in which the data importer operates, its size, number of customers and reputation)?	Unlikely. Workato is a SaaS provider. We are not in the types of businesses, such as telecommunication providers, which are commonly subject to such requests.
17.	Does the data importer maintain annual reports or statistics regarding requests/demands received from law enforcement or intelligence agencies (e.g., number/type of requests/demands, requesting authority, etc.)?	Workato maintains records but not annual statistics. Workato has not received any requests thus far. We anticipate that we'll receive them on rare occasions given the nature of our business.
18.	Does the data importer maintain a written procedure(s) for: 1. Responding to or challenging requests/ demands of law enforcement or intelligence agencies that apply to EU personal data? 7. Informing customers of requests/demands from law enforcement or intelligence agencies where permitted by applicable law?	Workato does not currently have a written policy because no requests have been received. We fully commit to evaluate such requests on a case by case basis in accordance with our agreements with NAVEX Global. Workato and NAVEX Global entered into a contractual agreement requiring Workato to cooperate and mutually agree on any appropriate actions, to notify NAVEX Globalof any requests unless explicitly required otherwise under applicable law, to put any access request on hold, and to use reasonable efforts to obtain the right to waive any notice prohibitions and oppose any such request and contest its legal validity where possible and permitted. The contract additionally ensures Workato will not make any disclosures that are determined to be massive, disproportionate, and indiscriminate in a manner that would go beyond what is necessary in a democratic society. Workato is obliged to document and demonstrate to the assessments made and the actions taken. Workato undertakes to regularly review, assess, and continuously monitor the scope of the access to personal data by public authorities in the countries where Workato is processing personal data, as well as the safeguards and recourses in place to protect data subjects, and to immediately inform NAVEX Global in the case of a change in applicable law that would materially impact such access by public authorities or recourses available to data subjects.
19.	Are the data importer's commitments enabling data subjects to exercise their rights as provided in the SCCs thwarted by the laws and/or practices in the U.S. and any other third countries involved, or can these rights	Workato does not believe that U.S. laws limit its ability to fulfill such requests.

#	Factor	Response
	be effectively applied in practice?	
Onward transfers and exposure to government surveillance		
20.	Does the data importer share EU personal data further with third-party data recipients in [the U.S./other jurisdiction]?	Yes. See https://www.workato.com/legal/sub-processors.
21.	What measures does the third-party data recipient take to ensure the protection of EU personal data transferred to it?	Where Workto engages sub-processors that have access to EU personal data, Workato enters into written agreements with sub-processors that include safeguards for EU personal data in accordance with the GDPR requirements.
22.	What assurances has the data importer received from third-party data recipients with respect to requests/demands for EU personal data from [U.S./other jurisdiction] public authorities?	Workato will update written agreements with sub-processors to include additional measures for the protection of EU personal data, where required by applicable law or regulation(s). Workato has current agreements in place with such sub-processors for the protection of EU personal data under applicable law.
23.	Is the vendor's (or its sub-processor's) sector or business directly subject to such laws in its jurisdiction that permit government access to personal data, or require the assistance of data importer to disclose personal data to public authorities, for surveillance and intelligence gathering purposes?	Generally no, but we may be considered a "remote computing service" under 18 U.S. Code § 2711 given the broad definition.

Conclusion/Risk of transfers

Very limited-risk data transfer

In particular, Workato and NAVEX Global identified the following factors (based on the assessment documented above and any additional information), that are likely to indicate a very limited-risk transfer:

The data importer has never received requests/demands from intelligence services for disclosure of EU personal data.

In the unlikely event that Workato receives such request(s), the Privacy team will review them with the Legal team and to seek counsel on how to respond and will coordinate the response with all stakeholders and the requesting legal authorities.

Based on the nature of its services and data processing activities, the data importer does not expect to be the target of requests/demands pursuant to national security or intelligence agencies for disclosure of EU personal data.

Such data transfers are not directly nor practically in scope of requests/demands from national security or intelligence agencies for disclosure of EU personal data.

D. Supplementary Measures

Notwithstanding the Conclusion set forth in the above TRA, Workato has also adopted the following supplemental measures. We believe that by implementing such supplemental measures, we are following best practices and are demonstrating our serious commitment to the protection of customer data.

Contractual safeguards	Workato and NAVEX Global have entered into supplementary contractual assurances as part of the data processing addendum.
	The SCCs themselves contain a number of contractual commitments by Workato and NAVEX Global, aimed at serving as safeguards for EU personal data. We have also entered into a robust general data processing addendum.
Organizational safeguards	Workato maintains written processes and procedures provide for review of and limit the scope of EU personal data disclosed by Workato in response to requests from public authorities.
	Workato maintains internal record of requests made by public authorities concerning EU personal data.
	Workato takes steps to limit the volume of disclosed data, where possible.
	Workato take data minimization measures such as redacting unnecessary identifiable personal data or personal data that may be of increased interest to intelligence agencies before complying with a request to disclosure EU personal data.
Technical safeguards	Encrypt personal data in transit.
	Encrypt personal data at rest.
	Appropriate access controls.
	Limit timespan for using personal data "in the clear" (i.e., in identifiable form).
	Mask stored personal data.
	Enable only remote access or view-only access.

Conclusion

Having regard to the level of risk of the data transfer (**very limited risk**), Workato and NAVEX Global consider that the measures identified above are **sufficient and effective** in light of the circumstances of the transfers, in

conjunction with the supplementary measures and safeguards provided by the SCCs, to allow the data importer to comply with its obligations under the SCCs and provide an appropriate level of protection for the transfer.

Hotline and Incident Management: US Hosted

NAVEX GLOBAL

US HOSTED HOTLINE AND INCIDENT MANAGEMENT - EU/UK DATA TRANSFER RISK ASSESSMENTS

I. INTRODUCTION

NAVEX Global must conduct Transfer Risk Assessments ("TRA" or "TRAs") for transfers of personal data from the European Economic Area ("EEA")[7] or the United Kingdom ("UK") (collectively "EU personal data") to third countries that are not deemed to provide an adequate level of data protection.

II. SCOPE

These TRAs apply to NAVEX Global's US Hosted Hotline and Incident Management customers*.

This TRA process applies to personal data transferred to NAVEX Global pursuant to the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council. This TRA is specifically designed to address Clause 14 of the foregoing set of Standard Contractual Clauses. Personal data from the UK is also in scope and shall be assessed pursuant to the European Commission's decision (C(2010)593) of 5 February 2010 on Standard Contractual Clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection. We collectively refer to the sets of Standard Contractual Clauses as the "SCCs." NAVEX Global agrees and acknowledges the UK will be issuing its own set of standard contractual clauses and related Schrems II guidance. We will update this TRA on an ongoing basis as needed.

This TRA process takes into account the European Data Protection Board's Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data adopted on 18 June 2021 (the "EDPB Guidance").

NAVEX Global has separate TRAs for its non-affiliate sub-processing activities, where NAVEX Global utilizes such sub-processors for the processing of personal data who receive customer EU personal data in third countries that have not been deemed adequate by the European Commission. These are available as part of our compliance documentation and on request.

This TRA is not intended for transfers (i) within the EEA, (ii) between the EEA and the UK, or (iii) from the EEA or UK to a country recognized by the European Commission or UK law as adequate at this time (i.e., Andorra, Argentina, Canada (commercial organizations subject to PIPEDA), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, UK, and Uruguay).

The TRA is completed by the NAVEX Global Privacy Team, which consists of the Data Privacy Officer & Senior Counsel, Deputy Data Privacy Officer & Senior Counsel, and Privacy Counsel.

**Hotline and Incident Management (HLIM) consists of either AlertLine/Integrlink or EthicsPoint. NAVEX Global is decommissioning AlertLine/Integrilink as a legacy product. These TRAs apply generally to both services, however, for the most enhanced functionality, we recommend AlertLine/Integrlink customers migrate to EthicsPoint. All AlertLine/Integrilink customers will be asked to migrate in the near future.*

[7] The European Economic Area consists of the Member States of the EU (Austria, Belgium, Bulgaria, Croatia, Cyprus, Czechia, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain and Sweden), plus Iceland, Liechtenstein and Norway.

III. ASSESSING THE ADEQUACY OF EU/UK DATA TRANSFERS – TO NAVEX GLOBAL IN THE U.S.

In assessing the adequacy of transfers of personal data from the EU/UK to NAVEX Global in the U.S. we have taken the following steps:

1. **STEP 1:** Identified the relevant data transfers and the legal mechanism that NAVEX Global is relying on for such transfers (e.g., SCCs).

2. **STEP 2:** Conducted due diligence and collected information about the scope of the transfers, the exposure of NAVEX Global to local law that may require disclosure of EU personal data about individuals, and any other relevant information.

3. **STEP 3:** Completed the "Transfer Risk Assessment" in **Section IV** to assess whether the SCCs is effective in light of all circumstances of the transfer.

4. **STEP 4:** Included additional "Supplementary Measures" as set forth in **Section IV (D)**.

5. **STEP 5:** Documented the assessment for accountability purposes. We encourage our customers to do the same.

6. **STEP 6:** NAVEX Global is responsible for the periodic review of the assessment, which should take place at least annually, to ensure that the transfer of the EU personal data continues to be afforded an adequate level of protection.

IV. TRANSFER RISK ASSESSMENT

Name Of Data Importer: NAVEX Global
Scope of TRA: Transfers to NAVEX Global in the United States as part of the Hotline and Incident Management Services provided to US Hosted Customers

****Our customers elect the hosting and storage location. As a result, NAVEX Global has many customers subject to the GDPR on our US hosted and storage configuration, as chosen by the customer.****

Completed By: NAVEX Global's Privacy Team
Date: 25 September 2021

A. Type of Data Importer

Name of data importer: NAVEX Global. The SCCs between customer and NAVEX Global is part of a master services agreement between customer and NAVEX Global, Inc., a Delaware corporation, having its principal place of business at 5500 Meadows Road, Suite 500, Lake Oswego, Oregon 97035.

Upon reviewing the broad definitions set forth within U.S. surveillance laws under scrutiny pursuant to the CJEU ruling in the Schrems II case, NAVEX Global identifies itself as follows:

NAVEX Global does not consider itself a "telecommunications carrier" as defined in 47 U.S.C. 152.

NAVEX Global acknowledges that certain of its services could be viewed by U.S. government authorities as an "electronic communication service" as defined in 18 U.S.C. 2510.

NAVEX Global acknowledges that certain of its services could be viewed by U.S. government authorities as a "remote computing service" as defined in 18 U.S.C. 2711.

NAVEX Global acknowledges that certain of its services could be viewed by U.S. government authorities as other communication services where there may be access to wire or electronic communications.

B. Details of Data Transfers

Data transfer mechanism Appropriate Controller to Processor SCCs between customer and NAVEX Global.
Scope of personal data covered by the data transfer mechanism in place The SCCs cover transfers of EU personal data from the EEA/UK to the U.S., including the following categories of data subjects: • Employees of data exporter • Clients, business partners and vendors of data exporter (who are natural persons) • Employees or contact persons of data exporters' third-party suppliers, business partners and vendors • Data exporter's users authorized by data exporter to use the relevant Service(s)

C. Transfer Risk Assessment

The table below aids identification and evaluation of risk factors in relation to the specific data transfer. The assessment of each risk factor is recorded in appropriate detail.

#	Factor	Response
Scope of the transfers		
1.	What is the type of transfer?	EU personal data is stored and hosted within the U.S. NAVEX Global's hosting providers either cannot or do not access EU personal data. Select NAVEX Global personnel have access to provision the services in accordance with our agreements, subject to the principle of least privilege and our access control policies and processed.
2.	Is the transfer necessary?	Yes. NAVEX Global's customers elect their storage and hosting location. Many customers choose and prefer the U.S. For NAVEX Global to securely store the data in the U.S. as elected by the customer, they must transfer the data to this location via the services. For NAVEX Global to be able to provide the services, our personnel must be able to access the systems to provide support, administrative functions, contact centre services, technical work, and IT/Hosting support. Without the above, we wouldn't be able to provide the services or meet our service level commitments.
3.	Is the transfer proportionate?	Yes. The reports are submitted from either the phone or the web intake site to customer's case management system for them to manage directly. The data is securely stored and NAVEX Global processes data to maintain the services and in accordance with its customer's instructions.
4.	Is the transfer occasional/non-routine or frequent/routine?	The transfer is frequent/routine. This is necessary in order to host, store, and provide the services from the U.S. as requested.
5.	Will the transferred personal data be processed for a relatively long or short period	During the life of the agreement, the customer

#	Factor	Response
	of time?	decides how long to maintain the personal data in the system in accordance with their own policies and processes. NAVEX Global maintains the personal data within the services, as elected by the customer, for the duration of the agreement.
6.	Is the transferred data encrypted and/ or pseudonymized?	Yes. NAVEX Global employs encryption at rest using either full-disk encryption or within the database using TDE. Data at rest will be encrypted using AES 256 or better, data in flight will be accomplished using TLS 1.2 or higher on public untrusted networks. Upon reviewing pseudonymization in the context of this transfer, it is inapplicable to the services we need to support.
Specific circumstances of the transfer		
7.	What are the purposes for which the data are transferred and processed?	To securely store the data in the U.S. as requested by our customers. To provide the best support, maintenance, and services as committed to in our agreements with our customers.
8.	What are the types of entities involved in the processing?	NAVEX Global is a data processor and a private company. Our customers are the data controllers and may consist of both private and public companies.
9.	In which sector does the transfer occur?	NAVEX Global provides risk and compliance management SaaS based software. ***This factor is especially important as the purposes of our services is to enable organizations support their risk, ethics, and compliance programs. ***
10.	What are the categories of personal data transferred?	As instructed by NAVEX Global's customer, including but not limited to: • name, job title, job position, location, employer, relationship with the organization, e-mail address, telephone number, log-in credentials, date of birth; • for whistle-blower hotline and incident management reports, in addition to the foregoing, the following may also be

#	Factor	Response
		captured: o facts reported by a reporter about a suspected violation, including how and where the suspected violation occurred and how the reporter learned about the suspected violation; o identity, function and contact details of individuals allegedly involved in the suspected violation; and o identity, function and contact details of individuals who could provide information relating to the suspected violation. Given the nature of incident management services, our customers, reporters, or authorized users of the services may submit sensitive categories of data to their case management systems. We recommend our customers have strict policies around the management of such report data in their use of the services, in accordance with the laws subject to them.
11.	What is the format of the personal data to be transferred?	NAVEX Global employs encryption at rest using either full-disk encryption or within the database using TDE. Data at rest will be encrypted using AES 256 or better, data in flight will be accomplished using TLS 1.2 or higher on public untrusted networks. When access is provided to NAVEX Global personnel in the U.S. for the purposes described in this TRA, customer data must be accessible in the clear to provide the requisite support or service function.
12.	What is the storage location of the data transferred?	The United States.
13.	What are the sub-processing activities?	Please see details here: https://www.navexglobal.com/en-us/service-hosting-providers. These are temporary and limited sub-processing activities. All requirements are flown down to each sub-processor.
Importer's exposure to government surveillance and practical application of Section 702 FISA		
14.	Is the data importer's sector or business directly subject to such laws in its jurisdiction that permit government access to personal data, or require the assistance of data importer to disclose personal data to public	No. In our reasonable opinion upon internal and outside counsel review, we do not find NAVEX Global to be directly subject to such laws. As a practical matter based on the nature of NAVEX

#	Factor	Response
	authorities, for surveillance and intelligence gathering purposes?	Global's services, the types of personal data processed, and the absence of any prior requests received in the past, NAVEX Global believes it is extremely unlikely to receive requests from U.S. government agencies to obtain customer data for national security purposes or to participate in the types of U.S. bulk surveillance programs scrutinized by the CJEU in its recent ruling on data transfer mechanisms.
	c. Specifically, what is data importer's analysis regarding Section 702 FISA under the SCCs and EDPB Guidance?	1) Data exporters may decide to proceed with the transfer without supplementary measures, if they consider there to be no reason to believe that the relevant and problematic legislation (those in the U.S. in this instance) will be applied, in practice, to the transferred data and/or NAVEX Global. a. In our reasonable opinion upon internal and outside counsel review, we do not find U.S. surveillance laws, including Section 702 FISA, to practically apply to these transfers. b. It is important to note that given the broad definitions of these laws, the vast majority of organizations are going to have to acknowledge their potential application. However, this does not mean they directly apply or practically apply in practice. c. We believe NAVEX Global is generally out of scope and that these laws are overall not going to apply to the services we provide, as the intent is for surveillance of certain telecom and internet service providers for targeted information. This typically involves to surveillance of real time emails, texts, and chat conversations. The foregoing is not what NAVEX Global provides and in order to obtain this sought for information, authorities would pursue those providers directly as it would be impractical to make a request through NAVEX Global. 2) Data exporters may also take into consideration documented practical experience of data importer with relevant prior instances of requests for access received from public authorities in the U.S. a. ***To this point, NAVEX Global has never received a Section 702 FISA request or an EO 12.333 request or order. Please see our**

#	Factor	Response
		Public Authority Disclosure Request Policy for more details. * b. The EDPB Guidance implies that the lack of requests received in the past plus no prohibition on providing information about such requests, could be sufficient to conclude Section 702 FISA does not apply in practice. Note there is no prohibition on NAVEX Global to provide information about these requests. 3) If you conclude Section 702 FISA does not apply in practice to the particular transfer, it is possible to proceed with the transfer without any supplementary measures. **a. While NAVEX Global takes the approach that Section 702 FISA does not apply in practice, we still have elected to provide for supplementary measures with regard to these transfers. Please see Section IV (D).**
15.	Within the last three (3) years, has the data importer received requests/demands from public authorities in its jurisdiction to disclose EU personal data pursuant to the SCCs?	No, not to the best of our knowledge.
	a. Approximately how many requests/demands from public authorities has the data importer received in that time period concerning EU personal data pursuant to the SCCs?	None, to the best of our knowledge.
	b. Approximately how many of these requests/demands are pursuant to criminal law procedure in the destination country? *[Regular court proceedings are not the issue under Schrems II, but intelligence programs are scrutinized.]*	While NAVEX Global has not received a Section 702 FISA request, an EO 12.333 request or order, or a public authority request specifically targeting EU personal data under the SCCs, we have received a limited number of formal requests or demands from U.S. government authorities concerning customer data. These requests have been made in the context of criminal and civil actions in the form of a subpoena issued to NAVEX Global as a third party, by a state or federal court. In each instance, we've notified the customer straight away and they have directed us to comply with the subpoena. We've only fulfilled such requests with full customer clearance and direction on how to handle.
	c. Approximately how many of these requests/demands are pursuant to national security or intelligence agencies in the destination country?	None, to the best of our knowledge. The data importer can represent that it has not received requests/demands from intelligence agencies. NAVEX Global offers signed contracts, warranting it has not received such requests, via either a data processing addendum or amendment to data processing addendum.

#	Factor	Response
	d. Has the data importer been able to contest/minimize such disclosure of EU personal data, where appropriate?	Not applicable
	e. What types of EU personal data has the data importer been required to disclose to public authorities in its jurisdiction?	Not applicable
16.	How likely is it that the data importer will receive bulk data surveillance requests to disclose EU personal data to public authorities in its jurisdiction in the future (e.g., based on factors such as the type of services provided and sector in which the data importer operates, its size, number of customers and reputation)?	Unlikely. As a practical matter based on the nature of NAVEX Global's services, the types of personal data processed, and the absence of any prior requests received in the past, NAVEX Global believes it is extremely unlikely to receive requests from U.S. government agencies to obtain customer data for national security purposes or to participate in the types of U.S. bulk surveillance programs scrutinized by the CJEU in its recent ruling on data transfer mechanisms. We have no reason to believe we may receive such requests in the future.
17.	Does the data importer maintain annual reports or statistics regarding requests/demands received from law enforcement or intelligence agencies (e.g., number/type of requests/demands, requesting authority, etc.)?	Not applicable. NAVEX Global has not received a Section 702 FISA request, an EO 12.333 request or order, or a public authority request specifically targeting EU personal data under the SCCs. As a result, if we get such requests in the future, we will provide such statistics and update our TRA process and Public Authority Disclosure Policy accordingly.
18.	Does the data importer maintain a written procedure(s) for: 1. Responding to or challenging requests/ demands of law enforcement or intelligence agencies that apply to EU personal data? 4. Informing customers of requests/demands from law enforcement or intelligence agencies where permitted by applicable law?	Yes, please see our Public Authority Disclosure Request Policy.
19.	Are the data importer's commitments enabling data subjects to exercise their rights as provided in the SCCs thwarted by the laws and/or practices in the U.S. or can these rights be effectively applied in practice?	NAVEX Global has never encountered a situation where it felt it could not enable data subject rights, including judicial redress. We do not believe the laws subject to us prevent us from enabling, supporting, and fulfilling data subject rights under the SCCs.
Onward transfers and exposure to government surveillance		
20.	Does the data importer share EU personal data further with sub-processors whose processing takes place in third countries?	Yes.
21.	What measures does the third-party data	

#	Factor	Response
	recipient take to ensure the protection of EU personal data transferred to it?	NAVEX Global enters into written agreements with sub-processors that include safeguards for EU personal data in accordance with the GDPR requirements.
22.	What assurances has the data importer received from third-party data recipients with respect to requests/demands for EU personal data from [U.S./other jurisdiction] public authorities?	NAVEX Global has updated, or is in the process of updating, all written agreements with sub-processors to include additional measures for the protection of EU personal data, where required.

Conclusion/Risk of transfers

Likely limited-risk data transfer

In particular, NAVEX Global identified the following factors (based on the assessment documented above and any additional information), that are likely to indicate a limited-risk transfer:

The data importer has never received requests/demands from intelligence services for disclosure of EU personal data.

The data importer has received limited requests/demands from public authorities for disclosure of EU personal data (such as for disclosure of employee data), but the requests related to regular criminal law procedure and did not go beyond what is necessary and proportionate to meet the purpose of the request.

The data importer has a process in place for handling and contesting public authority access requests, if received.

Based on the nature of its services and data processing activities, the data importer does not expect to be the target of requests/demands pursuant to national security or intelligence agencies for disclosure of EU personal data.

Such data transfers are not directly nor practically in scope of requests/demands from national security or intelligence agencies for disclosure of EU personal data.

D. Supplementary Measures

Notwithstanding the Conclusion set forth in the above TRA, NAVEX Global has also adopted the following supplemental measures. We believe that by implementing such supplemental measures, we are following best practices and are demonstrating our serious commitment to the protection of customer data.

Contractual safeguards	The SCCs themselves contain a number of contractual commitments by NAVEX Global and its customer, aimed at serving as safeguards for EU personal data.
	Supplementary contractual assurances are offered via our standard data processing addendum or an amendment to the data processing addendum. Please reach out to

	privacy@navexglobal.com in order to get this in place.
	NAVEX Global agrees to audit and monitor its obligations, and to support its customers auditing and monitoring obligations, regarding the level of government access to data.
	NAVEX Global provides a data processing agreement to support GDPR compliance, which includes the SCCs. As the data processor/importer, we process personal data strictly in accordance with your instructions and to provide the services. Our customers are the owners of the personal data within our service applications. NAVEX Global offers a Data Security Addendum, providing for contractual commitments to its information security program.
Organizational safeguards	NAVEX Global maintains written processes and procedures which provide for review of and limit the scope of EU personal data disclosed by NAVEX Global in response to requests from public authorities. Please see our Public Authority Disclosure Request Policy.
	NAVEX Global maintains internal records of requests made by public authorities concerning EU personal data.
	NAVEX Global takes steps to limit the volume of disclosed data, where possible.
	NAVEX Global would take data minimization measures such as redacting unnecessary identifiable personal data or personal data that may be of increased interest to intelligence agencies before complying with a request to disclosure EU personal data.
	NAVEX Global has developed a Standard Contractual Clauses Assurance Guide, which details our commitment to compliance with the SCCs. NAVEX Global remains a participant and has certified its compliance with the EU-U.S. Privacy Shield Framework and the Swiss- U.S. Privacy Shield Framework. NAVEX Global, Inc. is committed to subjecting all personal information received from the European Economic Area, United Kingdom, and Switzerland, respectively, in reliance on each Privacy Shield Framework, to the Frameworks' applicable Principles. To learn more about the Privacy Shield program, and to view our certification, please visit https://www.privacyshield.gov. NAVEX Global provides an independent recourse mechanism to EU individuals, currently TrustArc.

Technical safeguards	Encrypt personal data in transit.
	Encrypt personal data at rest.
	Appropriate access controls.
	Customers can implement data minimization (e.g., store the least amount of data necessary).
	Timespan for any access to personal data "in the clear" is limited to the specific function.
	NAVEX Global equips its services with self-servicing functionality, allowing you to manage the personal data on your own through the use of the services. NAVEX Global engages a recognized, independent third party to conduct a Statement on Standards for Attestation Engagements No. 16, Service Organization Control 2, Type 2 ("SSAE 18 SOC 2 Type 2") audit (or its equivalent or successor) of its information security program and its administrative, technical, and physical safeguards for all facilities used to deliver the Services, which specifically includes privacy controls. NAVEX Global maintains an annual Standardized Information Gathering Questionnaire ("SIG"), which details our robust security program with supporting documentation.

Conclusion

Having regard to the level of risk of the data transfer (**limited risk**), NAVEX Global considers that the measures identified above are **sufficient and effective** in light of the circumstances of the transfers, in conjunction with the supplementary measures and safeguards provided by the SCCs, to allow the data importer to comply with its obligations under the SCCs and provide an appropriate level of protection for the transfer.

Hotline and Incident Management US Hosted Sub-Processing Activity: Interpretations with Transatlantic Translations

NAVEX GLOBAL SUB-PROCESSING ACTIVITY

US HOSTED HOTLINE AND INCIDENT MANAGEMENT – LIVE PHONE INTERPRETATION TRANSFER RISK ASSESSMENT

I. SCOPE

This TRA applies to NAVEX Global's US Hosted Hotline customers. This TRA applies specifically to the live phone interpretations taking place as part of the Hotline services.

As part of NAVEX Global's Hotline service component, customers are provisioned with telephony for receiving reports submitted by individuals via telephone. When a call is received in the English language, no Interpreters are used. When a call is received in a language other than English, a sub-processor may be used to provide interpretation services. NAVEX Global outsources multi-lingual individuals and is therefore capable of processing calls received in languages other than English in some, but not all, instances. If NAVEX Global does not have any available agents capable of interpreting a call received in a particular language, NAVEX Global's sub-processor is contacted and the next available linguist who speaks the language needed is connected to the call ("Interpreter"), joining the reporter and a NAVEX Global contact centre agent. NAVEX Global does not have any discretion over who the Interpreter for a given call will be, or where they may be located, as there is no way to predict when a call will be received or what Interpreters will be available at that time. The individual Interpreters are located throughout the world to support growth in demand for non-English language services.

Once an Interpreter has been connected to the call, they will provide real-time interpretation services so that the NAVEX Global contact centre agent may collect the information from the reporter. The Interpreter does not record or maintain any report information and only makes a note of the date, the duration of the call, and the NAVEX Global billing ID to which the report pertains (for the purpose of billing NAVEX Global for the interpretation services).

II. TRANSFER ANALYSIS

In NAVEX Global's reasonable opinion, upon review with internal and outside counsel, it is unlikely that the interpretation services will be considered a transfer, as defined under the GDPR. There is a reasonable argument, in the UK specifically, that a purely verbal disclosure of information to an interpreter does not trigger the GDPR's mandates, provided that the call (or a transcript of the call) is not recorded by the interpreter at any point in time.

Under UK decision *Scott v LGBT Foundation*, the court found that the information provided orally was not "recorded" and thus did not constitute "data" or "personal data", and accordingly, the (UK) Data Protection Act 1998 did not apply to that disclosure of information. The court also looked to the previous decision of the Court of Appeal in *Durant* v *Financial Services Authority* which confirms the need for information to be recorded in either electronic or manual form in order for it to constitute personal data. While the case was decided under the (UK) Data Protection Act 1998, the relevant provisions under the GDPR are analogous.

At no point is the information provided in the call recorded with the intention that it is processed in the future, but instead the interpretation happens "live", and no record is kept by the Interpreter. While this conclusion would need to be reviewed carefully across the Member States, the determination that live interpretation is not a transfer under the GDPR is reasonable considering the foregoing.

Nevertheless, NAVEX Global approaches its responsibilities with respect to privacy with utmost importance and considers it best practice to apply all the same compliance requirements to this sub-processing activity. As such, we have included interpretations as part of its TRA process.

III. ASSESSING THE ADEQUACY OF EU/UK DATA TRANSFERS – LIVE PHONE INTERPRETATION SERVICES

In assessing the adequacy of transfers of personal data from the EU/UK to NAVEX Global's sub-processor pursuant to the interpretation services provided by said sub-processor, we have taken the following steps:

1. **STEP 1:** Identified the relevant data transfers and the legal mechanism that NAVEX Global and sub-processor is relying on for such transfers (e.g., SCCs).

2. **STEP 2:** Conducted due diligence and collected information about the scope of the transfers, the exposure of the sub-processor to local law that may require disclosure of EU personal data about individuals, and any other relevant information.

3. **STEP 3:** Completed the "Transfer Risk Assessment" in **Section IV** to assess whether the SCCs is effective in light of all circumstances of the transfer.

4. **STEP 4:** Included additional "Supplementary Measures" as set forth in **Section IV (D)**.

5. **STEP 5:** Documented the assessment for accountability purposes. We encourage our customers to do the same.

6. **STEP 6:** NAVEX Global and its sub-processor is responsible for the periodic review of the assessment, which should take place at least annually, to ensure that the transfer of the EU personal data continues to be afforded an adequate level of protection.

IV. TRANSFER RISK ASSESSMENT

Name Of Data Importer: Transatlantic Translations Company, LLC **(**NAVEX Global's sub-processor)
Completed By: NAVEX Global's Privacy Team and TTG's Vicki Crothall
Date: 25 September 2021

A. Type of Data Importer

Name of data importer: Transatlantic Translations Company, LLC, on behalf of itself and Transatlantic Translations Limited ("TTG"). The Processor to Processor SCCs between NAVEX Global and TTG is part of a master services agreement between NAVEX Global and TTG.

Does TTG provide the following services to NAVEX Global:

	Data Importer	
Telecommunications	☐ Yes	☒ No
Other electronic communications (such as an Internet Service Provider or a provider of email, text message, VoIP, remote desktop or VPN services)?	☐ Yes	☒ No
Remote computing services	☐ Yes	☒ No
Other communications service where there may be access to wire or electronic communications	☒ Yes	☐ No

TTG acknowledges that its services could be viewed as meeting the definition of a communication service.

B. Details of Data Transfers

Data transfer mechanism Appropriate Processor to Processor SCCs between TTG and NAVEX Global.
Scope of personal data covered by the data transfer mechanism in place

The SCCs cover transfers of EU personal data from the EEA/UK to third countries, including the following categories of data subjects:

- Employees of customer Data Controller
- Clients, business partners and vendors of customer Data Controller (who are natural persons)
- Employees or contact persons of customer Data Controllers' third-party suppliers, business partners and vendors
- Customer Data Controller's users authorized by data exporter to use the relevant Service(s)

C. Transfer Risk Assessment

The table below aids identification and evaluation of risk factors in relation to the specific data transfer. The assessment of each risk factor is recorded in appropriate detail.

#	Factor	Response
Scope of the transfers		
1.	What is the type of transfer?	Live phone interpretation. There is no storage or remote access by TTG. The call is not recorded nor transcribed by the individual interpreters.
2.	Is the transfer necessary?	Yes. The transfer is critical and necessary to provide the services to NAVEX Global, on behalf of NAVEX Global's customers. To intake reports from individuals on important ethics and compliance matters, we must be able the provide the best language support resources available, to allow these reporters effective whistle blowing capabilities.
3.	Is the transfer proportionate?	Yes. The transfer is strictly limited to interpreting the given reported information via the phone call only.
4.	Is the transfer occasional/non-routine or frequent/routine?	The transfer is occasional and non-routine to TTG interpreters on a per call basis.
5.	Will the transferred personal data be processed for a relatively long or short period of time?	Personal data transferred is processed for a relatively short period of time, in order to interpret the live phone call.
6.	Is the transferred data encrypted and/ or pseudonymized?	Yes. Encryption – when the call reaches NAVEX Global's platform (and thereafter, the Interpreters), the data is encrypted with 256 AES encryption both in transit and at rest. NAVEX

#	Factor	Response
		Global and NAVEX Global's customer using the Interpreting services will ensure their own data encryption arrangements are in place.
Specific circumstances of the transfer		
7.	What are the purposes for which the data are transferred and processed?	To provide the best language interpretation support to hotline reporters.
8.	What are the types of entities involved in the processing?	TTG is a data sub-processor and a private company. NAVEX Global is a data processor and private company. NAVEX Global's customers are the data controllers and may consist of both private and public companies.
9.	In which sector does the transfer occur?	NAVEX Global provides risk and compliance management SaaS based software. ***This factor is especially important as the purposes of our services are to enable organizations to support their risk, ethics, and compliance programs. ***
10.	What are the categories of personal data transferred?	As instructed by NAVEX Global's customer, including but not limited to: • name, job title, job position, location, employer, relationship with the organization, e-mail address, telephone number, log-in credentials, date of birth; • for whistle-blower hotline reports, in addition to the foregoing, the following may also be captured: o facts reported by a reporter about a suspected violation, including how and where the suspected violation occurred and how the reporter learned about the suspected violation; o identity, function and contact details of individuals allegedly involved in the suspected violation; and o identity, function and contact details of individuals who could provide information relating to the suspected violation. Given the nature of hotline services, reporters may submit sensitive categories of data in a report. NAVEX Global recommends its customers have strict policies around the management of such report data in their use of the services, in accordance with the laws subject

#	Factor	Response
		to them.
11.	What is the format of the personal data to be transferred?	When access is provided to an individual interpreter for the purposes described in this TRA, personal data must be accessible in the clear to provide the interpretation. The data is encrypted in transit and at rest as detailed above.
12.	What is the storage location of the data transferred?	The United States via NAVEX Global's secure data centres.
13.	What are the sub-sub-processing activities?	Please see details here: https://www.navexglobal.com/en-us/service-hosting-providers. For the interpretation services, TTG engages Language Services Associates for additional interpreter resources. This processing activity is still limited to the interpretation of a phone call and subject to all the same compliance requirements.
Importer's exposure to government surveillance and practical application of Section 702 FISA		
14.	Is the data importer's sector or business directly subject to such laws in its jurisdiction that permit government access to personal data, or require the assistance of data importer to disclose personal data to public authorities, for surveillance and intelligence gathering purposes?	No, TTG's business is currently not directly subject to such laws.
	a. Specifically, what is data importer's analysis regarding third country surveillance laws, especially Section 702 FISA, under the SCCs and EDPB Guidance?	1) Data exporters may decide to proceed with the transfer without supplementary measures, if they consider there to be no reason to believe that the relevant and problematic legislation (for example, those in the U.S.) will be applied, in practice, to the transferred data and/or TTG. a. In our reasonable opinion upon internal and outside counsel review, we do not find third country surveillance laws, including Section 702 FISA from the U.S., to practically apply to these transfers. b. It is important to note that given the broad definitions of these laws, the vast majority of organizations are going to have to acknowledge their potential application. However, this does not mean they directly apply or

#	Factor	Response
		practically apply in practice. c. We believe TTG is generally out of scope and that these laws are overall not going to apply to the services we provide, as the intent is for surveillance of certain telecom and internet service providers for targeted information. This typically involves surveillance of real time emails, texts, and chat conversations. The foregoing is not what NAVEX Global nor TTG provides and in order to obtain this sought for information, authorities would pursue those providers directly as it would be impractical to make a request through TTG. 2) Data exporters may also take into consideration documented practical experience of data importer with relevant prior instances of requests for access received from public authorities, including those in the U.S. a. ***To this point, TTG has never received a Section 702 FISA request, an EO 12.333 request or order, or any other country access request. *** b. The EDPB Guidance implies that the lack of requests received in the past plus no prohibition on providing information about such requests, could be sufficient to conclude Section 702 FISA does not apply in practice. Note there is no prohibition on TTG to provide information about these requests. 3) If you conclude Section 702 FISA, or any other potential similar types of surveillance law, does not apply in practice to the particular transfer, it is possible to proceed with the transfer without any supplementary measures. **While NAVEX Global and TTG take the approach that Section 702 FISA does not apply in practice, we still have elected to provide for supplementary measures with regard to these transfers. Please see Section IV (D).**
15.	Within the last three (3) years, has the data	

#	Factor	Response
	importer received requests/demands from public authorities in its jurisdiction to disclose EU personal data?	Based on available information, TTG's entities in the U.S. do not receive requests/demands for disclosure of, or access to, EU personal data.
	a. Approximately how many requests/demands from public authorities has the data importer received in that time period concerning EU personal data?	None, to the best of our knowledge.
	b. Approximately how many of these requests/demands are pursuant to criminal law procedure in the destination country? *[Regular court proceedings are not the issue under Schrems II, but intelligence programs are scrutinized.]*	None, to the best of our knowledge.
	c. Approximately how many of these requests/demands are pursuant to national security or intelligence agencies in the destination country?	None, to the best of our knowledge. TTG can represent that it has not received requests/demands from intelligence agencies.
	d. Has the data importer been able to contest/minimize such disclosure of EU personal data, where appropriate?	Not applicable.
	e. What types of EU personal data has the data importer been required to disclose to public authorities in its jurisdiction?	Not applicable.
16.	How likely is it that the data importer will receive bulk data surveillance requests to disclose EU personal data to public authorities in its jurisdiction in the future (e.g., based on factors such as the type of services provided and sector in which the data importer operates, its size, number of customers and reputation)?	Unlikely. TTG's entities in the U.S. do not receive requests/demands by public authorities for disclosure of, or access to, EU personal data, and have no reason to believe that they might receive such in the future.
17.	Does the data importer maintain annual reports or statistics regarding requests/demands received from law enforcement or intelligence agencies (e.g., number/type of requests/demands, requesting authority, etc.)?	Not applicable. TTG has not received requests from public authorities for EU personal data under the SCCs or otherwise. As a result, if TTG gets such requests in the future, it will notify NAVEX Global and this TRA will be updated accordingly.
18.	Does the data importer maintain a written procedure(s) for: 1. Responding to or challenging requests/ demands of law enforcement or intelligence agencies that apply to EU personal data? 8. Informing customers of requests/demands from law enforcement or intelligence agencies where permitted by applicable law?	Yes. While TTG has never received such requests, it does have a policy and procedure should the event ever happen. Included in the procedure, there will be a list of any and all such requests.
19.	Are the data importer's commitments enabling data subjects to exercise their rights as provided in the SCCs thwarted by the laws	Data subjects' rights can be effectively applied in practice. TTG has never encountered a situation

#	Factor	Response
	and/or practices in the U.S. and any other third countries involved, or can these rights be effectively applied in practice?	where it felt it could not enable data subject rights, including judicial redress. We do not believe the laws subject to us prevent us from enabling, supporting, and fulfilling data subject rights under the SCCs.
Onward transfers and exposure to government surveillance		
20.	Does the data importer share EU personal data further with third-party data recipients in [the U.S./other jurisdiction]?	Yes. TTG utilizes Language Services Associates (LSA) for additional interpretation resources.
21.	What measures does the third-party data recipient take to ensure the protection of EU personal data transferred to it?	Where TTG engages LSA to have access to EU personal data, TTG enters into written agreements with LSA that include safeguards for EU personal data in accordance with the GDPR requirements.
22.	What assurances has the data importer received from third-party data recipients with respect to requests/demands for EU personal data from [U.S./other jurisdiction] public authorities?	TTG has updated written agreements, or has ensured such updates are in progress, with LSA to include additional measures for the protection of EU personal data, where required.
23.	Is the vendor's (or its sub-processor's) sector or business directly subject to such laws in its jurisdiction that permit government access to personal data, or require the assistance of data importer to disclose personal data to public authorities, for surveillance and intelligence gathering purposes?	No, TTG does not believe in its reasonable opinion that it or its sub-processors are directly subject to such laws in their jurisdiction.

Conclusion/Risk of transfers

Very limited-risk data transfer

In particular, TTG and NAVEX Global identified the following factors (based on the assessment documented above and any additional information), that are likely to indicate a very limited-risk transfer:

No further processing outside of an interpretation of a live phone call takes place. As such, it is reasonable to determine that no transfer is taking place under the GDPR.

The data importer has never received requests/demands from intelligence services for disclosure of EU personal data.

The data importer has received limited requests/demands from public authorities for disclosure of EU personal data (such as for disclosure of employee data), but the requests related to regular criminal law procedure and did not go beyond what is necessary and proportionate to meet the purpose of the request.

The data importer has a process in place for handling and contesting public authority access requests, if received.

Based on the nature of its services and data processing activities, the data importer does not expect to be the target of requests/demands pursuant to national security or intelligence agencies for disclosure

#	Factor	Response
		of EU personal data. Such data transfers are not directly nor practically in scope of requests/demands from national security or intelligence agencies for disclosure of EU personal data.

D. Supplementary Measures

Notwithstanding the Conclusion set forth in the above TRA, TTG has also adopted the following supplemental measures. We believe that by implementing such supplemental measures, we are following best practices and are demonstrating our serious commitment to the protection of customer data.

Contractual safeguards	TTG and NAVEX Global have entered into supplementary contractual assurances as an amendment to the data processing addendum.
	The SCCs themselves contain a number of contractual commitments by TTG and NAVEX Global, aimed at serving as safeguards for EU personal data. We have also entered into a robust general data processing addendum.
	TTG is committed to implementing other transparency, audit and monitoring obligations regarding the level of government access to data, including, a policy and process to address any potential requests for disclosure to governmental agencies around the world. This is to include a legend of any such request received and actioned.
Organizational safeguards	TTG maintains written processes and procedures provide for review of and limit the scope of EU personal data disclosed by TTG in response to requests from public authorities.
	TTG would maintain internal record of requests made by public authorities concerning EU personal data.
	TTG takes steps to limit the volume of disclosed data, where possible.
	TTG would take data minimization measures such as redacting unnecessary identifiable personal data or personal data that may be of increased interest to intelligence agencies before complying with a request to disclosure EU personal data.
Technical safeguards	Encrypt personal data in transit, as detailed above
	Encrypt personal data at rest, as detailed above.

	Appropriate access controls.
	Calls are not recorded, ensuring the limit timespan for processing personal data "in the clear" (i.e., in identifiable form).

Conclusion

Having regard to the level of risk of the data transfer (**very limited risk**), TTG and NAVEX Global consider that the measures identified above are **sufficient and effective** in light of the circumstances of the transfers, in conjunction with the supplementary measures and safeguards provided by the SCCs, to allow the data importer to comply with its obligations under the SCCs and provide an appropriate level of protection for the transfer.

Hotline and Incident Management US Hosted Sub-Processing Activity: Interpretations with Certified Languages

NAVEX GLOBAL SUB-PROCESSING ACTIVITY

US HOSTED HOTLINE AND INCIDENT MANAGEMENT – LIVE PHONE INTERPRETATION TRANSFER RISK ASSESSMENT

I. SCOPE

This TRA applies to NAVEX Global's US Hosted Hotline customers. This TRA applies specifically to the live phone interpretation taking place as part of the Hotline services.

As part of NAVEX Global's Hotline service component, customers are provisioned with telephony for receiving reports submitted by individuals via telephone. When a call is received in the English language no Interpreters are used. When a call is received in a language other than English, a sub-processor may be used to provide interpretation services. NAVEX Global outsources multi-lingual individuals and is therefore capable of processing calls received in languages other than English in some, but not all, instances. If NAVEX Global does not have any available agents capable of interpreting a call received in a particular language, NAVEX Global's sub-processors are contacted and the next available sub-processor employee who speaks the language needed is connected to the call ("Interpreter"), joining the reporter and a NAVEX Global contact centre agent. NAVEX Global does not have any discretion over who the Interpreter for a given call will be, or where they may be located, as there is no way to predict when a call will be received or what Interpreters will be available at that time. The individual Interpreters are located in the U.S.

Once an Interpreter has been connected to the call, they will provide real-time interpretation services so that the NAVEX Global contact centre agent may collect the information from the reporter. The Interpreter does not record or maintain any report information and only makes a note of the date, the duration of the call, and the NAVEX Global customer to which the report pertains (for the purpose of billing NAVEX Global for the interpretation services).

II. TRANSFER ANALYSIS

In NAVEX Global's reasonable opinion, upon review with internal and outside counsel, it is unlikely that the interpretation services will be considered a transfer, as defined under the GDPR. There is a reasonable argument, in the UK specifically, that a purely verbal disclosure of information to an interpreter does not trigger the GDPR's mandates, provided that the call (or a transcript of the call) is not recorded by the interpreter at any point in time.

Under UK decision *Scott v LGBT Foundation*, the court found that the information provided orally was not "recorded" and thus did not constitute "data" or "personal data", and accordingly, the (UK) Data Protection Act 1998 did not apply to that disclosure of information. The court also looked to the previous decision of the Court of Appeal in *Durant* v *Financial Services Authority* which confirms the need for information to be recorded in either electronic or manual form in order for it to constitute personal data. While the case was decided under the (UK) Data Protection Act 1998, the relevant provisions under the GDPR are analogous.

At no point is the information provided in the call recorded with the intention that it is processed in the future, but instead the interpretation happens "live", and no record is kept by the Interpreter. While this conclusion would need to be reviewed carefully across the Member States, the determination that live interpretation is not a transfer under the GDPR is reasonable considering the foregoing.

Nevertheless, NAVEX Global approaches its responsibilities with respect to privacy with utmost importance and considers it best practice to apply all the same compliance requirements to this sub-processing activity. As such, we have included interpretations as part of its TRA process.

III. ASSESSING THE ADEQUACY OF EU/UK DATA TRANSFERS – LIVE PHONE INTERPRETATION SERVICES

In assessing the adequacy of transfers of personal data from the EU/UK to NAVEX Global's sub-processor pursuant to the interpretation services provided by said sub-processor, we have taken the following steps:

1. **STEP 1:** Identified the relevant data transfers and the legal mechanism that NAVEX Global and sub-processor is relying on for such transfers (e.g., SCCs).

2. **STEP 2:** Conducted due diligence and collected information about the scope of the transfers, the exposure of the sub-processor to local law that may require disclosure of EU personal data about individuals, and any other relevant information.

3. **STEP 3:** Completed the "Transfer Risk Assessment" in **Section IV** to assess whether the SCCs is effective in light of all circumstances of the transfer.

4. **STEP 4:** Included additional "Supplementary Measures" as set forth in **Section IV (D)**.

5. **STEP 5:** Documented the assessment for accountability purposes. We encourage our customers to do the same.

6. **STEP 6:** NAVEX Global and its sub-processor is responsible for the periodic review of the assessment, which should take place at least annually, to ensure that the transfer of the EU personal data continues to be afforded an adequate level of protection.

IV. TRANSFER RISK ASSESSMENT

Name Of Data Importer: Certified Languages International, LLC **(**NAVEX Global's sub-processor)
Completed By: NAVEX Global's Privacy Team and CLI's Compliance Team
Date: 25 September 2021

A. Type of Data Importer

Name of data importer: Certified Languages International, LLC ("CLI"). The Processor to Processor SCCs between NAVEX Global and CLI is part of a master services agreement between NAVEX Global and CLI.

Does CLI provide the following services to NAVEX Global:

	Data Importer	
Telecommunications	☐ Yes	☒ No
Other electronic communications (such as an Internet Service Provider or a provider of email, text message, VoIP, remote desktop or VPN services)?	☐ Yes	☒ No
Remote computing services	☐ Yes	☒ No
Other communications service where there may be access to wire or electronic communications	☒ Yes	☐ No

CLI acknowledges that its services could be viewed as meeting the definition of a communication service.

B. Details of Data Transfers

Data transfer mechanism Appropriate Processor to Processor SCCs between CLI and NAVEX Global.
Scope of personal data covered by the data transfer mechanism in place The SCCs cover transfers of EU personal data from the EEA/UK to the third countries, including the following categories of data subjects: • Employees of customer Data Controller • Clients, business partners and vendors of customer Data Controller (who are natural persons) • Employees or contact persons of customer Data Controllers' third-party suppliers, business partners and vendors • Customer Data Controller's users authorized by data exporter to use the relevant Service(s)

C. Transfer Risk Assessment

The table below aids identification and evaluation of risk factors in relation to the specific data transfer. The assessment of each risk factor is recorded in appropriate detail.

#	Factor	Response
Scope of the transfers		
1.	What is the type of transfer?	Live phone interpretation. There is no storage or remote access by CLI. The call is not recorded nor transcribed by the individual interpreters.

#	Factor	Response
2.	Is the transfer necessary?	Yes. The transfer is critical and necessary to provide the services to NAVEX Global, on behalf of NAVEX Global's U.S. hosted customers. To intake reports from individuals on important ethics and compliance matters, we have to be able the provide the best language support resources available, to allow these reporters effective whistle blowing capabilities.
3.	Is the transfer proportionate?	Yes. The transfer is strictly limited to interpreting the given reported information via the phone call only.
4.	Is the transfer occasional/non-routine or frequent/routine?	The transfer is occasional and non-routine to CLI interpreters on a per call basis.
5.	Will the transferred personal data be processed for a relatively long or short period of time?	Personal data transferred is processed for a relatively short period of time, to interpret the live phone call.
6.	Is the transferred data encrypted and/ or pseudonymized?	Yes. CSR phone calls are encrypted. Calls are not recorded nor transcribed by the interpreter. Call data is submitted to NAVEX Global's case management systems on behalf of the customer Data Controllers which deploy encryption at rest.
Specific circumstances of the transfer		
7.	What are the purposes for which the data are transferred and processed?	To provide the best language interpretation support to hotline reporters.
8.	What are the types of entities involved in the processing?	CLI is a data sub-processor and a private company. NAVEX Global is a data processor and private company. NAVEX Global's customers are the data controllers and may consist of both private and public companies.
9.	In which sector does the transfer occur?	NAVEX Global provides risk and compliance management SaaS based software. ***This factor is especially important as the purposes of our services is to enable organizations support their risk, ethics, and compliance programs. ***
10.	What are the categories of personal data transferred?	• name, job title, job position, location, employer, relationship with the

#	Factor	Response
		organization, e-mail address, telephone number; • for whistle-blower hotline reports, in addition to the foregoing, the following may also be captured: o facts reported by a reporter about a suspected violation, including how and where the suspected violation occurred and how the reporter learned about the suspected violation; o identity, function and contact details of individuals allegedly involved in the suspected violation; and o identity, function and contact details of individuals who could provide information relating to the suspected violation. Given the nature of hotline services, reporters may submit sensitive categories of data in a report. NAVEX Global recommends its customers have strict policies around the management of such report data in their use of the services, in accordance with the laws subject to them.
11.	What is the format of the personal data to be transferred?	When access is provided to an individual interpreter for the purposes described in this TRA, personal data must be accessible in the clear to provide the interpretation. Interpretation service occurs in real-time over commercial phone lines. Calls are not recorded.
12.	What is the storage location of the data transferred?	The United States once the call data is submitted to the NAVEX Global secure data centres.
13.	What are the sub-sub-processing activities?	Not applicable.
Importer's exposure to government surveillance and practical application of Section 702 FISA		
14.	Is the data importer's sector or business directly subject to such laws in its jurisdiction that permit government access to personal data, or require the assistance of data importer to disclose personal data to public authorities, for surveillance and intelligence gathering purposes?	No. CLI's business is currently not directly subject to such laws.
	a. Specifically, what is data importer's analysis regarding Section 702 FISA	1) Data exporters may decide to proceed with the transfer without supplementary

#	Factor	Response
	under the SCCs and EDPB Guidance?	measures, if they consider there to be no reason to believe that the relevant and problematic legislation (those in the U.S. in this instance) will be applied, in practice, to the transferred data and/or CLI. a. In our reasonable opinion upon internal and outside counsel review, we do not find U.S. surveillance laws, including Section 702 FISA, to practically apply to these transfers. b. It is important to note that given the broad definitions of these laws, the vast majority of organizations are going to have to acknowledge their potential application. However, this does not mean they directly apply or practically apply in practice. c. We believe CLI is generally out of scope and that these laws are overall not going to apply to the services we provide, as the intent is for surveillance of certain telecom and internet service providers for targeted information. This typically involves to surveillance of real time emails, texts, and chat conversations. The foregoing is not what CLI provides and in order to obtain this sought for information, authorities would pursue those providers directly as it would be impractical to make a request through CLI. 2) Data exporters may also take into consideration documented practical experience of data importer with relevant prior instances of requests for access received from public authorities in the U.S. a. ***To this point, CLI has never received a Section 702 FISA request or an EO 12.333 request or order.** * b. The EDPB Guidance implies that the lack of requests received in the past plus no prohibition on providing information about such requests, could be sufficient to conclude Section 702 FISA does not apply in practice. Note there is no prohibition on CLI to provide information about

#	Factor	Response
		these requests. 3) If you conclude Section 702 FISA does not apply in practice to the particular transfer, it is possible to proceed with the transfer without any supplementary measures. **While NAVEX Global and CLI takes the approach that Section 702 FISA does not apply in practice, we still have elected to provide for supplementary measures with regard to these transfers. Please see Section IV (D).**
15.	Within the last three (3) years, has the data importer received requests/demands from public authorities in its jurisdiction to disclose EU personal data?	Based on available information, CLI's entities do not receive requests/demands for disclosure of, or access to, EU personal data.
	a. Approximately how many requests/demands from public authorities has the data importer received in that time period concerning EU personal data?	None, to the best of our knowledge.
	b. Approximately how many of these requests/demands are pursuant to criminal law procedure in the destination country? *[Regular court proceedings are not the issue under Schrems II, but intelligence programs are scrutinized.]*	None, to the best of our knowledge.
	c. Approximately how many of these requests/demands are pursuant to national security or intelligence agencies in the destination country?	None, to the best of our knowledge. CLI can represent that it has not received requests/demands from intelligence agencies.
	d. Has the data importer been able to contest/minimize such disclosure of EU personal data, where appropriate?	Not applicable.
	e. What types of EU personal data has the data importer been required to disclose to public authorities in its jurisdiction?	Not applicable.
16.	How likely is it that the data importer will receive bulk data surveillance requests to disclose EU personal data to public authorities in its jurisdiction in the future (e.g., based on factors such as the type of services provided and sector in which the data importer operates, its size, number of customers and reputation)?	Unlikely. CLI's entities do not receive requests/demands by public authorities for disclosure of, or access to, EU personal data, and have no reason to believe that they might receive such in the future.
17.	Does the data importer maintain annual reports or statistics regarding requests/demands received from law enforcement or intelligence agencies (e.g., number/type of requests/demands, requesting authority, etc.)?	Not applicable. CLI has not received requests from public authorities for EU personal data under the SCCs or otherwise. As a result, if CLI gets such requests in the future, it will notify NAVEX Global and this TRA will be updated accordingly.
18.	Does the data importer maintain a written	

#	Factor	Response
	procedure(s) for: 1. Responding to or challenging requests/ demands of law enforcement or intelligence agencies that apply to EU personal data? 9. Informing customers of requests/demands from law enforcement or intelligence agencies where permitted by applicable law?	Not applicable. CLI has not received requests from public authorities for EU personal data under the SCCs or otherwise. As a result, if CLI gets such requests in the future, it will notify NAVEX Global and this TRA will be updated accordingly. CLI and NAVEX Global entered into a contractual agreement requiring CLI to cooperate and mutually agree on any appropriate actions, to notify NAVEX Global of any requests unless explicitly required otherwise under applicable law, to put any access request on hold, and to use reasonable efforts to obtain the right to waive any notice prohibitions and oppose any such request and contest its legal validity where possible and permitted. The contract additionally ensures CLI will not make any disclosures that are determined to be massive, disproportionate, and indiscriminate in a manner that would go beyond what is necessary in a democratic society. CLI is obliged to document and demonstrate to the assessments made and the actions taken. CLI undertakes to regularly review, assess, and continuously monitor the scope of the access to personal data by public authorities in the countries where CLI is processing personal data, as well as the safeguards and recourses in place to protect data subjects, and to immediately inform NAVEX Global in the case of a change in applicable law that would materially impact such access by public authorities or recourses available to data subjects.
19.	Are the data importer's commitments enabling data subjects to exercise their rights as provided in the SCCs thwarted by the laws and/or practices in the U.S. and any other third countries involved, or can these rights be effectively applied in practice?	No. Data subjects' rights can be effectively applied in practice. CLI has never encountered a situation where it felt it could not enable data subject rights, including judicial redress. We do not believe the laws subject to us prevent us from enabling, supporting, and fulfilling data subject rights under the SCCs.
Onward transfers and exposure to government surveillance		
20.	Does the data importer share EU personal data further with third-party data recipients in [the U.S./other jurisdiction]?	No, not applicable.
	Conclusion/Risk of transfers **Very limited-risk data transfer** **In particular, CLI and NAVEX Global identified the following factors (based on the assessment documented above and any additional information), that are likely to indicate a very limited-risk transfer:** No further processing outside of an interpretation of a live phone call takes place. As such, it is	

#	Factor	Response
		reasonable to determine that no transfer is taking place under the GDPR. The data importer has never received requests/demands from intelligence services for disclosure of EU personal data. The data importer has never even received requests for disclosure of EU personal data related to regular criminal law procedure. Based on the nature of its services and data processing activities, the data importer does not expect to be the target of requests/demands pursuant to national security or intelligence agencies for disclosure of EU personal data. Such data transfers are not directly nor practically in scope of requests/demands from national security or intelligence agencies for disclosure of EU personal data.

D. Supplementary Measures

Notwithstanding the Conclusion set forth in the above TRA, CLI has also adopted the following supplemental measures. We believe that by implementing such supplemental measures, we are following best practices and are demonstrating our serious commitment to the protection of customer data.

Contractual safeguards	CLI and NAVEX Global have entered into supplementary contractual assurances as an amendment to the data processing addendum.
	The SCCs themselves contain a number of contractual commitments by CLI and NAVEX Global, aimed at serving as safeguards for EU personal data. We have also entered into a robust general data processing addendum.
	CLI is committed to implementing other transparency, audit and monitoring obligations on CLI regarding the level of government access to data. This is to include a legend of any such request received and actioned.
Organizational safeguards	CLI maintains written processes and procedures provide for review of and limit the scope of EU personal data disclosed by CLI in response to requests from public authorities.
	CLI would maintain internal record of requests made by public authorities concerning EU personal data.
	CLI takes steps to limit the volume of disclosed data, where possible.
	CLI would take data minimization measures such as redacting unnecessary identifiable personal data or personal data that may be of increased interest to intelligence agencies before complying

	with a request to disclosure EU personal data.
Technical safeguards	Encrypt personal data in transit, as applicable and as detailed above.
	Encrypt personal data at rest, as detailed above.
	Appropriate access controls.
	Calls are not recorded, ensuring the limit timespan for processing personal data "in the clear" (i.e., in identifiable form).

Conclusion

Having regard to the level of risk of the data transfer (**very limited risk**), CLI and NAVEX Global consider that the measures identified above are **sufficient and effective** in light of the circumstances of the transfers, in conjunction with the supplementary measures and safeguards provided by the SCCs, to allow the data importer to comply with its obligations under the SCCs and provide an appropriate level of protection for the transfer.

Hotline and Incident Management US Hosted Sub-Processing Activity: Interpretations with United Language Group

NAVEX GLOBAL SUB-PROCESSING ACTIVITY

US HOSTED HOTLINE AND INCIDENT MANAGEMENT – LIVE PHONE INTERPRETATION TRANSFER RISK ASSESSMENT

I. SCOPE

This TRA applies to NAVEX Global's US Hosted Hotline customers. This TRA applies specifically to the live phone interpretation taking place as part of the Hotline services.

As part of NAVEX Global's Hotline service component, customers are provisioned with telephony for receiving reports submitted by individuals via telephone. When a call is received in the English language no Interpreters are used. When a call is received in a language other than English, a sub-processor may be used to provide interpretation services. NAVEX Global outsources multi-lingual individuals and is therefore capable of processing calls received in languages other than English in some, but not all, instances. If NAVEX Global does not have any available agents capable of interpreting a call received in a particular language, NAVEX Global's sub-processors are contacted and the next available sub-processor employee who speaks the language needed is connected to the call ("Interpreter"), joining the reporter and a NAVEX Global contact centre agent. NAVEX Global does not have any discretion over who the Interpreter for a given call will be, or where they may be located, as there is no way to predict when a call will be received or what Interpreters will be available at that time. The individual Interpreters are located throughout the world to support growth in demand for non-English language services.

Once an Interpreter has been connected to the call, they will provide real-time interpretation services so that the NAVEX Global contact centre agent may collect the information from the reporter. The Interpreter does not record or maintain any report information and only makes a note of the date, the duration of the call, and the NAVEX Global customer to which the report pertains (for the purpose of billing NAVEX Global for the interpretation services).

II. TRANSFER ANALYSIS

In NAVEX Global's reasonable opinion, upon review with internal and outside counsel, it is unlikely that the interpretation services will be considered a transfer, as defined under the GDPR. There is a reasonable argument, in the UK specifically, that a purely verbal disclosure of information to an interpreter does not trigger the GDPR's mandate, provided that the call (or a transcript of the call) is not recorded by the interpreter at any point in time.

Under UK decision *Scott v LGBT Foundation*, the court found that the information provided orally was not "recorded" and thus did not constitute "data" or "personal data", and accordingly, the (UK) Data Protection Act 1998 did not apply to that disclosure of information. The court also looked to the previous decision of the Court of Appeal in *Durant* v *Financial Services Authority* which confirms the need for information to be recorded in either electronic or manual form in order for it to constitute personal data. While the case was decided under the (UK) Data Protection Act 1998, the relevant provisions under the GDPR are analogous.

At no point is the information provided in the call recorded with the intention that it is processed in the future, but instead the interpretation happens "live", and no record is kept by the Interpreter. While this conclusion would need to be reviewed carefully across the Member States, the determination that live interpretation is not a transfer under the GDPR is reasonable considering the foregoing.

Nevertheless, NAVEX Global approaches its responsibilities with respect to privacy with utmost importance and considers it best practice to apply all the same compliance requirements to this sub-processing activity. As such, we have included interpretations as part of its TRA process.

III. ASSESSING THE ADEQUACY OF EU/UK DATA TRANSFERS – LIVE PHONE INTERPRETATION SERVICES

In assessing the adequacy of transfers of personal data from the EU/UK to NAVEX Global's sub-processor pursuant to the interpretation services provided by said sub-processor, we have taken the following steps:

1. **STEP 1:** Identified the relevant data transfers and the legal mechanism that NAVEX Global and sub-processor is relying on for such transfers (e.g., SCCs).

2. **STEP 2:** Conducted due diligence and collected information about the scope of the transfers, the exposure of the sub-processor to local law that may require disclosure of EU personal data about individuals, and any other relevant information.

3. **STEP 3:** Completed the "Transfer Risk Assessment" in **Section IV** to assess whether the SCCs is effective in light of all circumstances of the transfer.

4. **STEP 4:** Included additional "Supplementary Measures" as set forth in **Section IV (D)**.

5. **STEP 5:** Documented the assessment for accountability purposes. We encourage our customers to do the same.

6. **STEP 6:** NAVEX Global and its sub-processor is responsible for the periodic review of the assessment, which should take place at least annually, to ensure that the transfer of the EU personal data continues to be afforded an adequate level of protection.

IV. TRANSFER RISK ASSESSMENT

Name Of Data Importer: United Language Group, Inc. **(**NAVEX Global's sub-processor)
Completed By: NAVEX Global's Privacy Team and ULG Privacy Representatives
Date: 25 September 2021

A. Type of Data Importer

Name of data importer: United Language Group, Inc. ("ULG"). The Processor to Processor SCCs between NAVEX Global and ULG is part of a master services agreement between NAVEX Global and ULG.

Does ULG provide the following services to NAVEX Global:

	Data Importer	
Telecommunications	☐ Yes	☒ No
Other electronic communications (such as an Internet Service Provider or a provider of email, text message, VoIP, remote desktop or VPN services)?	☐ Yes	☐ No
Remote computing services	☐ Yes	☒ No
Other communications service where there may be access to wire or electronic communications	☒ Yes	☐ No

ULG provides live phone interpretation to NAVEX Global customers, processed by individual request. Call data is not stored and calls are not recorded. ULG acknowledges that its services could be viewed as meeting the definition of a communication service.

B. Details of Data Transfers

Data transfer mechanism Appropriate Processor to Processor SCCs between ULG and NAVEX Global.
Scope of personal data covered by the data transfer mechanism in place The SCCs cover transfers of EU personal data from the EEA/UK to the third countries, including the following categories of data subjects: • Employees of customer Data Controller • Clients, business partners and vendors of customer Data Controller (who are natural persons) • Employees or contact persons of customer Data Controllers' third-party suppliers, business partners and vendors • Customer Data Controller's users authorized by data exporter to use the relevant Service(s)

C. Transfer Risk Assessment

The table below aids identification and evaluation of risk factors in relation to the specific data transfer. The assessment of each risk factor is recorded in appropriate detail.

#	Factor	Response
Scope of the transfers		
1.	What is the type of transfer?	Live phone interpretation. There is no storage or remote access by ULG. The call is not recorded nor transcribed by the individual interpreters.
2.	Is the transfer necessary?	Yes. The transfer is critical and necessary to provide the services to NAVEX Global, on behalf of NAVEX Global's U.S. hosted customers. To intake reports from individuals on important ethics and compliance matters, we have to be able the provide the best language support resources available, to allow these reporters effective whistle blowing capabilities.
3.	Is the transfer proportionate?	Yes. The transfer is strictly limited to interpreting the given reported information via the phone call only. Any limited data processing activities are solely concerned with the processing of live call information and not resulting data is stored and/ or subsequently processed.
4.	Is the transfer occasional/non-routine or frequent/routine?	The transfer is occasional and non-routine to ULG interpreters on a per call basis.
5.	Will the transferred personal data be processed for a relatively long or short period of time?	Personal data transferred is processed for a relatively short period of time, to interpret the live phone call.
6.	Is the transferred data encrypted and/ or pseudonymized?	Yes, Encryption -- ULG utilizes FIPS compatible transfer mechanism. This mechanism uses 128 Mbps encryption. SFTP is used for secure file transfer.
Specific circumstances of the transfer		
7.	What are the purposes for which the data are transferred and processed?	To provide the best language interpretation support to hotline reporters.
8.	What are the types of entities involved in the processing?	ULG is a data sub-processor and a private

#	Factor	Response
		company. ULG's network of interpreters may be employees, contractors or subcontractors of ULG. NAVEX Global is a data processor and private company. NAVEX Global's customers are the data controllers and may consist of both private and public companies.
9.	In which sector does the transfer occur?	NAVEX Global provides risk and compliance management SaaS based software. ***This factor is especially important as the purposes of our services is to enable organizations support their risk, ethics, and compliance programs. *** ULG provides SaaS based software and a range of interpretation and translation services.
10.	What are the categories of personal data transferred?	• name, job title, job position, location, employer, relationship with the organization, e-mail address, telephone number; • for whistle-blower hotline reports, in addition to the foregoing, the following may also be captured: o facts reported by a reporter about a suspected violation, including how and where the suspected violation occurred and how the reporter learned about the suspected violation; o identity, function and contact details of individuals allegedly involved in the suspected violation; and o identity, function and contact details of individuals who could provide information relating to the suspected violation. Given the nature of hotline services, reporters may submit sensitive categories of data in a report. NAVEX Global recommends its customers have strict policies around the management of such report data in their use of the services, in accordance with the laws subject to them.
11.	What is the format of the personal data to be transferred?	When access is provided to an individual interpreter for the purposes described in this TRA, personal data must be accessible in the clear to provide the interpretation. ULG utilizes FIPS compatible transfer

#	Factor	Response
		mechanism. This mechanism uses 128 Mbps encryption. SFTP is used for secure file transfer.
12.	What is the storage location of the data transferred?	The processing principally takes place in the US but may take place in a range of overseas jurisdictions depending on the location of the interpreter. In any event, for the purposes of the interpretation services, no data is stored. The interpreted report is ultimately dispatched and stored via NAVEX Global's secure data centres in the United States.
13.	What are the sub-sub-processing activities?	Not applicable.
Importer's exposure to government surveillance and practical application of Section 702 FISA		
14.	Is the data importer's sector or business directly subject to such laws in its jurisdiction that permit government access to personal data, or require the assistance of data importer to disclose personal data to public authorities, for surveillance and intelligence gathering purposes?	No. ULG's business is currently not directly subject to such laws. in light of the scope of FISA, ULG does provide ancillary services which would fall within the definition of an electronic communication service under FISA. However, ULG does not consider itself involved in a sector that is universally accepted as being subject to a FISA remit (such sectors principally being telcos, mail exchanges, web hosting, data center providers and other cloud providers and social media organizations).
	a. Specifically, what is data importer's analysis regarding third country surveillance laws, especially Section 702 FISA, under the SCCs and EDPB Guidance?	1) Data exporters may decide to proceed with the transfer without supplementary measures, if they consider there to be no reason to believe that the relevant and problematic legislation (for example, those in the U.S.) will be applied, in practice, to the transferred data and/or ULG. a. In our reasonable opinion upon internal and outside counsel review, we do not consider ULG to be active in a sector which would make it a target for access orders pursuant to FISA 702, nor would be consider ULG's data processing activities of interest to US intelligence agencies under EO 12.333, PPD-28, the Cloud Act, or other problematic third country surveillance laws. b. It is important to note that given the broad definitions of these laws, the vast majority of organizations are going to have to acknowledge their potential application. However, this

#	Factor	Response
		does not mean they directly apply or practically apply in practice. c. We believe ULG is generally out of scope and that these laws are overall not going to apply to the services we provide, as the intent is for surveillance of certain telecom and internet service providers for targeted information. This typically involves to surveillance of real time emails, texts, and chat conversations. The foregoing is not what ULG nor NAVEX Global provides and in order to obtain this sought for information, authorities would pursue those providers directly as it would be impractical to make a request through ULG. 2) Data exporters may also take into consideration documented practical experience of data importer with relevant prior instances of requests for access received from public authorities, including those in the U.S. a. ***To this point, ULG has never received a Section 702 FISA request or an EO 12.333 request or order.** * b. The EDPB Guidance implies that the lack of requests received in the past plus no prohibition on providing information about such requests, could be sufficient to conclude Section 702 FISA does not apply in practice. Note there is no prohibition on ULG to provide information about these requests. 3) If you conclude Section 702 FISA does not apply in practice to the particular transfer, it is possible to proceed with the transfer without any supplementary measures. **While NAVEX Global and ULG take the approach that Section 702 FISA does not apply in practice, we still have elected to provide for supplementary measures with regard to these transfers. Please see Section IV (D).**
15.	Within the last three (3) years, has the data importer received requests/demands from public authorities in its jurisdiction to disclose EU personal data?	Based on available information, ULG's entities in the US do not routinely receive requests/demands for disclosure of, or access

#	Factor	Response
		to, EU personal data.
	a. Approximately how many requests/demands from public authorities has the data importer received in that time period concerning EU personal data?	None, to the best of our knowledge.
	b. Approximately how many of these requests/demands are pursuant to criminal law procedure in the destination country? *[Regular court proceedings are not the issue under Schrems II, but intelligence programs are scrutinized.]*	None, to the best of our knowledge.
	c. Approximately how many of these requests/demands are pursuant to national security or intelligence agencies in the destination country?	None, to the best of our knowledge. The data importer can represent that it has not received requests/demands from such intelligence agencies. ULG is not subject to FISA 702 requests.
	d. Has the data importer been able to contest/minimize such disclosure of EU personal data, where appropriate?	Not applicable.
	e. What types of EU personal data has the data importer been required to disclose to public authorities in its jurisdiction?	Not applicable.
16.	How likely is it that the data importer will receive bulk data surveillance requests to disclose EU personal data to public authorities in its jurisdiction in the future (e.g., based on factors such as the type of services provided and sector in which the data importer operates, its size, number of customers and reputation)?	Unlikely. ULG does not consider itself active within a sector which is the subject to surveillance gathering activities and consider it extremely remote that it would receive any bulk data surveillance requests.
17.	Does the data importer maintain annual reports or statistics regarding requests/demands received from law enforcement or intelligence agencies (e.g., number/type of requests/demands, requesting authority, etc.)?	Yes. This is maintained for ULG internal only purposes and are to be provided to NAVEX Global in accordance with the terms of the data processing agreement. At this time we have received no requests regarding FISA 702 surveillance or from public authorities for EU data under the SCCs or otherwise.
18.	Does the data importer maintain a written procedure(s) for: 1. Responding to or challenging requests/ demands of law enforcement or intelligence agencies that apply to EU personal data? 10. Informing customers of requests/demands from law enforcement or intelligence agencies where permitted by applicable law?	Not applicable. ULG has not received requests from public authorities for EU personal data under the SCCs or otherwise. If ULG gets such requests in the future, we would escalate the matter and as such would follow our documented notification process requiring & insuring that we would notify NAVEX Global. ULG and NAVEX Global entered into a contractual agreement requiring ULG to cooperate and mutually agree on any appropriate actions, to notify NAVEX Global of any requests unless explicitly required otherwise

#	Factor	Response
		under applicable law, to put any access request on hold, and to use reasonable efforts to obtain the right to waive any notice prohibitions and oppose any such request and contest its legal validity where possible and permitted. The contract additionally ensures ULG will not make any disclosures that are determined to be massive, disproportionate, and indiscriminate in a manner that would go beyond what is necessary in a democratic society. ULG is obliged to document and demonstrate to the assessments made and the actions taken. ULG undertakes to regularly review, assess, and continuously monitor the scope of the access to personal data by public authorities in the countries where ULG is processing personal data, as well as the safeguards and recourses in place to protect data subjects, and to immediately inform NAVEX Global in the case of a change in applicable law that would materially impact such access by public authorities or recourses available to data subjects
19.	Are the data importer's commitments enabling data subjects to exercise their rights as provided in the SCCs thwarted by the laws and/or practices in the U.S. and any other third countries involved, or can these rights be effectively applied in practice?	ULG does not consider itself to be active in a sector which is considered a target for FISA 702 related surveillance activities and maintains a data subject access request policy in respect of any traditional Data Production Request orders.
Onward transfers and exposure to government surveillance		
20.	Does the data importer share EU personal data further with third-party data recipients?	No, not applicable. As part of company policy, ULG has not shared data with anyone.

Conclusion/Risk of transfers

Very limited-risk data transfer

In particular, ULG and NAVEX Global identified the following factors (based on the assessment documented above and any additional information), that are likely to indicate a very limited-risk transfer:

No further processing outside of an interpretation of a live phone call takes place. As such, it may be reasonable to determine that no transfer is taking place under the GDPR.

The data importer has never received requests/demands from intelligence services for disclosure of EU personal data. The data importer is not active in a sector which is regarded as subject to requests/demands from intelligence services. The data importer has a process in place for handling and contesting public authority access requests, if received.

Based on the nature of its services and data processing activities and to the extent that the data importer can disclose, the data importer does not expect to be the target of requests/demands pursuant to national security or intelligence agencies for disclosure of EU personal data.

#	Factor	Response
Such data transfers are not directly nor practically in scope of requests/demands from national security or intelligence agencies for disclosure of EU personal data.		

D. Supplementary Measures

Notwithstanding the Conclusion set forth in the above TRA, ULG has also adopted the following supplemental measures. We believe that by implementing such supplemental measures, we are following best practices and are demonstrating our serious commitment to the protection of customer data.

Contractual safeguards	ULG and NAVEX Global have entered into supplementary contractual assurances as an amendment to the data processing addendum.
	The SCCs themselves contain a number of contractual commitments by ULG and NAVEX Global, aimed at serving as safeguards for EU personal data. We have also entered into a robust general data processing addendum.
	Implement other transparency, audit and monitoring obligations on ULG regarding the level of government access to data.
Organizational safeguards	ULG maintains written processes and procedures provide for review of and limit the scope of EU personal data disclosed by ULG in response to requests from public authorities.
	ULG maintains internal record of requests made by public authorities concerning EU personal data.
	ULG takes steps to limit the volume of disclosed data, where possible.
	ULG takes data minimization measures such as redacting unnecessary identifiable personal data or personal data that may be of increased interest to intelligence agencies before complying with a request to disclosure EU personal data.
	All requests from law enforcement for data will be handled by a qualified individual as dictated by ULG's written policies.
Technical safeguards	Encrypt personal data in transit.
	Enhance access controls.

	Enhance data minimization (e.g., store the least amount of data necessary).
	Calls are not recorded, ensuring the limit timespan for processing personal data "in the clear" (i.e., in identifiable form).

Conclusion

Having regard to the level of risk of the data transfer (**very limited risk**), ULG and NAVEX Global consider that the measures identified above are **sufficient and effective** in light of the circumstances of the transfers, in conjunction with the supplementary measures and safeguards provided by the SCCs, to allow the data importer to comply with its obligations under the SCCs and provide an appropriate level of protection for the transfer.

Hotline and Incident Management US Hosted Sub-Processing Activity: Translations with Transatlantic Translations

NAVEX GLOBAL SUB-PROCESSING ACTIVITY

US HOSTED HOTLINE AND INCIDENT MANAGEMENT – WEB REPORT TRANSLATIONS TRANSFER RISK ASSESSMENT

I. SCOPE

This TRA applies to NAVEX Global's US Hosted Incident Management customers. This TRA applies specifically to the web report translation services taking place as part of the Incident Management services.

As part of NAVEX Global's Incident Management service component, customers are provided with a web intake site to receive reports submitted via the web. When a report is received via the website in a language other than English, an electronic copy of the report is sent, in its original language, to a secure web-portal (the "Translation Management System") managed by Transatlantic Translations. A translator, who may be located in various countries throughout the world, then logs into the Translation Management System, performs the translation, and sends the report back through the Translation Management System for the NAVEX Global communication specialist to retrieve. The Translation Management System for Transatlantic Translation resides on servers owned by Wordbee S.A. in Amsterdam---via Microsoft Azure. Once the translation is complete and returned to NAVEX Global, the report is deleted permanently within the Translation Management System.

II. ASSESSING THE ADEQUACY OF EU/UK DATA TRANSFERS – WEB REPORT TRANSLATION SERVICES

In assessing the adequacy of transfers of personal data from the EU/UK to NAVEX Global's sub-processor pursuant to the web report translation services provided by said sub-processor, we have taken the following steps:

1. **STEP 1:** Identified the relevant data transfers and the legal mechanism that NAVEX Global and sub-processor is relying on for such transfers (e.g., SCCs).

2. **STEP 2:** Conducted due diligence and collected information about the scope of the transfers, the exposure of the sub-processor to local law that may require disclosure of EU personal data about individuals, and any other relevant information.

3. **STEP 3:** Completed the "Transfer Risk Assessment" in **Section IV** to assess whether the SCCs is effective in light of all circumstances of the transfer.

4. **STEP 4:** Included additional "Supplementary Measures" as set forth in **Section IV (D)**.

5. **STEP 5:** Documented the assessment for accountability purposes. We encourage our customers to do the same.

6. **STEP 6:** NAVEX Global and its sub-processor is responsible for the periodic review of the assessment, which should take place at least annually, to ensure that the transfer of the EU personal data continues to be afforded an adequate level of protection.

III. TRANSFER RISK ASSESSMENT

Name Of Data Importer: Transatlantic Translations Company, LLC **(**NAVEX Global's sub-processor)
Completed By: NAVEX Global's Privacy Team and Vicki Crothall
Date: 25 September 2021

A. Type of Data Importer

Name of data importer: Transatlantic Translations Company, LLC, on behalf of itself and Transatlantic Translations Limited ("TTG"). The Processor to Processor SCCs between NAVEX Global and TTG is part of a master services agreement between NAVEX Global and TTG.

Does TTG provide the following services to NAVEX Global:

	Data Importer	
Telecommunications	☐ Yes	☒ No
Other electronic communications (such as an Internet Service Provider or a provider of email, text message, VoIP, remote desktop or VPN services)?	☐ Yes	☒ No
Remote computing services	☐ Yes	☒ No
Other communications service where there may be access to wire or electronic communications	☒ Yes	☐ No

TTG acknowledges that its services could be viewed as meeting the definition of a communication service.

B. Details of Data Transfers

Data transfer mechanism Appropriate Processor to Processor SCCs between TTG and NAVEX Global.
Scope of personal data covered by the data transfer mechanism in place The SCCs cover transfers of EU personal data from the EEA/UK to third countries, including the

following categories of data subjects:

- Employees of customer Data Controller
- Clients, business partners and vendors of customer Data Controller (who are natural persons)
- Employees or contact persons of customer Data Controllers' third-party suppliers, business partners and vendors
- Customer Data Controller's users authorized by data exporter to use the relevant Service(s)

C. Transfer Risk Assessment

The table below aids identification and evaluation of risk factors in relation to the specific data transfer. The assessment of each risk factor is recorded in appropriate detail.

#	Factor	Response
Scope of the transfers		
1.	What is the type of transfer?	Web report translation services. There is no persistent storage or access by TTG. The processing by the individual translators is limited to the performance of the translation of the given web report.
2.	Is the transfer necessary?	Yes. The transfer is critical and necessary to provide the services to NAVEX Global, on behalf of NAVEX Global's customers. To intake reports from individuals on important ethics and compliance matters, we have to be able the provide the best language support resources available, to allow these reporters effective whistle blowing capabilities.
3.	Is the transfer proportionate?	Yes. The transfer is strictly limited to translating the reported information submitted via the website.
4.	Is the transfer occasional/non-routine or frequent/routine?	The transfer is occasional and non-routine to TTG translators on a per report basis.
5.	Will the transferred personal data be processed for a relatively long or short period of time?	Personal data transferred is processed for a relatively short period of time, in order to translate the report.
6.	Is the transferred data encrypted and/ or pseudonymized?	Yes. Encryption - all data, including all files uploaded to the Wordbee Translation Management System, all translated data,

#	Factor	Response
		translation memories, projects, jobs, users, and companies, etc.—is encrypted at transfer time and while at rest. The encryption technologies that Wordbee uses, for the Translation Management System, meet industry security standards for preventing malicious attacks and data theft and for ensuring that data is protected.
Specific circumstances of the transfer		
7.	What are the purposes for which the data are transferred and processed?	To provide the best language translation support to web reporters.
8.	What are the types of entities involved in the processing?	TTG is a data sub-processor and a private company. NAVEX Global is a data processor and private company. NAVEX Global's customers are the data controllers and may consist of both private and public companies.
9.	In which sector does the transfer occur?	NAVEX Global provides risk and compliance management SaaS based software. ***This factor is especially important as the purposes of our services are to enable organizations to support their risk, ethics, and compliance programs. ***
10.	What are the categories of personal data transferred?	As instructed by NAVEX Global's customer, including but not limited to: • name, job title, job position, location, employer, relationship with the organization, e-mail address, telephone number, log-in credentials, date of birth; • for whistle-blower hotline and case management reports, in addition to the foregoing, the following may also be captured: o facts reported by a reporter about a suspected violation, including how and where the suspected violation occurred and how the reporter learned about the suspected violation; o identity, function and contact details of individuals allegedly involved in the suspected violation; and o identity, function and contact details of individuals who could provide information relating to the suspected violation. Given the nature of incident management

#	Factor	Response
		services, reporters may submit sensitive categories of data in a report. NAVEX Global recommends its customers have strict policies around the management of such report data in their use of the services, in accordance with the laws subject to them.
11.	What is the format of the personal data to be transferred?	When access is provided to an individual translator for the purposes described in this TRA, personal data must be accessible in the clear to provide the translation. The data is encrypted as detailed above.
12.	What is the storage location of the data transferred?	The European Union via the Wordbee Translator and ultimately via NAVEX Global's secure data centres in the United States.
13.	What are the sub-sub-processing activities?	Please see details here: https://www.navexglobal.com/en-us/service-hosting-providers. For the translation services, TTG engages Wordbee for the secure hosting of the translation management system. Wordbee utilizes the secure environment of Microsoft Azure. Storage and hosting as part of these sub-sub-processing activities is located within the European Union.
Importer's exposure to government surveillance and practical application of Section 702 FISA		
14.	Is the data importer's sector or business directly subject to such laws in its jurisdiction that permit government access to personal data, or require the assistance of data importer to disclose personal data to public authorities, for surveillance and intelligence gathering purposes?	No, TTG's business is currently not directly subject to such laws.
	a. Specifically, what is data importer's analysis regarding third country surveillance laws, especially Section 702 FISA, under the SCCs and EDPB Guidance?	1) Data exporters may decide to proceed with the transfer without supplementary measures, if they consider there to be no reason to believe that the relevant and problematic legislation (for example, those in the U.S.) will be applied, in practice, to the transferred data and/or TTG. a. In our reasonable opinion upon internal and outside counsel review, we do not find third country surveillance laws, including Section 702 FISA from the U.S., to practically apply to these transfers. b. It is important to note that given the

#	Factor	Response
		broad definitions of these laws, the vast majority of organizations are going to have to acknowledge their potential application. However, this does not mean they directly apply or practically apply in practice. c. We believe TTG is generally out of scope and that these laws are overall not going to apply to the services we provide, as the intent is for surveillance of certain telecom and internet service providers for targeted information. This typically involves surveillance of real time emails, texts, and chat conversations. The foregoing is not what NAVEX Global nor TTG provides and in order to obtain this sought for information, authorities would pursue those providers directly as it would be impractical to make a request through TTG. 2) Data exporters may also take into consideration documented practical experience of data importer with relevant prior instances of requests for access received from public authorities, including those in the U.S. a. *** To this point, TTG has never received a Section 702 FISA request, an EO 12.333 request or order, or any other country access request.** * b. The EDPB Guidance implies that the lack of requests received in the past plus no prohibition on providing information about such requests, could be sufficient to conclude Section 702 FISA does not apply in practice. Note there is no prohibition on TTG to provide information about these requests. 3) If you conclude Section 702 FISA, or any other potential similar types of surveillance law, does not apply in practice to the particular transfer, it is possible to proceed with the transfer without any supplementary measures. **While NAVEX Global and TTG take the approach that Section 702 FISA does not apply in practice, we still have elected to**

#	Factor	Response
		provide for supplementary measures with regard to these transfers. Please see Section IV (D).
15.	Within the last three (3) years, has the data importer received requests/demands from public authorities in its jurisdiction to disclose EU personal data?	Based on available information, TTG entities in the U.S. do not receive requests/demands for disclosure of, or access to, EU personal data.
	a. Approximately how many requests/demands from public authorities has the data importer received in that time period concerning EU personal data?	None, to the best of our knowledge.
	b. Approximately how many of these requests/demands are pursuant to criminal law procedure in the destination country? *[Regular court proceedings are not the issue under Schrems II, but intelligence programs are scrutinized.]*	None, to the best of our knowledge.
	c. Approximately how many of these requests/demands are pursuant to national security or intelligence agencies in the destination country?	None, to the best of our knowledge. The data importer can represent that it has not received requests/demands from intelligence agencies.
	d. Has the data importer been able to contest/minimize such disclosure of EU personal data, where appropriate?	Not applicable.
	e. What types of EU personal data has the data importer been required to disclose to public authorities in its jurisdiction?	Not applicable.
16.	How likely is it that the data importer will receive bulk data surveillance requests to disclose EU personal data to public authorities in its jurisdiction in the future (e.g., based on factors such as the type of services provided and sector in which the data importer operates, its size, number of customers and reputation)?	Unlikely. TTG's entities in the U.S. do not receive requests/demands by public authorities for disclosure of, or access to, EU personal data, and have no reason to believe that they might receive such in the future.
17.	Does the data importer maintain annual reports or statistics regarding requests/demands received from law enforcement or intelligence agencies (e.g., number/type of requests/demands, requesting authority, etc.)?	Not applicable. TTG has not received requests from public authorities for EU personal data under the SCCs or otherwise. As a result, if TTG gets such requests in the future, it will notify NAVEX Global and this TRA will be updated accordingly.
18.	Does the data importer maintain a written procedure(s) for: 1. Responding to or challenging requests/ demands of law enforcement or intelligence agencies that apply to EU personal data? 11. Informing customers of requests/demands from law	Yes. While TTG has never received such requests, it does have a policy and procedure should the event ever happen. Included in the procedure, there will be a list of any and all such requests.

#	Factor	Response
	enforcement or intelligence agencies where permitted by applicable law?	
19.	Are the data importer's commitments enabling data subjects to exercise their rights as provided in the SCCs thwarted by the laws and/or practices in the U.S. and any other third countries involved, or can these rights be effectively applied in practice?	Data subjects' rights can be effectively applied in practice. TTG has never encountered a situation where it felt it could not enable data subject rights, including judicial redress. We do not believe the laws subject to us prevent us from enabling, supporting, and fulfilling data subject rights under the SCCs.
Onward transfers and exposure to government surveillance		
20.	Does the data importer share EU personal data further with third-party data recipients in [the U.S./other jurisdiction]?	Yes. TTG utilizes Wordbee specifically for their Translation Management System for the processing of all Translation requests. Only TTG Secure Linguists complete the actual translation work.
21.	What measures does the third-party data recipient take to ensure the protection of EU personal data transferred to it?	Where TTG engages Wordbee that have access to EU personal data, TTG enters into written agreements with Wordbee that include safeguards for EU personal data in accordance with the GDPR requirements.
22.	What assurances has the data importer received from third-party data recipients with respect to requests/demands for EU personal data from [U.S./other jurisdiction] public authorities?	TTG has updated written agreements, or has ensured such updates are in progress, with Wordbee to include additional measures for the protection of EU personal data, where required.
23.	Is the vendor's (or its sub-processor's) sector or business directly subject to such laws in its jurisdiction that permit government access to personal data, or require the assistance of data importer to disclose personal data to public authorities, for surveillance and intelligence gathering purposes?	No, TTG does not believe in its reasonable opinion that it or its sub-processors are directly subject to such laws in their jurisdiction.

Conclusion/Risk of transfers

Very limited-risk data transfer

In particular, TTG and NAVEX Global identified the following factors (based on the assessment documented above and any additional information), that are likely to indicate a very limited-risk transfer:

No further processing outside of translation of a given web report takes place.

The data importer has never received requests/demands from intelligence services for disclosure of EU personal data.

The data importer has received limited requests/demands from public authorities for disclosure of EU personal data (such as for disclosure of employee data), but the requests related to regular criminal law procedure and did not go beyond what is necessary and proportionate to meet the purpose of the request.

#	Factor	Response
	The data importer has a process in place for handling and contesting public authority access requests, if received. Based on the nature of its services and data processing activities, the data importer does not expect to be the target of requests/demands pursuant to national security or intelligence agencies for disclosure of EU personal data. Such data transfers are not directly nor practically in scope of requests/demands from national security or intelligence agencies for disclosure of EU personal data.	

D. Supplementary Measures

Notwithstanding the Conclusion set forth in the above TRA, TTG has also adopted the following supplemental measures. We believe that by implementing such supplemental measures, we are following best practices and are demonstrating our serious commitment to the protection of customer data.

Contractual safeguards	TTG and NAVEX Global have entered into supplementary contractual assurances as an amendment to the data processing addendum.
	The SCCs themselves contain a number of contractual commitments by TTG and NAVEX Global, aimed at serving as safeguards for EU personal data. We have also entered into a robust general data processing addendum.
	TTG is committed to implementing other transparency, audit and monitoring obligations regarding the level of government access to data, including, a policy and process to address any potential requests for disclosure to governmental agencies around the world. This is to include a legend of any such request received and actioned.
Organizational safeguards	TTG maintains written processes and procedures provide for review of and limit the scope of EU personal data disclosed by TTG in response to requests from public authorities.
	TTG would maintain internal record of requests made by public authorities concerning EU personal data.
	TTG takes steps to limit the volume of disclosed data, where possible.
	TTG would take data minimization measures such as redacting unnecessary identifiable personal data or personal data that may be of increased interest to intelligence agencies before complying with a request to disclosure EU personal data.
Technical safeguards	Encrypt personal data in transit, as detailed above.

	Encrypt personal data at rest, as detailed above.
	Translation Management System encryption key kept in the EU.
	Appropriate access controls.
	Limit timespan is ensured for using personal data "in the clear" (i.e., in identifiable form).
	Store personal data in the EU and enable only remote access or view-only access.

Conclusion

Having regard to the level of risk of the data transfer (**very limited risk**), TTG and NAVEX Global consider that the measures identified above are **sufficient and effective** in light of the circumstances of the transfers, in conjunction with the supplementary measures and safeguards provided by the SCCs, to allow the data importer to comply with its obligations under the SCCs and provide an appropriate level of protection for the transfer.

Hotline and Incident Management US Hosted Sub-Processing Activity: Translations with United Language Group

NAVEX GLOBAL SUB-PROCESSING ACTIVITY

US HOSTED HOTLINE AND INCIDENT MANAGEMENT – WEB REPORT TRANSLATIONS TRANSFER RISK ASSESSMENT

I. SCOPE

This TRA applies to NAVEX Global's US Hosted Incident Management customers. This TRA applies specifically to the web report translation services taking place as part of the Incident Management services.

As part of NAVEX Global's Incident Management service component, customers are provided with a web intake site to receive reports submitted via the web. When a report is received via the website in a language other than English, an electronic copy of the report is sent, in its original language, to a secure web-portal (the "Translation Management System") managed by either United Language Group or Transatlantic Translations. This TRA applies to United Language Group only. A translator, who may be located in various countries throughout the world, then logs into the Translation Management System, performs the translation, and sends the report back through the Translation Management System for the NAVEX Global communication specialist to retrieve. The Translation Management System for United Language Group resides on colocation servers in the United States.

Once the translation is complete, it is securely stored within ULG's Translation Management System, then archived down and ultimately deleted following this schedule:

For the Contact Center group all NAVEX all material is deleted after 5 business days.

II. ASSESSING THE ADEQUACY OF EU/UK DATA TRANSFERS – WEB REPORT TRANSLATION SERVICES

In assessing the adequacy of transfers of personal data from the EU/UK to NAVEX Global's sub-processor pursuant to the web report translation services provided by said sub-processor, we have taken the following steps:

1. **STEP 1:** Identified the relevant data transfers and the legal mechanism that NAVEX Global and sub-processor is relying on for such transfers (e.g., SCCs).

2. **STEP 2:** Conducted due diligence and collected information about the scope of the transfers, the exposure of the sub-processor to local law that may require disclosure of EU personal data about individuals, and any other relevant information.

3. **STEP 3:** Completed the "Transfer Risk Assessment" in **Section IV** to assess whether the SCCs is effective in light of all circumstances of the transfer.

4. **STEP 4:** Included additional "Supplementary Measures" as set forth in **Section IV (D)**.

5. **STEP 5:** Documented the assessment for accountability purposes. We encourage our customers to do the same.

6. **STEP 6:** NAVEX Global and its sub-processor is responsible for the periodic review of the assessment, which should take place at least annually, to ensure that the transfer of the EU personal data continues to be afforded an adequate level of protection.

III. TRANSFER RISK ASSESSMENT

Name Of Data Importer: United Language Group, Inc. **(**NAVEX Global's sub-processor)
Completed By: NAVEX Global's Privacy Team and ULG Privacy Representatives
Date: 25 September 2021

A. Type of Data Importer

Name of data importer: United Language Group, Inc. ("ULG"). The Processor to Processor SCCs between NAVEX Global and ULG is part of a master services agreement between NAVEX Global and ULG.

Does ULG provide the following services to NAVEX Global:

	Data Importer	
Telecommunications	☐ Yes	☒ No
Other electronic communications (such as an Internet Service Provider or a provider of email, text message, VoIP, remote desktop or VPN services)?	☒ Yes	☐ No
Remote computing services	☐ Yes	☒ No
Other communications service where there may be access to wire or electronic	☒ Yes	☐ No

communications		

ULG acknowledges that its services could be viewed as meeting the definition of a communication service.

B. Details of Data Transfers

Data transfer mechanism Appropriate Processor to Processor SCCs between ULG and NAVEX Global.
Scope of personal data covered by the data transfer mechanism in place The SCCs cover transfers of EU personal data from the EEA/UK to third countries, including the following categories of data subjects: • Employees of customer Data Controller • Clients, business partners and vendors of customer Data Controller (who are natural persons) • Employees or contact persons of customer Data Controllers' third-party suppliers, business partners and vendors • Customer Data Controller's users authorized to use the relevant Service(s)

C. Transfer Risk Assessment

The table below aids identification and evaluation of risk factors in relation to the specific data transfer. The assessment of each risk factor is recorded in appropriate detail.

#	Factor	Response
Scope of the transfers		
1.	What is the type of transfer?	Web report translation services. There is no persistent storage or access by ULG. The processing by the individual translators is limited to the performance of the translation of the given web report.
2.	Is the transfer necessary?	Yes. The transfer is critical and necessary to provide the services to NAVEX Global, on behalf of NAVEX Global's customers. To intake reports from individuals on important ethics and compliance matters, we have to be able the provide the best language support resources available, to allow these reporters effective whistle blowing capabilities.
3.	Is the transfer proportionate?	Yes. The transfer is strictly limited to translating the reported information submitted via the website.
4.	Is the transfer occasional/non-routine or	

#	Factor	Response
	frequent/routine?	The transfer is occasional and non-routine to ULG translators on a per report basis.
5.	Will the transferred personal data be processed for a relatively long or short period of time?	Personal data transferred is processed for a relatively short period of time, in order to translate the report.
6.	Is the transferred data encrypted and/ or pseudonymized?	Yes, Encryption -- Data is encrypted at rest (AES256).
Specific circumstances of the transfer		
7.	What are the purposes for which the data are transferred and processed?	To provide the best language translation support to web reporters.
8.	What are the types of entities involved in the processing?	ULG is a data sub-processor and a private company. ULG's network of translators may be employees, contractors or subcontractors of ULG. NAVEX Global is a data processor and private company. NAVEX Global's customers are the data controllers and may consist of both private and public companies.
9.	In which sector does the transfer occur?	NAVEX Global provides risk and compliance management SaaS based software. ***This factor is especially important as the purposes of our services is to enable organizations support their risk, ethics, and compliance programs. *** ULG provides SaaS based software and a range of interpretation and translation services.
10.	What are the categories of personal data transferred?	• name, job title, job position, location, employer, relationship with the organization, e-mail address, telephone number; • for whistle-blower hotline reports, in addition to the foregoing, the following may also be captured: o facts reported by a reporter about a suspected violation, including how and where the suspected violation occurred and how the reporter learned about the suspected violation; o identity, function and contact details of individuals allegedly involved in the suspected

#	Factor	Response
		violation; and o identity, function and contact details of individuals who could provide information relating to the suspected violation. Given the nature of incident management services, reporters may submit sensitive categories of data in a report. NAVEX Global recommends its customers have strict policies around the management of such report data in their use of the services, in accordance with the laws subject to them.
11.	What is the format of the personal data to be transferred?	When access is provided to an individual translator for the purposes described in this TRA, personal data must be accessible in the clear to provide the translation. ULG utilizes encryption at rest (AES256).
12.	What is the storage location of the data transferred?	For ULG, report data is temporarily stored in the United States, to ultimately be stored with NAVEX Global. NAVEX Global's secure data centres are located in the United States.
13.	What are the sub-sub-processing activities?	Not applicable.
Importer's exposure to government surveillance and practical application of Section 702 FISA		
14.	Is the data importer's sector or business directly subject to such laws in its jurisdiction that permit government access to personal data, or require the assistance of data importer to disclose personal data to public authorities, for surveillance and intelligence gathering purposes?	No. ULG's business is currently not directly subject to such laws. In light of the scope of FISA, ULG does provide ancillary services which would fall within the definition of an electronic communication service under FISA. However, ULG does not consider itself involved in a sector that is universally accepted as being subject to a FISA remit (such sectors principally being telcos, mail exchanges, web hosting, data center providers and other cloud providers and social media organizations).
	a. Specifically, what is data importer's analysis regarding third country surveillance laws, especially Section 702 FISA under the SCCs and EDPB Guidance?	1) Data exporters may decide to proceed with the transfer without supplementary measures, if they consider there to be no reason to believe that the relevant and problematic legislation (for example, those in the U.S.) will be applied, in practice, to the transferred data and/or ULG. a. In our reasonable opinion upon internal and outside counsel review,

#	Factor	Response
		we do not consider ULG to be active in a sector which would make it a target for access orders pursuant to FISA 702, nor would be consider ULG's data processing activities of interest to US intelligence agencies under EO 12.333, PPD-28, the Cloud Act, or other problematic third country surveillance laws. b. It is important to note that given the broad definitions of these laws, the vast majority of organizations are going to have to acknowledge their potential application. However, this does not mean they directly apply or practically apply in practice. c. We believe ULG is generally out of scope and that these laws are overall not going to apply to the services we provide, as the intent is for surveillance of certain telecom and internet service providers for targeted information. This typically involves to surveillance of real time emails, texts, and chat conversations. The foregoing is not what ULG nor NAVEX Global provides and in order to obtain this sought for information, authorities would pursue those providers directly as it would be impractical to make a request through ULG. 2) Data exporters may also take into consideration documented practical experience of data importer with relevant prior instances of requests for access received from public authorities in the U.S. a. ***To this point, ULG has never received a Section 702 FISA request or an EO 12.333 request or order.** * b. The EDPB Guidance implies that the lack of requests received in the past plus no prohibition on providing information about such requests, could be sufficient to conclude Section 702 FISA does not apply in practice. Note there is no prohibition on ULG to provide information about these requests. 3) If you conclude Section 702 FISA does not

#	Factor	Response
		apply in practice to the particular transfer, it is possible to proceed with the transfer without any supplementary measures. **While NAVEX Global takes the approach that Section 702 FISA does not apply in practice, we still have elected to provide for supplementary measures with regard to these transfers. Please see Section IV (D).**
15.	Within the last three (3) years, has the data importer received requests/demands from public authorities in its jurisdiction to disclose EU personal data?	Based on available information, ULG's entities in the US do not routinely receive requests/demands for disclosure of, or access to, EU personal data.
	a. Approximately how many requests/demands from public authorities has the data importer received in that time period concerning EU personal data?	None, to the best of our knowledge.
	b. Approximately how many of these requests/demands are pursuant to criminal law procedure in the destination country? *[Regular court proceedings are not the issue under Schrems II, but intelligence programs are scrutinized.]*	None, to the best of our knowledge.
	c. Approximately how many of these requests/demands are pursuant to national security or intelligence agencies in the destination country?	None, to the best of our knowledge. The data importer can represent that it has not received requests/demands from intelligence agencies. ULG is not subject to FISA 702 requests.
	d. Has the data importer been able to contest/minimize such disclosure of EU personal data, where appropriate?	Not applicable.
	e. What types of EU personal data has the data importer been required to disclose to public authorities in its jurisdiction?	Not applicable.
16.	How likely is it that the data importer will receive bulk data surveillance requests to disclose EU personal data to public authorities in its jurisdiction in the future (e.g., based on factors such as the type of services provided and sector in which the data importer operates, its size, number of customers and reputation)?	Unlikely. ULG does not consider itself active within a sector which is the subject to surveillance gathering activities and consider it extremely remote that it would receive any bulk data surveillance requests.
17.	Does the data importer maintain annual reports or statistics regarding requests/demands received from law enforcement or intelligence agencies (e.g., number/type of requests/demands, requesting authority, etc.)?	Yes. This is maintained for ULG internal purposes and are to be provided to NAVEX Global in accordance with the terms of the data processing agreement.
18.	Does the data importer maintain a written procedure(s) for:	No, not applicable. ULG has not received requests from public authorities for EU personal data under the SCCs or otherwise.

#	Factor	Response
	1. Responding to or challenging requests/ demands of law enforcement or intelligence agencies that apply to EU personal data? 12. Informing customers of requests/demands from law enforcement or intelligence agencies where permitted by applicable law?	If ULG gets such requests in the future, it will escalate the matter and as such would follow our documented notification process requiring & insuring that we would notify NAVEX Global. As a result, if ULG gets such requests in the future, it will notify NAVEX Global (unless otherwise strictly prohibited) and this TRA will be updated accordingly. ULG and NAVEX Global entered into a contractual agreement requiring ULG to cooperate and mutually agree on any appropriate actions, to notify NAVEX Global of any requests unless explicitly required otherwise under applicable law, to put any access request on hold, and to use reasonable efforts to obtain the right to waive any notice prohibitions and oppose any such request and contest its legal validity where possible and permitted. The contract additionally ensures ULG will not make any disclosures that are determined to be massive, disproportionate, and indiscriminate in a manner that would go beyond what is necessary in a democratic society. ULG is obliged to document and demonstrate to the assessments made and the actions taken. ULG undertakes to regularly review, assess, and continuously monitor the scope of the access to personal data by public authorities in the countries where ULG is processing personal data, as well as the safeguards and recourses in place to protect data subjects, and to immediately inform NAVEX Global in the case of a change in applicable law that would materially impact such access by public authorities or recourses available to data subjects.
19.	Are the data importer's commitments enabling data subjects to exercise their rights as provided in the SCCs thwarted by the laws and/or practices in the U.S. and any other third countries involved, or can these rights be effectively applied in practice?	ULG does not consider itself to be active in a sector which is considered a target for FISA 702 related surveillance activities and maintains a data subject access request policy in respect of any traditional Data Production Request orders.
Onward transfers and exposure to government surveillance		
20.	Does the data importer share EU personal data further with third-party data recipients?	Not applicable.
Conclusion/Risk of transfers **Very limited-risk data transfer** **In particular, ULG and NAVEX Global identified the following factors (based on the assessment documented above and any additional information), that are likely to indicate a very limited-risk transfer:**		

#	Factor	Response
		No further processing outside of translation of a given web report takes place. The data importer is not active in a sector which is regarded as subject to requests/demands from intelligence services. The data importer has never received requests/demands from intelligence services for disclosure of EU personal data.The data importer has a process in place for handling and contesting public authority access requests, if received. Based on the nature of its services and data processing activities and to the extent that the data importer can disclose, the data importer does not expect to be the target of requests/demands pursuant to national security or intelligence agencies for disclosure of EU personal data. Such data transfers are not directly nor practically in scope of requests/demands from national security or intelligence agencies for disclosure of EU personal data.

D. Supplementary Measures

Notwithstanding the Conclusion set forth in the above TRA, ULG has also adopted the following supplemental measures. We believe that by implementing such supplemental measures, we are following best practices and are demonstrating our serious commitment to the protection of customer data.

Contractual safeguards	ULG and NAVEX Global have entered into supplementary contractual assurances as an amendment to the data processing addendum.
	The SCCs themselves contain a number of contractual commitments by ULG and NAVEX Global, aimed at serving as safeguards for EU personal data. We have also entered into a robust general data processing addendum.
	Implement other transparency, audit and monitoring obligations on ULG regarding the level of government access to data.
Organizational safeguards	ULG maintains written processes and procedures provide for review of and limit the scope of EU personal data disclosed by ULG in response to requests from public authorities.
	ULG maintains internal record of requests made by public authorities concerning EU personal data.
	ULG takes steps to limit the volume of disclosed data, where possible.
	ULG takes data minimization measures such as redacting unnecessary identifiable personal data or personal data that may be of increased interest to intelligence agencies before complying with a request to disclosure EU personal data.

	All requests from law enforcement for data will be handled by a qualified individual as dictated by ULG's written policies.
Technical safeguards	Encrypt personal data in transit.
	Encrypt personal data at rest.
	Enhance access controls.
	Enhance data minimization (e.g., store the least amount of data necessary).
	Limit timespan for using personal data "in the clear" (i.e., in identifiable form).

Conclusion

Having regard to the level of risk of the data transfer (**very limited risk**), ULG and NAVEX Global consider that the measures identified above are **sufficient and effective** in light of the circumstances of the transfers, in conjunction with the supplementary measures and safeguards provided by the SCCs, to allow the data importer to comply with its obligations under the SCCs and provide an appropriate level of protection for the transfer.

Hotline and Incident Management US Hosted Sub-Processing Activity: Contact Centre Services with Teleperformance

NAVEX GLOBAL SUB-PROCESSING ACTIVITY

US HOSTED HOTLINE AND INCIDENT MANAGEMENT – CONTACT CENTRE SERVICES

I. SCOPE

This TRA applies to NAVEX Global's US Hosted Hotline and Incident Management customers. This TRA applies specifically to the contact centre services taking place as part of the Hotline and Incident Management services.

As part of NAVEX Global's Hotline service component, customers are provided with telephony to receive reports submitted via telephone. As part of NAVEX Global's Incident Management service component, customers are provided with a web intake site to receive reports submitted via the web. NAVEX Global utilizes two sub-processors for additional contact centre support services, for the intake and dispatch of the phone reports. This TRA applies to Teleperformance Colombia S.A.S. only. Teleperformance Colombia S.A.S. is also utilized for the dispatch of web reports. The contact centre agents are located in Colombia and Guyana. NAVEX Global discloses Nicaragua and Peru as backup locations, however, at the time of this TRA there is no processing in Nicaragua nor Peru.

II. ASSESSING THE ADEQUACY OF EU/UK DATA TRANSFERS – CONTACT CENTRE SERVICES

In assessing the adequacy of transfers of personal data from the EU/UK to NAVEX Global's sub-processor pursuant to the contact centre services provided by said sub-processor, we have taken the following steps:

1. **STEP 1:** Identified the relevant data transfers and the legal mechanism that NAVEX Global and sub-processor is relying on for such transfers (e.g., SCCs).

2. **STEP 2:** Conducted due diligence and collected information about the scope of the transfers, the exposure of the sub-processor to local law that may require disclosure of EU personal data about individuals, and any other relevant information.

3. **STEP 3:** Completed the "Transfer Risk Assessment" in **Section IV** to assess whether the SCCs is effective in light of all circumstances of the transfer.

4. **STEP 4:** Included additional "Supplementary Measures" as set forth in **Section IV (D)**.

5. **STEP 5:** Documented the assessment for accountability purposes. We encourage our customers to do the same.

6. **STEP 6:** NAVEX Global and its sub-processor is responsible for the periodic review of the assessment, which should take place at least annually, to ensure that the transfer of the EU personal data continues to be afforded an adequate level of protection.

III. TRANSFER RISK ASSESSMENT

Name Of Data Importer: Telepeformance Colombia SAS **(**NAVEX Global's sub-processor)
Completed By: NAVEX Global's Privacy Team and Teleperformance Colombia S.A.S.
Date: 25 September 2021

A. Type of Data Importer

Name of data importer: Teleperformance Colombia SAS ("TP"). The Processor to Processor SCCs between NAVEX Global and TP is part of a master services agreement between NAVEX Global and TP.

Does TP provide the following services to NAVEX Global:

	Data Importer	
Telecommunications	☐ Yes	☒ No
Other electronic communications (such as an Internet Service Provider or a provider of email, text message, VoIP, remote desktop or VPN services)?	☐ Yes	☒ No
Remote computing services	☐ Yes	☒ No
Other communications service where there may be access to wire or electronic communications	☒ Yes	☐ No

For clarity, TP provides Business Process Outsourcing services that include the provision of contact center services with telephone specialists that attend whistleblowers´ claims or requests within NAVEX Global systems by means of a virtual desktop infrastructure ("VDI") connection through TP devices.

B. Details of Data Transfers

Data transfer mechanism Appropriate Processor to Processor SCCs between TP and NAVEX Global.
Scope of personal data covered by the data transfer mechanism in place The SCCs cover transfers of EU personal data from the EEA/UK to Colombia and Guyana, including the following categories of data subjects: • Employees of customer Data Controller • Clients, business partners and vendors of customer Data Controller (who are natural persons) • Employees or contact persons of customer Data Controllers' third-party suppliers, business partners and vendors • Customer Data Controller's users authorized to use the relevant Service(s)

C. Transfer Risk Assessment

The table below aids identification and evaluation of risk factors in relation to the specific data transfer. The assessment of each risk factor is recorded in appropriate detail.

#	Factor	Response
Scope of the transfers		
1.	What is the type of transfer?	Intake and submission of phone and web reports as part of the contact centre services. Personal data is not copied over or stored with TP. The processing by the individual contact centre agent is limited to the intake and submission of the given phone or web report in real time. TP personnel input the information into NAVEX Global's proprietary and secure systems to be dispatched into the customer's case management system hosted in the U.S.
2.	Is the transfer necessary?	Yes. The transfer is necessary to provide the services to NAVEX Global, on behalf of NAVEX Global's customers. To intake reports from individuals on important ethics and compliance matters, we have to be able the provide the best available contact centre and language support resources available, to allow these reporters effective whistle blowing capabilities.
3.	Is the transfer proportionate?	Yes. The transfer is strictly limited to taking and submitting the report in real time.
4.	Is the transfer occasional/non-routine or frequent/routine?	The transfers are routine, as TP has to be

#	Factor	Response
		available to take the phone calls and dispatch reports.
5.	Will the transferred personal data be processed for a relatively long or short period of time?	Personal data transferred is processed for a relatively short period of time, in order to intake dispatch reports.
6.	Is the transferred data encrypted, pseudonymized or otherwise processed in an unintelligible form, during all stages of the processing (i.e., in transit, in rest and while in use)?	Yes, Encryption in transit and at rest upon NAVEX Global's secure data centres. Any session TP accesses to NAVEX Global systems are over an encrypted session. Obfuscation, by which the personal data is masked with a particular ID, code, character, or other modified content in order to safeguard the original personal data or any sensitive data and prevent unauthorized access or use of such data.
Specific circumstances of the transfer		
7.	What are the purposes for which the data are transferred and processed?	To provide the best available contact centre resources and language support to reporters.
8.	What are the types of entities involved in the processing?	TP is a data sub-processor and a private company. NAVEX Global is a data processor and private company. NAVEX Global's customers are the data controllers and may consist of both private and public companies.
9.	In which sector does the transfer occur?	NAVEX Global provides risk and compliance management SaaS based software. ***This factor is especially important as the purposes of our services is to enable organizations support their risk, ethics, and compliance programs. ***
10.	What are the categories of personal data transferred?	• Name, job title, job position, location, employer, relationship with the organization, e-mail address, telephone number, • For whistle-blower hotline reports, in addition to the foregoing, the following may also be captured: o facts reported by a reporter about a suspected violation, including how and where the suspected violation occurred and how the reporter learned about the suspected violation, o identity, function and contact details

#	Factor	Response
		of individuals allegedly involved in the suspected violation; and o identity, function and contact details of individuals who could provide information relating to the suspected violation. Given the nature of hotline and incident management services, reporters may submit sensitive categories of data in a report. NAVEX Global recommends its customers have strict policies around the management of such report data in their use of the services, in accordance with the laws subject to them.
11.	What is the format of the personal data to be transferred?	When access is provided to an individual contact centre agent for the purposes described in this TRA, personal data is delivered through the application for the Agent and submit the phone or web report. Regarding web reports, once the Agents receive a call, they proceed to fill out an intake form which is uploaded to ICBM and/or I3 web-based tools. The form will subsequently be sent to either NAVEX Global or to the company that was mentioned within the call according to the instructions provided by NAVEX Global.
12.	What is the storage location of the data transferred?	The United States via NAVEX Global's secure servers. There is no storage of data by TP.
13.	What are the sub-sub-processing activities?	Not applicable.
Importer's exposure to government surveillance and practical application of problematic legislation		
14.	Is the data importer's sector or business directly subject to such laws in its jurisdiction that permit government access to personal data, or require the assistance of data importer to disclose personal data to public authorities, for surveillance and intelligence gathering purposes?	TP is directly subject to Law 1621 of 2013, enable government authorities to request access and use of personal data within the scope of activities related to surveillance and intelligence being in the territory of Colombia. However, according to Statutory Law 1581 of 2012, the data importer, can deny the access and use of data under its control, if the government authorities, does not comply with all legal requirements and procedures. The law only applies to TP and does not apply to NAVEX Global's business nor services. The GDPR protects the data subjects, which is a standard similar to Colombia's data privacy laws. Notwithstanding the foregoing, it is very

#	Factor	Response
		important to keep in mind that Statutory Law 1581 of 2012, develops constitutional principles, and has a higher hierarchy than Law 1621 of 2013. Due to this, Statutory Law 1581 of 2012, is the prevailing norm, when personal data is involved. Considering the scope and the applicability of Colombia´s privacy law, a government authority will not request access to NAVEX Global customers´ personal data for national security purposes or bulk surveillance programs, especially because such data is considered highly confidential and subject to higher standards of data privacy and data protection. The authority may request access solely to verify that TP is complying with the privacy law, and it is not incurring in any violation of the privacy regulations or incurring in illegal practices when processing personal data. Additionally, as further detailed herein, TP has never received a request for surveillance or intelligence gathering purposes, and to the best of TP´s knowledge, it is rare that it happens altogether.
	a. Specifically, what is data importer's analysis regarding any applicable surveillance laws in Colombia and Guyana under the SCCs and EDPB Guidance?	1) Data exporters may decide to proceed with the transfer without supplementary measures, if they consider there to be no reason to believe that any relevant and problematic legislation will be applied, in practice, to the transferred data and/or TP. a. In our reasonable opinion, upon we do not find these surveillance laws, to practically apply to these transfers. b. It is important to note that given the broad definitions of these laws, the vast majority of organizations are going to have to acknowledge their potential application. However, this does not mean they directly apply or practically apply in practice. c. We believe TP is generally out of scope and that these laws are overall not going to apply to the services we provide, as the intent is for surveillance of certain telecom and internet service providers for targeted information. This typically involves to surveillance of real time emails, texts, and chat

#	Factor	Response
		conversations. The foregoing is not what TP provides and in order to obtain this sought for information, authorities would pursue those providers directly as it would be impractical to make a request through TP. 2) Data exporters may also take into consideration documented practical experience of data importer with relevant prior instances of requests for access received from public authorities. a. ***To this point, TP has never received a request/demand from government authority to disclose personal information for security/ surveillance purposes and, additionally, Statutory Law 1581 of 2012, has established clear and broad safeguards that TP has in place in order to avoid sharing unminimized or un anonymized data in order to protect data subjects.** * b. The EDPB Guidance implies that the lack of requests received in the past plus no prohibition on providing information about such requests, could be sufficient to conclude such laws do not apply in practice. Note there is no prohibition on TP to provide information about these requests. 3) If you conclude such laws do not apply in practice to the particular transfer, it is possible to proceed with the transfer without any supplementary measures. a. **While TP takes the approach that such laws do not apply in practice, we still have elected to provide for supplementary measures with regard to these transfers. Please see Section IV (D).**
15.	Within the last three (3) years, has the data importer received requests/demands from public authorities in its jurisdiction to disclose EU personal data?	Based on available information, TP subsidiaries in Colombia and Guyana do not receive requests/demands for disclosure of, or access to, EU personal data for security or surveillance purposes.
	a. Approximately how many requests/demands from public authorities has the data importer received in that time period concerning EU personal	None, to the best of our knowledge.

#	Factor	Response
	data?	
	b. Approximately how many of these requests/demands are pursuant to criminal law procedure in the destination country? *[Regular court proceedings are not the issue under Schrems II, but intelligence programs are scrutinized.]*	None, to the best of our knowledge.
	c. Approximately how many of these requests/demands are pursuant to national security or intelligence agencies in the destination country?	None, to the best of our knowledge. The data importer can represent that it has not received requests/demands from intelligence agencies.
	d. Has the data importer been able to contest/minimize such disclosure of EU personal data, where appropriate?	Not applicable
	e. What types of EU personal data has the data importer been required to disclose to public authorities in its jurisdiction?	Not applicable
16.	How likely is it that the data importer will receive bulk data surveillance requests to disclose EU personal data to public authorities in its jurisdiction in the future (e.g., based on factors such as the type of services provided and sector in which the data importer operates, its size, number of customers and reputation)?	Unlikely. TP subsidiaries located in Colombia (and Guyana) are not likely to receive requests/demands by public authorities for disclosure of, or access to, EU personal data, and have no reason to believe that they might receive such in the future.
17.	Does the data importer maintain annual reports or statistics regarding requests/demands received from law enforcement or intelligence agencies (e.g., number/type of requests/demands, requesting authority, etc.)?	Yes.
18.	Does the data importer maintain a written procedure(s) for: 1. Responding to or challenging requests/ demands of law enforcement or intelligence agencies that apply to EU personal data? 13. Informing customers of requests/demands from law enforcement or intelligence agencies where permitted by applicable law?	Yes. The Global Privacy Office has established a procedure in order to answer government demands of every nature, how to escalate the request/demand, how to answer it, how to protect the data requested by the authority (data minimization) and finally, how to inform our customers of such requests/demands.
19.	Are the data importer's commitments enabling data subjects to exercise their rights as provided in the SCCs thwarted by the laws and/or practices in the U.S. and any other third countries involved, or can these rights be effectively applied in practice?	Applicable legislation in Colombia (including Guyana) requires companies to have in place specific channels and procedures in order to handle data subjects rights request, and we are fully compliant with those legal requirements. It is important to note that data subject rights in Colombia are almost the same as the ones consecrated in the GDPR.
Onward transfers and exposure to government surveillance		
20.	Does the data importer share EU personal data further with third-party data recipients in	Not applicable.

#	Factor	Response
	[the U.S./other jurisdiction]?	

Conclusion/Risk of transfers

Very limited-risk data transfer

In particular, TP and NAVEX Global identified the following factors (based on the assessment documented above and any additional information), that are likely to indicate a very limited-risk transfer:

No further processing outside of phone intake and submission takes place.

The data importer has never received requests/demands from intelligence services for disclosure of EU personal data.

The data importer has received limited requests/demands from public authorities for disclosure of EU personal data (such as for disclosure of employee data), but the requests related to regular criminal law procedure and did not go beyond what is necessary and proportionate to meet the purpose of the request.

The data importer has a process in place for handling and contesting public authority access requests, if received.

Based on the nature of its services and data processing activities, the data importer does not expect to be the target of requests/demands pursuant to national security or intelligence agencies for disclosure of EU personal data.

Such data transfers are not directly nor practically in scope of requests/demands from national security or intelligence agencies for disclosure of EU personal data.

D. Supplementary Measures

Notwithstanding the Conclusion set forth in the above TRA, TP has also adopted the following supplemental measures. We believe that by implementing such supplemental measures, we are following best practices and are demonstrating our serious commitment to the protection of customer data.

Contractual safeguards	TP and NAVEX Global have entered into supplementary contractual assurances as an amendment to the data processing addendum.
	The SCCs themselves contain a number of contractual commitments by TP and NAVEX Global, aimed at serving as safeguards for EU personal data. We have also entered into a robust general data processing addendum.
	Implement other transparency, audit and monitoring obligations on Teleperformance regarding the level of government access to data.
Organizational safeguards	Teleperformance maintains written processes and procedures provide for review of and limit the scope of EU personal data disclosed by Teleperformance in response to requests from public authorities.

	Teleperformance maintains internal record of requests made by public authorities concerning EU personal data.
	Teleperformance takes steps to limit the volume of disclosed data, where possible.
	Teleperformance takes data minimization measures such as redacting unnecessary identifiable personal data or personal data that may be of increased interest to intelligence agencies before complying with a request to disclosure EU personal data.
	Teleperformance has developed a broad set of controls that allow the company to evidence, keep track and be fully compliant with both, internal applicable legislation and the GDPR (in applicable cases).
Technical safeguards	Encrypt personal data in transit.
	Encrypt personal data at rest.
	Enhance access controls.
	Enhance data minimization (e.g., store the least amount of data necessary).
	Limit timespan for using personal data “in the clear” (i.e., in identifiable form).
	Pseudonymize/obfuscate stored personal data by which the personal data is masked with a particular ID, code, character, or other modified content to safeguard the original personal data or any sensitive data and prevent unauthorized access or use of such data.
	Other security measures implemented by internal Security Tools (EDR, AV, SIEM, FW, etc) that can add another security layer for the protection of the data or de devices related processing it.

Conclusion

Having regard to the level of risk of the data transfer (**very limited risk**), TP and NAVEX Global consider that the measures identified above are **sufficient and effective** in light of the circumstances of the transfers, in conjunction with the supplementary measures and safeguards provided by the SCCs, to allow the data importer to comply with its obligations under the SCCs and provide an appropriate level of protection for the transfer.

Hotline and Incident Management US Hosted Sub-Processing Activity: Contact Centre Services with Transparent BPO

NAVEX GLOBAL SUB-PROCESSING ACTIVITY

US HOSTED HOTLINE SERVICES– CONTACT CENTRE SERVICES

I. SCOPE

This TRA applies to NAVEX Global's US Hosted Hotline customers. This TRA applies specifically to the contact centre services taking place as part of the Hotline services.

As part of NAVEX Global's Hotline service component, customers are provided with telephony to receive reports submitted via telephone. NAVEX Global utilizes two sub-processors for additional contact centre support services, for the intake and dispatch of the phone reports. This TRA applies to Transparent BPO ("TBPO") only. The contact centre agents are located in Belize.

II. ASSESSING THE ADEQUACY OF EU/UK DATA TRANSFERS – CONTACT CENTRE SERVICES

In assessing the adequacy of transfers of personal data from the EU/UK to NAVEX Global's sub-processor pursuant to the contact centre services provided by said sub-processor, NAVEX Global have taken the following steps:

1. **STEP 1:** Identified the relevant data transfers and the legal mechanism that NAVEX Global and sub-processor is relying on for such transfers (e.g., SCCs).

2. **STEP 2:** Conducted due diligence and collected information about the scope of the transfers, the exposure of the sub-processor to local law that may require disclosure of EU personal data about individuals, and any other relevant information.

3. **STEP 3:** Completed the "Transfer Risk Assessment" in **Section IV** to assess whether the SCCs is effective in light of all circumstances of the transfer.

4. **STEP 4:** Included additional "Supplementary Measures" as set forth in **Section IV (D)**.

5. **STEP 5:** Documented the assessment for accountability purposes. NAVEX Global encourages NAVEX Global's customers to do the same.

6. **STEP 6:** NAVEX Global and its sub-processor is responsible for the periodic review of the assessment, which should take place at least annually, to ensure that the transfer of the EU personal data continues to be afforded an adequate level of protection.

III. TRANSFER RISK ASSESSMENT

Name Of Data Importer: TBPO **(**NAVEX Global's sub-processor)
Completed By: NAVEX Global's Privacy Team and TBPO Legal and Compliance
Date: 25 September 2021

A. Type of Data Importer

Name of data importer: TBPO. The Processor to Processor SCCs between NAVEX Global and TBPO is part of a master services agreement between NAVEX Global and TBPO.

Does TBPO provide the following services to NAVEX Global:

	Data Importer	
Telecommunications	☐ Yes	☒ No
Other electronic communications (such as an Internet Service Provider or a provider of email, text message, VoIP, remote desktop or VPN services)?	☐ Yes	☒ No
Remote computing services	☐ Yes	☒ No
Other communications service where there may be access to wire or electronic communications	☒ Yes	☐ No

TBPO acknowledges that its services could be viewed as meeting the definition of a communication service.

B. Details of Data Transfers

Data transfer mechanism

Appropriate Processor to Processor SCCs between TBPO and NAVEX Global.

Scope of personal data covered by the data transfer mechanism in place

The SCCs cover transfers of EU personal data from the EU/UK to Belize, including the following categories of data subjects:

- Employees of customer Data Controller
- Clients, business partners and vendors of customer Data Controller (who are natural persons)
- Employees or contact persons of customer Data Controllers' third-party suppliers, business partners and vendors
- Customer Data Controller's users authorized to use the relevant Service(s)

C. Transfer Risk Assessment

The table below aids identification and evaluation of risk factors in relation to the specific data transfer. The assessment of each risk factor is recorded in appropriate detail.

#	Factor	Response
Scope of the transfers		
1.	What is the type of transfer?	Intake and submission of phone reports as part of the contact centre services. Personal data is not copied over or stored with TBPO. The processing by the individual contact centre agent is limited to the intake and submission of

#	Factor	Response
		the given phone report in real time. TBPO personnel input the information into NAVEX Global's proprietary and secure systems to be dispatched into the customer's case management system hosted in the U.S.
2.	Is the transfer necessary?	Yes. The transfer is necessary to provide the services to NAVEX Global, on behalf of NAVEX Global's customers. To intake reports from individuals on important ethics and compliance matters, TBPO has to be able the provide the best available contact centre and language support resources available, to allow these reporters effective whistle blowing capabilities.
3.	Is the transfer proportionate?	Yes. The transfer is strictly limited to taking and submitting the report in real time.
4.	Is the transfer occasional/non-routine or frequent/routine?	The transfers are frequent/routine. NAVEX Global routes customer contacts to TBPO on a regular basis as a part of its normal contact handling processes. On a per data subject basis, the transfers are infrequent/non-routine.
5.	Will the transferred personal data be processed for a relatively long or short period of time?	Personal data transferred is processed for a relatively short period of time, in order to intake the report call and submit it.
6.	Is the transferred data encrypted and/ or pseudonymized?	Yes, Encryption in transit and at rest upon NAVEX Global's secure data centres. Any session TBPO accesses to NAVEX Global systems are over an encrypted (HTTPS) session.
Specific circumstances of the transfer		
7.	What are the purposes for which the data are transferred and processed?	The data are transferred and processed in order for identify the customer contact information for hotline reporting purposes.
8.	What are the types of entities involved in the processing?	TBPO is a data sub-processor and a private company. NAVEX Global is a data processor and private company. NAVEX Global's customers are the data controllers and may consist of both private and public companies.
9.	In which sector does the transfer occur?	NAVEX Global provides risk and compliance

#	Factor	Response
		management SaaS based software. ***This factor is especially important as the purposes of NAVEX Global's services is to enable organizations support their risk, ethics, and compliance programs. ***
10.	What are the categories of personal data transferred?	• name, job title, job position, location, employer, relationship with the organization, e-mail address, telephone number; • for whistle-blower hotline reports, in addition to the foregoing, the following may also be captured: o facts reported by a reporter about a suspected violation, including how and where the suspected violation occurred and how the reporter learned about the suspected violation; o identity, function and contact details of individuals allegedly involved in the suspected violation; and o identity, function and contact details of individuals who could provide information relating to the suspected violation. Given the nature of hotline and incident management services, reporters may submit sensitive categories of data in a report. NAVEX Global recommends its customers have strict policies around the management of such report data in their use of the services, in accordance with the laws subject to them.
11.	What is the format of the personal data to be transferred?	The personal data appears on the contact centre agent's computer screen for review and processing. All access to NAVEX Global's systems by TBPO agents is done over encrypted (HTTPS TLS1.2+) sessions.
12.	What is the storage location of the data transferred?	The United States via NAVEX Global's secure servers. There is no storage of data by TBPO.
13.	What are the sub-sub-processing activities?	Not applicable.
Importer's exposure to government surveillance and practical application of problematic legislation		
14.	Is the data importer's sector or business directly subject to such laws in its jurisdiction	No. In TBPO's reasonable opinion, TBPO's

#	Factor	Response
	that permit government access to personal data, or require the assistance of data importer to disclose personal data to public authorities, for surveillance and intelligence gathering purposes?	business is currently not directly subject to such laws. As a practical matter based on the nature of TBPO's services, the types of personal data processed, and the absence of any prior requests received in the past, TBPO believes it is extremely unlikely to receive requests from Belize government agencies to obtain NAVEX Global customer data for national security purposes or to participate in the types of bulk surveillance programs scrutinized by the CJEU in its recent ruling on data transfer mechanisms.
	a. Specifically, what is data importer's analysis regarding any applicable surveillance laws in Belize under the SCCs and EDPB Guidance?	TBPO researched Belize law and as of now, there are no specific regulations related to data privacy/protection (https://unctad.org/page/data-protection-and-privacy-legislation-worldwide). However, there is currently a bill proposed in the Belize Parliament (Data Protection Bill, 2021). It has not passed yet, but TBPO will carefully monitor any developments related to the Data Protection Bill. 1) Data exporters may decide to proceed with the transfer without supplementary measures, if they consider there to be no reason to believe that any relevant surveillance laws will be applied, in practice, to the transferred data and/or TBPO. a. In our reasonable opinion upon internal and outside counsel review, TBPO does not find third country surveillance laws to practically apply to these transfers. b. TBPO is generally out of scope and that these laws are overall not going to apply to the services we provide, as the intent is for surveillance of certain telecom and internet service providers for targeted information. This typically involves surveillance of real time emails, texts, and chat conversations. The foregoing is not what NAVEX Global nor TBPO provides and in order to obtain this sought for information, authorities would pursue those providers directly as it would be impractical to make a request through TBPO. 2) Data exporters may also take into consideration documented practical experience of data importer with relevant prior instances of requests for access received from public authorities. **To this point, TBPO has never received such public authority access requests scrutinized under the Schrems II decision.**

#	Factor	Response
		a. The EDPB Guidance implies that the lack of requests received in the past plus no prohibition on providing information about such requests, could be sufficient to conclude such laws do not apply in practice. Note there is no prohibition on TBPO to provide information about these requests. **While NAVEX Global and TBPO take the approach that problematic legislation does not apply in practice, we still have elected to provide for supplementary measures with regard to these transfers. Please see Section IV (D).**
15.	Within the last three (3) years, has the data importer received requests/demands from public authorities in its jurisdiction to disclose EU personal data?	Based on available information, TBPO's entities in Belize have not received requests/demands for disclosure of, or access to, EU personal data.
	a. Approximately how many requests/demands from public authorities has the data importer received in that time period concerning EU personal data?	None, to the best of TBPO's knowledge.
	b. Approximately how many of these requests/demands are pursuant to criminal law procedure in the destination country? *[Regular court proceedings are not the issue under Schrems II, but intelligence programs are scrutinized.]*	None, to the best of TBPO's knowledge.
	c. Approximately how many of these requests/demands are pursuant to national security or intelligence agencies in the destination country?	None, to the best of TBPO's knowledge. The data importer can represent that it has not received requests/demands from intelligence agencies.
	d. Has the data importer been able to contest/minimize such disclosure of EU personal data, where appropriate?	Not applicable
	e. What types of EU personal data has the data importer been required to disclose to public authorities in its jurisdiction?	Not applicable
16.	How likely is it that the data importer will receive bulk data surveillance requests to disclose EU personal data to public authorities in its jurisdiction in the future (e.g., based on factors such as the type of services provided and sector in which the data importer operates, its size, number of customers and reputation)?	Unlikely. To the best of TBPO's knowledge, there have been no, and TBPO does not expect there to be, requests or demands by public authorities for disclosure of, or access to, EU personal data.
17.	Does the data importer maintain annual reports or statistics regarding requests/demands received from law enforcement or intelligence agencies (e.g., number/type of requests/demands, requesting authority, etc.)?	Not applicable. TBPO has not received requests from public authorities for EU personal data under the SCCs or otherwise. As a result, if TBPO receives such requests in the future, TBPO will provide such statistics and update the

#	Factor	Response
		TBPO TRA process and Public Authority Disclosure Policy accordingly.
18.	Does the data importer maintain a written procedure(s) for: 1. Responding to or challenging requests/ demands of law enforcement or intelligence agencies that apply to EU personal data? 14. Informing customers of requests/demands from law enforcement or intelligence agencies where permitted by applicable law?	Yes. TBPO has adopted a Government Data Request Policy and is in the process of creating supporting Standard Operating Procedures with details to address responding/challenging requests and notification. This will be completed on or before October 31, 2021.
19.	Are the data importer's commitments enabling data subjects to exercise their rights as provided in the SCCs thwarted by the laws and/or practices in the U.S. and any other third countries involved, or can these rights be effectively applied in practice?	These rights can be effectively applied in practice. TBPO has never encountered a situation where it felt it could not enable data subject rights, including judicial redress. TBPO does not believe the laws subject to TBPO prevents TBPO from enabling, supporting, and fulfilling data subject rights under the SCCs.
Onward transfers and exposure to government surveillance		
20.	Does the data importer share EU personal data further with third-party data recipients in [the U.S./other jurisdiction]?	No, not applicable.

Conclusion/Risk of transfers

Very limited-risk data transfer

In particular, TBPO and NAVEX Global identified the following factors (based on the assessment documented above and any additional information), that are likely to indicate a very limited-risk transfer:

No further processing outside of phone intake and submission takes place.

The data importer has never received requests/demands from intelligence services for disclosure of EU personal data.

The data importer has received limited requests/demands from public authorities for disclosure of EU personal data (such as for disclosure of employee data), but the requests related to regular criminal law procedure and did not go beyond what is necessary and proportionate to meet the purpose of the request.

The data importer has a process in place for handling and contesting public authority access requests, if received.

Based on the nature of its services and data processing activities, the data importer does not expect to be the target of requests/demands pursuant to national security or intelligence agencies for disclosure of EU personal data.

Such data transfers are not directly nor practically in scope of requests/demands from national security or intelligence agencies for disclosure of EU personal data.

D. Supplementary Measures

Notwithstanding the Conclusion set forth in the above TRA, TBPO has also adopted the following supplemental measures. TBPO believes that by implementing such supplemental measures, TBPO is following best practices and are demonstrating TBPO's serious commitment to the protection of customer data.

Contractual safeguards	TBPO and NAVEX Global have entered into supplementary contractual assurances as an amendment to the data processing addendum.
	The SCCs themselves contain a number of contractual commitments by TBPO and NAVEX Global, aimed at serving as safeguards for EU personal data. TBPO and NAVEX Global have also entered into a robust general data processing addendum.
	Implement other transparency, audit and monitoring obligations on TBPO regarding the level of government access to data.
Organizational safeguards	TBPO maintains written processes and procedures provide for review of and limit the scope of EU personal data disclosed by TBPO in response to requests from public authorities.
	TBPO maintains internal record of requests made by public authorities concerning EU personal data.
	TBPO takes steps to limit the volume of disclosed data, where possible.
	TBPO takes data minimization measures such as redacting unnecessary identifiable personal data or personal data that may be of increased interest to intelligence agencies before complying with a request to disclosure EU personal data.
Technical safeguards	Encrypt personal data in transit.
	Encrypt personal data at rest via NAVEX Global's secure data centres.
	Appropriate access controls.
	Customer data controllers can implement data minimization (e.g., store the least amount of data necessary).
	Timespan for any access to personal data "in the clear" is limited to the specific function.

	Store personal data in the US via NAVEX Global's secure data centres and no access is provided to TBPO after report dispatch.

Conclusion

Having regard to the level of risk of the data transfer (**very limited risk**), TBPO and NAVEX Global consider that the measures identified above are **sufficient and effective** in light of the circumstances of the transfers, in conjunction with the supplementary measures and safeguards provided by the SCCs, to allow the data importer to comply with its obligations under the SCCs and provide an appropriate level of protection for the transfer.

PolicyTech: US Hosted

NAVEX GLOBAL

US HOSTED POLICYTECH - EU/UK DATA TRANSFER RISK ASSESSMENTS

I. INTRODUCTION

NAVEX Global must conduct Transfer Risk Assessments ("TRA" or "TRAs") for transfers of personal data from the European Economic Area ("EEA")[8] or the United Kingdom ("UK") (collectively "EU personal data") to third countries that are not deemed to provide an adequate level of data protection.

II. SCOPE

These TRAs apply to NAVEX Global's US Hosted PolicyTech customers.

This TRA process applies to personal data transferred to NAVEX Global pursuant to the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council. This TRA is specifically designed to address Clause 14 of the foregoing set of Standard Contractual Clauses. Personal data from the UK is also in scope and shall be assessed pursuant to the European Commission's decision (C(2010)593) of 5 February 2010 on Standard Contractual Clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection. We collectively refer to the sets of Standard Contractual Clauses as the "SCCs." NAVEX Global agrees and acknowledges the UK will be issuing its own set of standard contractual clauses and related Schrems II guidance. We will update this TRA on an ongoing basis as needed.

This TRA process takes into account the European Data Protection Board's Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data adopted on 18 June 2021 (the "EDPB Guidance").

This TRA is not intended for transfers (i) within the EEA, (ii) between the EEA and the UK, or (iii) from the EEA or UK to a country recognized by the European Commission or UK law as adequate at this time (i.e., Andorra,

[8] The European Economic Area consists of the Member States of the EU (Austria, Belgium, Bulgaria, Croatia, Cyprus, Czechia, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain and Sweden), plus Iceland, Liechtenstein and Norway.

Argentina, Canada (commercial organizations subject to PIPEDA), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, UK, and Uruguay).

The TRA is completed by the NAVEX Global Privacy Team, which consists of the Data Privacy Officer & Senior Counsel, Deputy Data Privacy Officer & Senior Counsel, and Privacy Counsel.

III. ASSESSING THE ADEQUACY OF EU/UK DATA TRANSFERS – TO NAVEX GLOBAL IN THE U.S.

In assessing the adequacy of transfers of personal data from the EU/UK to NAVEX Global in the U.S. we have taken the following steps:

1. **STEP 1:** Identified the relevant data transfers and the legal mechanism that NAVEX Global is relying on for such transfers (e.g., SCCs).

2. **STEP 2:** Conducted due diligence and collected information about the scope of the transfers, the exposure of NAVEX Global to local law that may require disclosure of EU personal data about individuals, and any other relevant information.

3. **STEP 3:** Completed the "Transfer Risk Assessment" in **Section IV** to assess whether the SCCs is effective in light of all circumstances of the transfer.

4. **STEP 4:** Included additional "Supplementary Measures" as set forth in **Section IV (D)**.

5. **STEP 5:** Documented the assessment for accountability purposes. We encourage our customers to do the same.

6. **STEP 6:** NAVEX Global is responsible for the periodic review of the assessment, which should take place at least annually, to ensure that the transfer of the EU personal data continues to be afforded an adequate level of protection.

IV. TRANSFER RISK ASSESSMENT

Name Of Data Importer: NAVEX Global

Scope of TRA: Transfers to NAVEX Global in the United States as part of the PolicyTech Services provided to US Hosted Customers

****Our customers elect the hosting and storage location. As a result, NAVEX Global has many customers subject to the GDPR on our US hosted and storage configuration, as chosen by the customer.****

Completed By: NAVEX Global's Privacy Team

Date: 25 September 2021

A. Type of Data Importer

Name of data importer: NAVEX Global. The SCCs between customer and NAVEX Global is part of a master services agreement between customer and NAVEX Global, Inc., a Delaware corporation, having its principal place of business at 5500 Meadows Road, Suite 500, Lake Oswego, Oregon 97035.

Upon reviewing the broad definitions set forth within U.S. surveillance laws under scrutiny pursuant to the CJEU ruling in the Schrems II case, NAVEX Global identifies itself as follows:

NAVEX Global does not consider itself a "telecommunications carrier" as defined in 47 U.S.C. 152.

NAVEX Global acknowledges that certain of its services could be viewed by U.S. government authorities as an "electronic communication service" as defined in 18 U.S.C. 2510.

NAVEX Global acknowledges that certain of its services could be viewed by U.S. government authorities as a "remote computing service" as defined in 18 U.S.C. 2711.

NAVEX Global acknowledges that certain of its services could be viewed by U.S. government authorities as other communication services where there may be access to wire or electronic communications.

B. Details of Data Transfers

Data transfer mechanism Appropriate Controller to Processor SCCs between customer and NAVEX Global.
Scope of personal data covered by the data transfer mechanism in place The SCCs cover transfers of EU personal data from the EEA/UK to the U.S., including the following categories of data subjects: • Employees of data exporter • Clients, business partners and vendors of data exporter (who are natural persons) • Employees or contact persons of data exporters' third-party suppliers, business partners and vendors • Data exporter's users authorized by data exporter to use the relevant Service(s)

C. Transfer Risk Assessment

The table below aids identification and evaluation of risk factors in relation to the specific data transfer. The assessment of each risk factor is recorded in appropriate detail.

#	Factor	Response
Scope of the transfers		
1.	What is the type of transfer?	

#	Factor	Response
		EU personal data is stored and hosted within the U.S. NAVEX Global's hosting providers either cannot or do not access EU personal data. Select NAVEX Global personnel have access to provision the services in accordance with our agreements, subject to the principle of least privilege and our access control policies and processed.
2.	Is the transfer necessary?	Yes. NAVEX Global's customers elect their storage and hosting location. Many customers choose and prefer the U.S. For NAVEX Global to securely store the data in the U.S. as elected by the customer, they must transfer the data to this location via the services. For NAVEX Global to be able to provide the services, our personnel must be able to access the systems to provide support, administrative functions, technical work, and IT/Hosting support. Without the above, we wouldn't be able to provide the services or meet our service level commitments.
3.	Is the transfer proportionate?	Yes. The data is securely stored and NAVEX Global processes data to maintain the services and in accordance with its customer's instructions.
4.	Is the transfer occasional/non-routine or frequent/routine?	The transfer is frequent/routine. This is necessary in order to host, store, and provide the services from the U.S. as requested.
5.	Will the transferred personal data be processed for a relatively long or short period of time?	During the life of the agreement, the customer decides how long to maintain the personal data in the system in accordance with their own policies and processes. NAVEX Global maintains the personal data within the services, as elected by the customer, for the duration of the agreement.
6.	Is the transferred data encrypted and/ or pseudonymized?	Yes. NAVEX Global employs encryption at rest using either full-disk encryption or within the database using TDE. Data at rest will be encrypted using

#	Factor	Response
		AES 256 or better, data in flight will be accomplished using TLS 1.2 or higher on public untrusted networks. Upon reviewing pseudonymization in the context of this transfer, it is inapplicable to the services we need to support.
Specific circumstances of the transfer		
7.	What are the purposes for which the data are transferred and processed?	To securely store the data in the U.S. as requested by our customers. To provide the best support, maintenance, and services as committed to in our agreements with our customers.
8.	What are the types of entities involved in the processing?	NAVEX Global is a data processor and a private company. Our customers are the data controllers and may consist of both private and public companies.
9.	In which sector does the transfer occur?	NAVEX Global provides risk and compliance management SaaS based software. ***This factor is especially important as the purposes of our services is to enable organizations support their risk, ethics, and compliance programs. ***
10.	What are the categories of personal data transferred?	• Name (first and last), email address, job site, job title, department, supervisor, log-in credentials, completion status, time and date of policies. ****No sensitive data, as defined under the GDPR, is transferred as part of the PolicyTech services.****
11.	What is the format of the personal data to be transferred?	NAVEX Global employs encryption at rest using either full-disk encryption or within the database using TDE. Data at rest will be encrypted using AES 256 or better, data in flight will be accomplished using TLS 1.2 or higher on public untrusted networks. When access is provided to NAVEX Global personnel in the U.S. for the purposes described in this TRA, customer data must be accessible in the clear to provide the requisite support or service function.

#	Factor	Response
12.	What is the storage location of the data transferred?	The United States.
13.	What are the sub-processing activities?	Please see details here: https://www.navexglobal.com/en-us/service-hosting-providers. All requirements are flown down to each sub-processor.
Importer's exposure to government surveillance and practical application of Section 702 FISA		
14.	Is the data importer's sector or business directly subject to such laws in its jurisdiction that permit government access to personal data, or require the assistance of data importer to disclose personal data to public authorities, for surveillance and intelligence gathering purposes?	No. In our reasonable opinion upon internal and outside counsel review, we do not find NAVEX Global to be directly subject to such laws. As a practical matter based on the nature of NAVEX Global's services, the types of personal data processed, and the absence of any prior requests received in the past, NAVEX Global believes it is extremely unlikely to receive requests from U.S. government agencies to obtain customer data for national security purposes or to participate in the types of U.S. bulk surveillance programs scrutinized by the CJEU in its recent ruling on data transfer mechanisms.
	a. Specifically, what is data importer's analysis regarding Section 702 FISA under the SCCs and EDPB Guidance?	1) Data exporters may decide to proceed with the transfer without supplementary measures, if they consider there to be no reason to believe that the relevant and problematic legislation (those in the U.S. in this instance) will be applied, in practice, to the transferred data and/or NAVEX Global. a. In our reasonable opinion upon internal and outside counsel review, we do not find U.S. surveillance laws, including Section 702 FISA, to practically apply to these transfers. b. It is important to note that given the broad definitions of these laws, the vast majority of organizations are going to have to acknowledge their potential application. However, this does not mean they directly apply or practically apply in practice. c. We believe NAVEX Global is generally out of scope and that these laws are overall not going to apply to the services we provide, as the intent is for surveillance of certain telecom and internet service providers for targeted information. This typically involves to surveillance of real time emails, texts, and chat conversations. The

#	Factor	Response
		foregoing is not what NAVEX Global provides and in order to obtain this sought for information, authorities would pursue those providers directly as it would be impractical to make a request through NAVEX Global. 2) Data exporters may also take into consideration documented practical experience of data importer with relevant prior instances of requests for access received from public authorities in the U.S. a. ***To this point, NAVEX Global has never received a Section 702 FISA request or an EO 12.333 request or order. Please see our Public Authority Disclosure Request Policy for more details.** * b. The EDPB Guidance implies that the lack of requests received in the past plus no prohibition on providing information about such requests, could be sufficient to conclude Section 702 FISA does not apply in practice. Note there is no prohibition on NAVEX Global to provide information about these requests. 3) If you conclude Section 702 FISA does not apply in practice to the particular transfer, it is possible to proceed with the transfer without any supplementary measures. **a. While NAVEX Global takes the approach that Section 702 FISA does not apply in practice, we still have elected to provide for supplementary measures with regard to these transfers. Please see Section IV (D).**
15.	Within the last three (3) years, has the data importer received requests/demands from public authorities in its jurisdiction to disclose EU personal data pursuant to the SCCs?	No, not to the best of our knowledge.
	a. Approximately how many requests/demands from public authorities has the data importer received in that time period concerning EU personal data pursuant to the SCCs?	None, to the best of our knowledge.
	b. Approximately how many of these requests/demands are pursuant to criminal law procedure in the destination country? *[Regular court proceedings are not the issue under Schrems II, but intelligence programs are scrutinized.]*	While NAVEX Global has not received a Section 702 FISA request, an EO 12.333 request or order, or a public authority request specifically targeting EU personal data under the SCCs, we have received a limited number of formal requests or demands from U.S. government authorities concerning customer data. These requests have been made in the context of criminal and civil actions in the form of a

#	Factor	Response
		subpoena issued to NAVEX Global as a third party, by a state or federal court. In each instance, we've notified the customer straight away and they have directed us to comply with the subpoena. We've only fulfilled such requests with full customer clearance and direction on how to handle.
	c. Approximately how many of these requests/demands are pursuant to national security or intelligence agencies in the destination country?	None, to the best of our knowledge. The data importer can represent that it has not received requests/demands from intelligence agencies. NAVEX Global offers signed contracts, warranting it has not received such requests, via either a data processing addendum or amendment to data processing addendum.
	d. Has the data importer been able to contest/minimize such disclosure of EU personal data, where appropriate?	Not applicable
	e. What types of EU personal data has the data importer been required to disclose to public authorities in its jurisdiction?	Not applicable
16.	How likely is it that the data importer will receive bulk data surveillance requests to disclose EU personal data to public authorities in its jurisdiction in the future (e.g., based on factors such as the type of services provided and sector in which the data importer operates, its size, number of customers and reputation)?	Unlikely. As a practical matter based on the nature of NAVEX Global's services, the types of personal data processed, and the absence of any prior requests received in the past, NAVEX Global believes it is extremely unlikely to receive requests from U.S. government agencies to obtain customer data for national security purposes or to participate in the types of U.S. bulk surveillance programs scrutinized by the CJEU in its recent ruling on data transfer mechanisms. We have no reason to believe we may receive such requests in the future.
17.	Does the data importer maintain annual reports or statistics regarding requests/demands received from law enforcement or intelligence agencies (e.g., number/type of requests/demands, requesting authority, etc.)?	Not applicable. NAVEX Global has not received a Section 702 FISA request, an EO 12.333 request or order, or a public authority request specifically targeting EU personal data under the SCCs. As a result, if we get such requests in the future, we will provide such statistics and update our TRA process and Public Authority Disclosure Policy accordingly.
18.	Does the data importer maintain a written procedure(s) for: 1. Responding to or challenging requests/demands of law enforcement or intelligence agencies that apply to EU personal data? 15. Informing customers of	Yes, please see our Public Authority Disclosure Request Policy.

#	Factor	Response
	requests/demands from law enforcement or intelligence agencies where permitted by applicable law?	
19.	Are the data importer's commitments enabling data subjects to exercise their rights as provided in the SCCs thwarted by the laws and/or practices in the U.S. or can these rights be effectively applied in practice?	NAVEX Global has never encountered a situation where it felt it could not enable data subject rights, including judicial redress. We do not believe the laws subject to us prevent us from enabling, supporting, and fulfilling data subject rights under the SCCs.
Onward transfers and exposure to government surveillance		
20.	Does the data importer share EU personal data further with sub-processors whose processing takes place in third countries?	No.

Conclusion/Risk of transfers

Likely limited-risk data transfer

In particular, NAVEX Global identified the following factors (based on the assessment documented above and any additional information), that are likely to indicate a limited-risk transfer:

The data importer has never received requests/demands from intelligence services for disclosure of EU personal data.

The data importer has received limited requests/demands from public authorities for disclosure of EU personal data (such as for disclosure of employee data), but the requests related to regular criminal law procedure and did not go beyond what is necessary and proportionate to meet the purpose of the request.

The data importer has a process in place for handling and contesting public authority access requests, if received.

Based on the nature of its services and data processing activities, the data importer does not expect to be the target of requests/demands pursuant to national security or intelligence agencies for disclosure of EU personal data.

Such data transfers are not directly nor practically in scope of requests/demands from national security or intelligence agencies for disclosure of EU personal data.

D. Supplementary Measures

Notwithstanding the Conclusion set forth in the above TRA, NAVEX Global has also adopted the following supplemental measures. We believe that by implementing such supplemental measures, we are following best practices and are demonstrating our serious commitment to the protection of customer data.

Contractual safeguards	The SCCs themselves contain a number of contractual commitments by NAVEX Global and its customer, aimed at serving as safeguards for EU personal data.
	Supplementary contractual assurances are offered via our standard data processing addendum or an amendment to the data processing addendum. Please reach out to privacy@navexglobal.com in order to get this in place.
	NAVEX Global agrees to audit and monitor its obligations, and to support its customers auditing and monitoring obligations, regarding the level of government access to data.
	NAVEX Global provides a data processing agreement to support GDPR compliance, which includes the SCCs. As the data processor/importer, we process personal data strictly in accordance with your instructions and to provide the services. Our customers are the owners of the personal data within our service applications. NAVEX Global offers a Data Security Addendum, providing for contractual commitments to its information security program.
Organizational safeguards	NAVEX Global maintains written processes and procedures which provide for review of and limit the scope of EU personal data disclosed by NAVEX Global in response to requests from public authorities. Please see our Public Authority Disclosure Request Policy.
	NAVEX Global maintains internal records of requests made by public authorities concerning EU personal data.
	NAVEX Global takes steps to limit the volume of disclosed data, where possible.
	NAVEX Global would take data minimization measures such as redacting unnecessary identifiable personal data or personal data that may be of increased interest to intelligence agencies before complying with a request to disclosure EU personal data.
	NAVEX Global has developed a Standard Contractual Clauses Assurance Guide, which details our commitment to compliance with the SCCs. NAVEX Global remains a participant and has certified its compliance with the EU-U.S. Privacy Shield Framework and the Swiss- U.S. Privacy Shield Framework. NAVEX Global, Inc. is committed to subjecting all personal information received from the European Economic Area, United Kingdom, and Switzerland,

	respectively, in reliance on each Privacy Shield Framework, to the Frameworks' applicable Principles. To learn more about the Privacy Shield program, and to view our certification, please visit https://www.privacyshield.gov. NAVEX Global provides an independent recourse mechanism to EU individuals, currently TrustArc.
Technical safeguards	Encrypt personal data in transit.
	Encrypt personal data at rest.
	Appropriate access controls.
	Customers can implement data minimization (e.g., store the least amount of data necessary).
	Timespan for any access to personal data "in the clear" is limited to the specific function.
	NAVEX Global equips its services with self-servicing functionality, allowing you to manage the personal data on your own through the use of the services. NAVEX Global engages a recognized, independent third party to conduct a Statement on Standards for Attestation Engagements No. 16, Service Organization Control 2, Type 2 ("SSAE 18 SOC 2 Type 2") audit (or its equivalent or successor) of its information security program and its administrative, technical, and physical safeguards for all facilities used to deliver the Services, which specifically includes privacy controls. NAVEX Global maintains an annual Standardized Information Gathering Questionnaire ("SIG"), which details our robust security program with supporting documentation.

Conclusion

Having regard to the level of risk of the data transfer (**limited risk**), NAVEX Global considers that the measures identified above are **sufficient and effective** in light of the circumstances of the transfers, in conjunction with the supplementary measures and safeguards provided by the SCCs, to allow the data importer to comply with its obligations under the SCCs and provide an appropriate level of protection for the transfer.

NAVEX GLOBAL

US HOSTED NAVEXENGAGE - EU/UK DATA TRANSFER RISK ASSESSMENTS

I. INTRODUCTION

NAVEX Global must conduct Transfer Risk Assessments ("TRA" or "TRAs") for transfers of personal data from the European Economic Area ("EEA")[9] or the United Kingdom ("UK") (collectively "EU personal data") to third countries that are not deemed to provide an adequate level of data protection.

II. SCOPE

These TRAs apply to NAVEX Global's US Hosted NAVEXEngage customers.

This TRA process applies to personal data transferred to NAVEX Global pursuant to the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council. This TRA is specifically designed to address Clause 14 of the foregoing set of Standard Contractual Clauses. Personal data from the UK is also in scope and shall be assessed pursuant to the European Commission's decision (C(2010)593) of 5 February 2010 on Standard Contractual Clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection. We collectively refer to the sets of Standard Contractual Clauses as the "SCCs." NAVEX Global agrees and acknowledges the UK will be issuing its own set of standard contractual clauses and related Schrems II guidance. We will update this TRA on an ongoing basis as needed.

This TRA process takes into account the European Data Protection Board's Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data adopted on 18 June 2021 (the "EDPB Guidance").

This TRA is not intended for transfers (i) within the EEA, (ii) between the EEA and the UK, or (iii) from the EEA or UK to a country recognized by the European Commission or UK law as adequate at this time (i.e., Andorra, Argentina, Canada (commercial organizations subject to PIPEDA), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, UK, and Uruguay).

The TRA is completed by the NAVEX Global Privacy Team, which consists of the Data Privacy Officer & Senior Counsel, Deputy Data Privacy Officer & Senior Counsel, and Privacy Counsel.

III. ASSESSING THE ADEQUACY OF EU/UK DATA TRANSFERS – TO NAVEX GLOBAL IN THE U.S.

In assessing the adequacy of transfers of personal data from the EU/UK to NAVEX Global in the U.S. we have taken the following steps:

1. **STEP 1:** Identified the relevant data transfers and the legal mechanism that NAVEX Global is relying on for such transfers (e.g., SCCs).

[9] The European Economic Area consists of the Member States of the EU (Austria, Belgium, Bulgaria, Croatia, Cyprus, Czechia, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain and Sweden), plus Iceland, Liechtenstein and Norway.

2. **STEP 2:** Conducted due diligence and collected information about the scope of the transfers, the exposure of NAVEX Global to local law that may require disclosure of EU personal data about individuals, and any other relevant information.

3. **STEP 3:** Completed the "Transfer Risk Assessment" in **Section IV** to assess whether the SCCs is effective in light of all circumstances of the transfer.

4. **STEP 4:** Included additional "Supplementary Measures" as set forth in **Section IV (D)**.

5. **STEP 5:** Documented the assessment for accountability purposes. We encourage our customers to do the same.

6. **STEP 6:** NAVEX Global is responsible for the periodic review of the assessment, which should take place at least annually, to ensure that the transfer of the EU personal data continues to be afforded an adequate level of protection.

IV. TRANSFER RISK ASSESSMENT

Name Of Data Importer: NAVEX Global

Scope of TRA: Transfers to NAVEX Global in the United States as part of the NAVEXEnage Services provided to US Hosted Customers

****Our customers elect the hosting and storage location. As a result, NAVEX Global has many customers subject to the GDPR on our US hosted and storage configuration, as chosen by the customer.****

Completed By: NAVEX Global's Privacy Team

Date: 25 September 2021

A. Type of Data Importer

Name of data importer: NAVEX Global. The SCCs between customer and NAVEX Global is part of a master services agreement between customer and NAVEX Global, Inc., a Delaware corporation, having its principal place of business at 5500 Meadows Road, Suite 500, Lake Oswego, Oregon 97035.

Upon reviewing the broad definitions set forth within U.S. surveillance laws under scrutiny pursuant to the CJEU ruling in the Schrems II case, NAVEX Global identifies itself as follows:

NAVEX Global does not consider itself a "telecommunications carrier" as defined in 47 U.S.C. 152.

NAVEX Global acknowledges that certain of its services could be viewed by U.S. government authorities as an "electronic communication service" as defined in 18 U.S.C. 2510.

NAVEX Global acknowledges that certain of its services could be viewed by U.S. government authorities as a "remote computing service" as defined in 18 U.S.C. 2711.

NAVEX Global acknowledges that certain of its services could be viewed by U.S. government authorities as other communication services where there may be access to wire or electronic communications.

B. Details of Data Transfers

Data transfer mechanism Appropriate Controller to Processor SCCs between customer and NAVEX Global.
Scope of personal data covered by the data transfer mechanism in place The SCCs cover transfers of EU personal data from the EEA/UK to the U.S., including the following categories of data subjects: • Employees of data exporter • Clients, business partners and vendors of data exporter (who are natural persons) • Employees or contact persons of data exporters' third-party suppliers, business partners and vendors • Data exporter's users authorized by data exporter to use the relevant Service(s)

C. Transfer Risk Assessment

The table below aids identification and evaluation of risk factors in relation to the specific data transfer. The assessment of each risk factor is recorded in appropriate detail.

#	Factor	Response
Scope of the transfers		
1.	What is the type of transfer?	EU personal data is stored and hosted within the U.S. NAVEX Global's hosting providers either cannot or do not access EU personal data. Select NAVEX Global personnel have access to provision the services in accordance with our agreements, subject to the principle of least privilege and our access control policies and processed.
2.	Is the transfer necessary?	Yes. NAVEX Global's customers elect their storage and hosting location. Many customers choose and prefer the U.S. For NAVEX Global to securely store the data in the U.S. as elected by the customer, they must transfer the data to this location via the services.

#	Factor	Response
		For NAVEX Global to be able to provide the services, our personnel must be able to access the systems to provide support, administrative functions, technical work, and IT/Hosting support. Without the above, we wouldn't be able to provide the services or meet our service level commitments.
3.	Is the transfer proportionate?	Yes. The data is securely stored and NAVEX Global processes data to maintain the services and in accordance with its customer's instructions.
4.	Is the transfer occasional/non-routine or frequent/routine?	The transfer is frequent/routine. This is necessary in order to host, store, and provide the services from the U.S. as requested.
5.	Will the transferred personal data be processed for a relatively long or short period of time?	During the life of the agreement, the customer decides how long to maintain the personal data in the system in accordance with their own policies and processes. NAVEX Global maintains the personal data within the services, as elected by the customer, for the duration of the agreement.
6.	Is the transferred data encrypted and/ or pseudonymized?	Yes. NAVEX Global employs encryption at rest using either full-disk encryption or within the database using TDE. Data at rest will be encrypted using AES 256 or better, data in flight will be accomplished using TLS 1.2 or higher on public untrusted networks. Upon reviewing pseudonymization in the context of this transfer, it is inapplicable to the services we need to support.
Specific circumstances of the transfer		
7.	What are the purposes for which the data are transferred and processed?	To securely store the data in the U.S. as requested by our customers. To provide the best support, maintenance, and services as committed to in our agreements with our customers.

#	Factor	Response
8.	What are the types of entities involved in the processing?	NAVEX Global is a data processor and a private company. Our customers are the data controllers and may consist of both private and public companies.
9.	In which sector does the transfer occur?	NAVEX Global provides risk and compliance management SaaS based software. ***This factor is especially important as the purposes of our services is to enable organizations support their risk, ethics, and compliance programs. ***
10.	What are the categories of personal data transferred?	• Name (first and last), email address, job site, job title, department, supervisor, log-in credentials, completion status, time and date of training media. ****No sensitive data, as defined under the GDPR, is transferred as part of the NAVEXEngage services.****
11.	What is the format of the personal data to be transferred?	NAVEX Global employs encryption at rest using either full-disk encryption or within the database using TDE. Data at rest will be encrypted using AES 256 or better, data in flight will be accomplished using TLS 1.2 or higher on public untrusted networks. When access is provided to NAVEX Global personnel in the U.S. for the purposes described in this TRA, customer data must be accessible in the clear to provide the requisite support or service function.
12.	What is the storage location of the data transferred?	The United States.
13.	What are the sub-processing activities?	Please see details here: https://www.navexglobal.com/en-us/service-hosting-providers. All requirements are flown down to each sub-processor.
Importer's exposure to government surveillance and practical application of Section 702 FISA		
14.	Is the data importer's sector or business directly subject to such laws in its jurisdiction that permit government access to personal data, or require the assistance of data importer to disclose personal data to public authorities, for surveillance and intelligence gathering purposes?	No. In our reasonable opinion upon internal and outside counsel review, we do not find NAVEX Global to be directly subject to such laws. As a practical matter based on the nature of NAVEX Global's services, the types of personal data processed, and the absence of any prior requests received in the past, NAVEX Global

#	Factor	Response
		believes it is extremely unlikely to receive requests from U.S. government agencies to obtain customer data for national security purposes or to participate in the types of U.S. bulk surveillance programs scrutinized by the CJEU in its recent ruling on data transfer mechanisms.
	a. Specifically, what is data importer's analysis regarding Section 702 FISA under the SCCs and EDPB Guidance?	1) Data exporters may decide to proceed with the transfer without supplementary measures, if they consider there to be no reason to believe that the relevant and problematic legislation (those in the U.S. in this instance) will be applied, in practice, to the transferred data and/or NAVEX Global. a. In our reasonable opinion upon internal and outside counsel review, we do not find U.S. surveillance laws, including Section 702 FISA, to practically apply to these transfers. b. It is important to note that given the broad definitions of these laws, the vast majority of organizations are going to have to acknowledge their potential application. However, this does not mean they directly apply or practically apply in practice. c. We believe NAVEX Global is generally out of scope and that these laws are overall not going to apply to the services we provide, as the intent is for surveillance of certain telecom and internet service providers for targeted information. This typically involves to surveillance of real time emails, texts, and chat conversations. The foregoing is not what NAVEX Global provides and in order to obtain this sought for information, authorities would pursue those providers directly as it would be impractical to make a request through NAVEX Global. 2) Data exporters may also take into consideration documented practical experience of data importer with relevant prior instances of requests for access received from public authorities in the U.S. a. ***To this point, NAVEX Global has never received a Section 702 FISA request or an EO 12.333 request or order. Please see our Public Authority Disclosure Request Policy for more details.** * b. The EDPB Guidance implies that

#	Factor	Response
		the lack of requests received in the past plus no prohibition on providing information about such requests, could be sufficient to conclude Section 702 FISA does not apply in practice. Note there is no prohibition on NAVEX Global to provide information about these requests. 3) If you conclude Section 702 FISA does not apply in practice to the particular transfer, it is possible to proceed with the transfer without any supplementary measures. **a. While NAVEX Global takes the approach that Section 702 FISA does not apply in practice, we still have elected to provide for supplementary measures with regard to these transfers. Please see Section IV (D).**
15.	Within the last three (3) years, has the data importer received requests/demands from public authorities in its jurisdiction to disclose EU personal data pursuant to the SCCs?	No, not to the best of our knowledge.
	a. Approximately how many requests/demands from public authorities has the data importer received in that time period concerning EU personal data pursuant to the SCCs?	None, to the best of our knowledge.
	b. Approximately how many of these requests/demands are pursuant to criminal law procedure in the destination country? *[Regular court proceedings are not the issue under Schrems II, but intelligence programs are scrutinized.]*	While NAVEX Global has not received a Section 702 FISA request, an EO 12.333 request or order, or a public authority request specifically targeting EU personal data under the SCCs, we have received a limited number of formal requests or demands from U.S. government authorities concerning customer data. These requests have been made in the context of criminal and civil actions in the form of a subpoena issued to NAVEX Global as a third party, by a state or federal court. In each instance, we've notified the customer straight away and they have directed us to comply with the subpoena. We've only fulfilled such requests with full customer clearance and direction on how to handle.
	c. Approximately how many of these requests/demands are pursuant to national security or intelligence agencies in the destination country?	None, to the best of our knowledge. The data importer can represent that it has not received requests/demands from intelligence agencies. NAVEX Global offers signed contracts, warranting it has not received such requests, via either a data processing addendum or amendment to data processing addendum.
	d. Has the data importer been able to contest/minimize such disclosure of EU	Not applicable

#	Factor	Response
	personal data, where appropriate?	
	e. What types of EU personal data has the data importer been required to disclose to public authorities in its jurisdiction?	Not applicable
16.	How likely is it that the data importer will receive bulk data surveillance requests to disclose EU personal data to public authorities in its jurisdiction in the future (e.g., based on factors such as the type of services provided and sector in which the data importer operates, its size, number of customers and reputation)?	Unlikely. As a practical matter based on the nature of NAVEX Global's services, the types of personal data processed, and the absence of any prior requests received in the past, NAVEX Global believes it is extremely unlikely to receive requests from U.S. government agencies to obtain customer data for national security purposes or to participate in the types of U.S. bulk surveillance programs scrutinized by the CJEU in its recent ruling on data transfer mechanisms. We have no reason to believe we may receive such requests in the future.
17.	Does the data importer maintain annual reports or statistics regarding requests/demands received from law enforcement or intelligence agencies (e.g., number/type of requests/demands, requesting authority, etc.)?	Not applicable. NAVEX Global has not received a Section 702 FISA request, an EO 12.333 request or order, or a public authority request specifically targeting EU personal data under the SCCs. As a result, if we get such requests in the future, we will provide such statistics and update our TRA process and Public Authority Disclosure Policy accordingly.
18.	Does the data importer maintain a written procedure(s) for: 1. Responding to or challenging requests/demands of law enforcement or intelligence agencies that apply to EU personal data? 16. Informing customers of requests/demands from law enforcement or intelligence agencies where permitted by applicable law?	Yes, please see our Public Authority Disclosure Request Policy.
19.	Are the data importer's commitments enabling data subjects to exercise their rights as provided in the SCCs thwarted by the laws and/or practices in the U.S. or can these rights be effectively applied in practice?	NAVEX Global has never encountered a situation where it felt it could not enable data subject rights, including judicial redress. We do not believe the laws subject to us prevent us from enabling, supporting, and fulfilling data subject rights under the SCCs.
Onward transfers and exposure to government surveillance		
20.	Does the data importer share EU personal data further with sub-processors whose processing takes place in third countries?	No.

#	Factor	Response
	Conclusion/Risk of transfers	
	Likely limited-risk data transfer	
	In particular, NAVEX Global identified the following factors (based on the assessment documented above and any additional information), that are likely to indicate a limited-risk transfer:	
	The data importer has never received requests/demands from intelligence services for disclosure of EU personal data.	
	The data importer has received limited requests/demands from public authorities for disclosure of EU personal data (such as for disclosure of employee data), but the requests related to regular criminal law procedure and did not go beyond what is necessary and proportionate to meet the purpose of the request.	
	The data importer has a process in place for handling and contesting public authority access requests, if received.	
	Based on the nature of its services and data processing activities, the data importer does not expect to be the target of requests/demands pursuant to national security or intelligence agencies for disclosure of EU personal data.	
	Such data transfers are not directly nor practically in scope of requests/demands from national security or intelligence agencies for disclosure of EU personal data.	

D. Supplementary Measures

Notwithstanding the Conclusion set forth in the above TRA, NAVEX Global has also adopted the following supplemental measures. We believe that by implementing such supplemental measures, we are following best practices and are demonstrating our serious commitment to the protection of customer data.

Contractual safeguards	The SCCs themselves contain a number of contractual commitments by NAVEX Global and its customer, aimed at serving as safeguards for EU personal data.
	Supplementary contractual assurances are offered via our standard data processing addendum or an amendment to the data processing addendum. Please reach out to privacy@navexglobal.com in order to get this in place.
	NAVEX Global agrees to audit and monitor its obligations, and to support its customers auditing and monitoring obligations,

	regarding the level of government access to data.
	NAVEX Global provides a data processing agreement to support GDPR compliance, which includes the SCCs. As the data processor/importer, we process personal data strictly in accordance with your instructions and to provide the services. Our customers are the owners of the personal data within our service applications. NAVEX Global offers a Data Security Addendum, providing for contractual commitments to its information security program.
Organizational safeguards	NAVEX Global maintains written processes and procedures which provide for review of and limit the scope of EU personal data disclosed by NAVEX Global in response to requests from public authorities. Please see our Public Authority Disclosure Request Policy.
	NAVEX Global maintains internal records of requests made by public authorities concerning EU personal data.
	NAVEX Global takes steps to limit the volume of disclosed data, where possible.
	NAVEX Global would take data minimization measures such as redacting unnecessary identifiable personal data or personal data that may be of increased interest to intelligence agencies before complying with a request to disclosure EU personal data.
	NAVEX Global has developed a Standard Contractual Clauses Assurance Guide, which details our commitment to compliance with the SCCs. NAVEX Global remains a participant and has certified its compliance with the EU-U.S. Privacy Shield Framework and the Swiss- U.S. Privacy Shield Framework. NAVEX Global, Inc. is committed to subjecting all personal information received from the European Economic Area, United Kingdom, and Switzerland, respectively, in reliance on each Privacy Shield Framework, to the Frameworks' applicable Principles. To learn more about the Privacy Shield program, and to view our certification, please visit https://www.privacyshield.gov. NAVEX Global provides an independent recourse mechanism to EU individuals, currently TrustArc.
Technical safeguards	Encrypt personal data in transit.

	Encrypt personal data at rest.
	Appropriate access controls.
	Customers can implement data minimization (e.g., store the least amount of data necessary).
	Timespan for any access to personal data "in the clear" is limited to the specific function.
	NAVEX Global equips its services with self-servicing functionality, allowing you to manage the personal data on your own through the use of the services. NAVEX Global engages a recognized, independent third party to conduct a Statement on Standards for Attestation Engagements No. 16, Service Organization Control 2, Type 2 ("SSAE 18 SOC 2 Type 2") audit (or its equivalent or successor) of its information security program and its administrative, technical, and physical safeguards for all facilities used to deliver the Services, which specifically includes privacy controls. NAVEX Global maintains an annual Standardized Information Gathering Questionnaire ("SIG"), which details our robust security program with supporting documentation.

Conclusion

Having regard to the level of risk of the data transfer (**limited risk**), NAVEX Global considers that the measures identified above are **sufficient and effective** in light of the circumstances of the transfers, in conjunction with the supplementary measures and safeguards provided by the SCCs, to allow the data importer to comply with its obligations under the SCCs and provide an appropriate level of protection for the transfer.

RiskRate: US Hosted

NAVEX GLOBAL

US HOSTED RISKRATE - EU/UK DATA TRANSFER RISK ASSESSMENTS

I. INTRODUCTION

NAVEX Global must conduct Transfer Risk Assessments ("TRA" or "TRAs") for transfers of personal data from the European Economic Area ("EEA")[10] or the United Kingdom ("UK") (collectively "EU personal data") to third countries that are not deemed to provide an adequate level of data protection.

II. SCOPE

These TRAs apply to NAVEX Global's US Hosted RiskRate customers.

This TRA process applies to personal data transferred to NAVEX Global pursuant to the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council. This TRA is specifically designed to address Clause 14 of the foregoing set of Standard Contractual Clauses. Personal data from the UK is also in scope and shall be assessed pursuant to the European Commission's decision (C(2010)593) of 5 February 2010 on Standard Contractual Clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection. We collectively refer to the sets of Standard Contractual Clauses as the "SCCs." NAVEX Global agrees and acknowledges the UK will be issuing its own set of standard contractual clauses and related Schrems II guidance. We will update this TRA on an ongoing basis as needed.

This TRA process takes into account the European Data Protection Board's Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data adopted on 18 June 2021 (the "EDPB Guidance").

NAVEX Global has separate TRAs for its non-affiliate sub-processing activities, where NAVEX Global utilizes such sub-processors for the processing of personal data who receive customer EU personal data in third countries that have not been deemed adequate by the European Commission. These are available as part of our compliance documentation and on request.

This TRA is not intended for transfers (i) within the EEA, (ii) between the EEA and the UK, or (iii) from the EEA or UK to a country recognized by the European Commission or UK law as adequate at this time (i.e., Andorra, Argentina, Canada (commercial organizations subject to PIPEDA), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, UK, and Uruguay).

The TRA is completed by the NAVEX Global Privacy Team, which consists of the Data Privacy Officer & Senior Counsel, Deputy Data Privacy Officer & Senior Counsel, and Privacy Counsel.

III. ASSESSING THE ADEQUACY OF EU/UK DATA TRANSFERS – TO NAVEX GLOBAL IN THE U.S.

In assessing the adequacy of transfers of personal data from the EU/UK to NAVEX Global in the U.S. we have taken the following steps:

1. **STEP 1:** Identified the relevant data transfers and the legal mechanism that NAVEX Global is relying on for such transfers (e.g., SCCs).

[10] The European Economic Area consists of the Member States of the EU (Austria, Belgium, Bulgaria, Croatia, Cyprus, Czechia, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain and Sweden), plus Iceland, Liechtenstein and Norway.

2. **STEP 2:** Conducted due diligence and collected information about the scope of the transfers, the exposure of NAVEX Global to local law that may require disclosure of EU personal data about individuals, and any other relevant information.

3. **STEP 3:** Completed the "Transfer Risk Assessment" in **Section IV** to assess whether the SCCs is effective in light of all circumstances of the transfer.

4. **STEP 4:** Included additional "Supplementary Measures" as set forth in **Section IV (D)**.

5. **STEP 5:** Documented the assessment for accountability purposes. We encourage our customers to do the same.

6. **STEP 6:** NAVEX Global is responsible for the periodic review of the assessment, which should take place at least annually, to ensure that the transfer of the EU personal data continues to be afforded an adequate level of protection.

IV. TRANSFER RISK ASSESSMENT

Name Of Data Importer: NAVEX Global

Scope of TRA: Transfers to NAVEX Global in the United States as part of the RiskRate Services provided to US Hosted Customers

****Our customers elect the hosting and storage location. As a result, NAVEX Global has many customers subject to the GDPR on our US hosted and storage configuration, as chosen by the customer.****

Completed By: NAVEX Global's Privacy Team

Date: 25 September 2021

Type of Data Importer

Name of data importer: NAVEX Global. The SCCs between customer and NAVEX Global is part of a master services agreement between customer and NAVEX Global, Inc., a Delaware corporation, having its principal place of business at 5500 Meadows Road, Suite 500, Lake Oswego, Oregon 97035.

Upon reviewing the broad definitions set forth within U.S. surveillance laws under scrutiny pursuant to the CJEU ruling in the Schrems II case, NAVEX Global identifies itself as follows:

NAVEX Global does not consider itself a "telecommunications carrier" as defined in 47 U.S.C. 152.

NAVEX Global acknowledges that certain of its services could be viewed by U.S. government authorities as an "electronic communication service" as defined in 18 U.S.C. 2510.

NAVEX Global acknowledges that certain of its services could be viewed by U.S. government authorities as a "remote computing service" as defined in 18 U.S.C. 2711.

NAVEX Global acknowledges that certain of its services could be viewed by U.S. government authorities as other communication services where there may be access to wire or electronic communications.

A. Details of Data Transfers

Data transfer mechanism Appropriate Controller to Processor SCCs between customer and NAVEX Global.
Scope of personal data covered by the data transfer mechanism in place The SCCs cover transfers of EU personal data from the EEA/UK to the U.S., including the following categories of data subjects: • Employees of data exporter • Clients, business partners and vendors of data exporter (who are natural persons) • Employees or contact persons of data exporters' third-party suppliers, business partners and vendors • Data exporter's users authorized by data exporter to use the relevant Service(s)

B. Transfer Risk Assessment

The table below aids identification and evaluation of risk factors in relation to the specific data transfer. The assessment of each risk factor is recorded in appropriate detail.

#	Factor	Response
Scope of the transfers		
1.	What is the type of transfer?	EU personal data is stored and hosted within the U.S. NAVEX Global's hosting providers either cannot or do not access EU personal data. Select NAVEX Global personnel have access to provision the services in accordance with our agreements, subject to the principle of least privilege and our access control policies and processed.
2.	Is the transfer necessary?	Yes. NAVEX Global's customers elect their storage and hosting location. Many customers choose and prefer the U.S.

#	Factor	Response
		For NAVEX Global to securely store the data in the U.S. as elected by the customer, they must transfer the data to this location via the services. For NAVEX Global to be able to provide the services, our personnel must be able to access the systems to provide support, administrative functions, technical work and product management, and IT/Hosting support. Without the above, we wouldn't be able to provide the services or meet our service level commitments.
3.	Is the transfer proportionate?	Yes. Customer elects the U.S. for storage and requests the RiskRate due diligence. The data is securely stored and NAVEX Global processes data to maintain the services and in accordance with its customer's instructions.
4.	Is the transfer occasional/non-routine or frequent/routine?	The transfer is frequent/routine. This is necessary in order to host, store, and provide the services from the U.S. as requested.
5.	Will the transferred personal data be processed for a relatively long or short period of time?	During the life of the agreement, the customer decides how long to maintain the personal data in the system in accordance with their own policies and processes. NAVEX Global maintains the personal data within the services, as elected by the customer, for the duration of the agreement.
6.	Is the transferred data encrypted and/ or pseudonymized?	Yes. NAVEX Global employs encryption at rest using either full-disk encryption or within the database using TDE. Data at rest will be encrypted using AES 256 or better, data in flight will be accomplished using TLS 1.2 or higher on public untrusted networks. Upon reviewing pseudonymization in the context of this transfer, it is inapplicable to the services we need to support.
Specific circumstances of the transfer		
7.	What are the purposes for which the data are transferred and processed?	To securely store the data in the U.S. as requested by our customers.

#	Factor	Response
		To provide the best support, maintenance, and services as committed to in our agreements with our customers.
8.	What are the types of entities involved in the processing?	NAVEX Global is a data processor and a private company. Our customers are the data controllers and may consist of both private and public companies.
9.	In which sector does the transfer occur?	NAVEX Global provides risk and compliance management SaaS based software. ***This factor is especially important as the purposes of our services is to enable organizations support their risk, ethics, and compliance programs. *** Many of our customers are required by law to conduct appropriate due diligence on third parties. As such, our customers request certain data to be screened and provided back to them, to allow them to conduct this due diligence.
10.	What are the categories of personal data transferred?	Generally, the RiskRate services implicate the following categories of personal data, as requested by the customer to perform the screening: • name, job title, job position, location, employer, relationship with the organization, e-mail address, telephone number, address, date of birth, manager, director, officer and affiliated or organization information Depending on the scope of the customer request, additional categories of personal data may be sent back to the customer for processing as part of their due diligence: • nationality, shareholder ID #, percentage of ownership, picture, ID # (passport, social security number, or national ID) ***No sensitive data, as defined under the GDPR, is transferred from customer to NAVEX Global as part of the RiskRate services. ***
11.	What is the format of the personal data to be transferred?	NAVEX Global employs encryption at rest using either full-disk encryption or within the database using TDE. Data at rest will be encrypted using AES 256 or better, data in flight will be

#	Factor	Response
		accomplished using TLS 1.2 or higher on public untrusted networks. When access is provided to NAVEX Global personnel in the U.S. for the purposes described in this TRA, customer data must be accessible in the clear to provide the requisite support or service function.
12.	What is the storage location of the data transferred?	The United States.
13.	What are the sub-processing activities?	Please see details here: https://www.navexglobal.com/en-us/service-hosting-providers. These are temporary and limited sub-processing activities. All requirements are flown down to each sub-processor.
Importer's exposure to government surveillance and practical application of Section 702 FISA		
14.	Is the data importer's sector or business directly subject to such laws in its jurisdiction that permit government access to personal data, or require the assistance of data importer to disclose personal data to public authorities, for surveillance and intelligence gathering purposes?	No. In our reasonable opinion upon internal and outside counsel review, we do not find NAVEX Global to be directly subject to such laws. As a practical matter based on the nature of NAVEX Global's services, the types of personal data processed, and the absence of any prior requests received in the past, NAVEX Global believes it is extremely unlikely to receive requests from U.S. government agencies to obtain customer data for national security purposes or to participate in the types of U.S. bulk surveillance programs scrutinized by the CJEU in its recent ruling on data transfer mechanisms. ***NAVEX Global has never received <u>ANY</u> requests for data pertaining to its RiskRate services. ***
	a. Specifically, what is data importer's analysis regarding Section 702 FISA under the SCCs and EDPB Guidance?	1) Data exporters may decide to proceed with the transfer without supplementary measures, if they consider there to be no reason to believe that the relevant and problematic legislation (those in the U.S. in this instance) will be applied, in practice, to the transferred data and/or NAVEX Global. a. In our reasonable opinion upon internal and outside counsel review, we do not find U.S. surveillance laws, including Section 702 FISA, to practically apply to these transfers. b. It is important to note that given the broad definitions of these laws, the vast majority of organizations are

#	Factor	Response
		going to have to acknowledge their potential application. However, this does not mean they directly apply or practically apply in practice. c. We believe NAVEX Global is generally out of scope and that these laws are overall not going to apply to the services we provide, as the intent is for surveillance of certain telecom and internet service providers for targeted information. This typically involves to surveillance of real time emails, texts, and chat conversations. The foregoing is not what NAVEX Global provides and in order to obtain this sought for information, authorities would pursue those providers directly as it would be impractical to make a request through NAVEX Global. 2) Data exporters may also take into consideration documented practical experience of data importer with relevant prior instances of requests for access received from public authorities in the U.S. a. ***To this point, NAVEX Global has never received a Section 702 FISA request or an EO 12.333 request or order. Please see our Public Authority Disclosure Request Policy for more details.** * **b. **NAVEX Global has never received <u>ANY</u> requests for data pertaining to its RiskRate services. *** c. The EDPB Guidance implies that the lack of requests received in the past plus no prohibition on providing information about such requests, could be sufficient to conclude Section 702 FISA does not apply in practice. Note there is no prohibition on NAVEX Global to provide information about these requests. 3) If you conclude Section 702 FISA does not apply in practice to the particular transfer, it is possible to proceed with the transfer without any supplementary measures. **a. While NAVEX Global takes the approach that Section 702 FISA does not apply in practice, we still have elected to provide for supplementary measures with regard to these transfers. Please see Section IV (D).**
15.	Within the last three (3) years, has the data	

#	Factor	Response
	importer received requests/demands from public authorities in its jurisdiction to disclose EU personal data pursuant to the SCCs?	No.
	a. Approximately how many requests/demands from public authorities has the data importer received in that time period concerning EU personal data pursuant to the SCCs?	None.
	b. Approximately how many of these requests/demands are pursuant to criminal law procedure in the destination country? *[Regular court proceedings are not the issue under Schrems II, but intelligence programs are scrutinized.]*	****NAVEX Global has never received <u>ANY</u> requests for data pertaining to its RiskRate services. *** While NAVEX Global has not received requests from public authorities for EU personal data under the SCCs or otherwise, we have received a limited number of formal requests or demands from U.S. government **authorities concerning customer data pertaining to its hotline and incident management services**. These requests have been made in the context of criminal and civil actions in the form of a subpoena issued to NAVEX Global as a third party, by a state or federal court. In each instance, we've notified the customer straight away and they have directed us to comply with the subpoena. We've only fulfilled such requests with full customer clearance and direction on how to handle.
	c. Approximately how many of these requests/demands are pursuant to national security or intelligence agencies in the destination country?	None, to the best of our knowledge. The data importer can represent that it has not received requests/demands from intelligence agencies. NAVEX Global offers signed contracts, warranting it has not received such requests, via either a data processing addendum or amendment to data processing addendum.
	d. Has the data importer been able to contest/minimize such disclosure of EU personal data, where appropriate?	Not applicable
	e. What types of EU personal data has the data importer been required to disclose to public authorities in its jurisdiction?	Not applicable
16.	How likely is it that the data importer will receive bulk data surveillance requests to disclose EU personal data to public authorities in its jurisdiction in the future (<u>e.g.</u>, based on factors such as the type of services provided and sector in which the data importer operates, its size, number of customers and reputation)?	Unlikely. As a practical matter based on the nature of NAVEX Global's services, the types of personal data processed, and the absence of any prior requests received in the past, NAVEX Global believes it is extremely unlikely to receive requests from U.S. government agencies to obtain customer data for national security purposes or to participate in the types of U.S. bulk surveillance programs scrutinized by the CJEU in its recent ruling on data transfer

#	Factor	Response
		mechanisms. We have no reason to believe we may receive such requests in the future.
17.	Does the data importer maintain annual reports or statistics regarding requests/demands received from law enforcement or intelligence agencies (e.g., number/type of requests/demands, requesting authority, etc.)?	Not applicable. NAVEX Global has not received requests from public authorities for EU personal data under the SCCs or otherwise. As a result, if we get such requests in the future, we will provide such statistics and update our TRA process and Public Authority Disclosure Policy accordingly.
18.	Does the data importer maintain a written procedure(s) for: 1. Responding to or challenging requests/demands of law enforcement or intelligence agencies that apply to EU personal data? 17. Informing customers of requests/demands from law enforcement or intelligence agencies where permitted by applicable law?	Yes, please see our Public Authority Disclosure Request Policy.
19.	Are the data importer's commitments enabling data subjects to exercise their rights as provided in the SCCs thwarted by the laws and/or practices in the U.S. or can these rights be effectively applied in practice?	NAVEX Global has never encountered a situation where it felt it could not enable data subject rights, including judicial redress. We do not believe the laws subject to us prevent us from enabling, supporting, and fulfilling data subject rights under the SCCs.
Onward transfers and exposure to government surveillance		
20.	Does the data importer share EU personal data further with sub-processors whose processing takes place in third countries?	Yes.
21.	What measures does the third-party data recipient take to ensure the protection of EU personal data transferred to it?	NAVEX Global enters into written agreements with sub-processors that include safeguards for EU personal data in accordance with the GDPR requirements.
22.	What assurances has the data importer received from third-party data recipients with respect to requests/demands for EU personal data from [U.S./other jurisdiction] public authorities?	NAVEX Global has updated, or is in the process of updating, all written agreements with sub-processors to include additional measures for the protection of EU personal data, where required.
Conclusion/Risk of transfers		

#	Factor	Response
	Likely limited-risk data transfer **In particular, NAVEX Global identified the following factors (based on the assessment documented above and any additional information), that are likely to indicate a limited-risk transfer:** The data importer has never received requests/demands from intelligence services for disclosure of EU personal data. The data importer has received limited requests/demands from public authorities for disclosure of EU personal data (such as for disclosure of employee data), but the requests related to regular criminal law procedure and did not go beyond what is necessary and proportionate to meet the purpose of the request. The data importer has a process in place for handling and contesting public authority access requests, if received. Based on the nature of its services and data processing activities, the data importer does not expect to be the target of requests/demands pursuant to national security or intelligence agencies for disclosure of EU personal data. Such data transfers are not directly nor practically in scope of requests/demands from national security or intelligence agencies for disclosure of EU personal data.	

C. Supplementary Measures

Notwithstanding the Conclusion set forth in the above TRA, NAVEX Global has also adopted the following supplemental measures. We believe that by implementing such supplemental measures, we are following best practices and are demonstrating our serious commitment to the protection of customer data.

Contractual safeguards	The SCCs themselves contain a number of contractual commitments by NAVEX Global and its customer, aimed at serving as safeguards for EU personal data.
	Supplementary contractual assurances are offered via our standard data processing addendum or an amendment to the data processing addendum. Please reach out to privacy@navexglobal.com in order to get this in place.
	NAVEX Global agrees to audit and monitor its obligations, and to support its customers auditing and monitoring obligations, regarding the level of government access to data.
	NAVEX Global provides a data processing agreement to support GDPR compliance, which includes the SCCs. As the data

	processor/importer, we process personal data strictly in accordance with your instructions and to provide the services. Our customers are the owners of the personal data within our service applications. NAVEX Global offers a Data Security Addendum, providing for contractual commitments to its information security program.
Organizational safeguards	NAVEX Global maintains written processes and procedures which provide for review of and limit the scope of EU personal data disclosed by NAVEX Global in response to requests from public authorities. Please see our Public Authority Disclosure Request Policy.
	NAVEX Global maintains internal records of requests made by public authorities concerning EU personal data.
	NAVEX Global takes steps to limit the volume of disclosed data, where possible.
	NAVEX Global would take data minimization measures such as redacting unnecessary identifiable personal data or personal data that may be of increased interest to intelligence agencies before complying with a request to disclosure EU personal data.
	NAVEX Global has developed a Standard Contractual Clauses Assurance Guide, which details our commitment to compliance with the SCCs. NAVEX Global remains a participant and has certified its compliance with the EU-U.S. Privacy Shield Framework and the Swiss- U.S. Privacy Shield Framework. NAVEX Global, Inc. is committed to subjecting all personal information received from the European Economic Area, United Kingdom, and Switzerland, respectively, in reliance on each Privacy Shield Framework, to the Frameworks' applicable Principles. To learn more about the Privacy Shield program, and to view our certification, please visit https://www.privacyshield.gov. NAVEX Global provides an independent recourse mechanism to EU individuals, currently TrustArc.
Technical safeguards	Encrypt personal data in transit.
	Encrypt personal data at rest.
	Appropriate access controls.

	Customers can implement data minimization (e.g., store the least amount of data necessary).
	Timespan for any access to personal data "in the clear" is limited to the specific function.
	NAVEX Global equips its services with self-servicing functionality, allowing you to manage the personal data on your own through the use of the services. NAVEX Global engages a recognized, independent third party to conduct a Statement on Standards for Attestation Engagements No. 16, Service Organization Control 2, Type 2 ("SSAE 18 SOC 2 Type 2") audit (or its equivalent or successor) of its information security program and its administrative, technical, and physical safeguards for all facilities used to deliver the Services, which specifically includes privacy controls. NAVEX Global maintains an annual Standardized Information Gathering Questionnaire ("SIG"), which details our robust security program with supporting documentation.

Conclusion

Having regard to the level of risk of the data transfer (**limited risk**), NAVEX Global considers that the measures identified above are **sufficient and effective** in light of the circumstances of the transfers, in conjunction with the supplementary measures and safeguards provided by the SCCs, to allow the data importer to comply with its obligations under the SCCs and provide an appropriate level of protection for the transfer.

RiskRate US Hosted Sub-processing Activity: Due Diligence with Regulatory DataCorp

NAVEX GLOBAL SUB-PROCESSING ACTIVITY

US HOSTED RISKRATE- REGULATORY DATACORP TRANSFER RISK ASSESSMENT

I. SCOPE

This TRA applies to NAVEX Global's US Hosted RiskRate customers. This TRA applies specifically to the services provided by NAVEX Global's sub-processor, Regulatory DataCorp, Inc. (RDC).

As part of NAVEX Global's RiskRate services, our customers provide certain personal data in NAVEX Global's systems to be received and processed by RDC as part of the due diligence screenings. For NAVEX Global's US Hosted customers, RDC utilizes servers located in the US for the applicable hosting.

RDC personnel access to customer personal data is limited to only a select group of RDC staff members through RDC's VPN and to limited and vetted sub-processors (applicable for Analyst Review only). The relevant RDC staff members are located in the United States, the United Kingdom, and Singapore. The sub-processors are located in the US, Romania, India and Bangladesh.

II. ASSESSING THE ADEQUACY OF EU/UK DATA TRANSFERS – RDC SERVICES

In assessing the adequacy of transfers of personal data from the EU/UK to NAVEX Global's sub-processor pursuant to the RDC services, we have taken the following steps:

1. **STEP 1:** Identified the relevant data transfers and the legal mechanism that NAVEX Global and sub-processor is relying on for such transfers (e.g., SCCs).

2. **STEP 2:** Conducted due diligence and collected information about the scope of the transfers, the exposure of the sub-processor to local law that may require disclosure of EU personal data about individuals, and any other relevant information.

3. **STEP 3:** Completed the "Transfer Risk Assessment" in **Section IV** to assess whether the SCCs is effective in light of all circumstances of the transfer.

4. **STEP 4:** Included additional "Supplementary Measures" as set forth in **Section IV (D)**.

5. **STEP 5:** Documented the assessment for accountability purposes. We encourage our customers to do the same.

6. **STEP 6:** NAVEX Global and its sub-processor is responsible for the periodic review of the assessment, which should take place at least annually, to ensure that the transfer of the EU personal data continues to be afforded an adequate level of protection.

III. TRANSFER RISK ASSESSMENT

Name Of Data Importer: Regulatory DataCorp, Inc. (NAVEX Global's sub-processor)

Completed By: NAVEX Global's Privacy Team and Moody's Privacy Team on behalf of RDC

Date: 25 September 2021

A. Type of Data Importer

Name of data importer: Regulatory DataCorp, Inc. ("RDC"). The Processor to Processor SCCs between NAVEX Global and RDC is part of a master services agreement between NAVEX Global and RDC.

B. Does RDC provide the following services to NAVEX Global:

	Data Importer	
Telecommunications	☐ Yes	☒ No
Other electronic communications (such as an Internet Service Provider or a provider of email, text message, VoIP, remote desktop or VPN services)?	☐ Yes	☒ No
Remote computing services	☐ Yes	☒ No
Other communications service where there may be access to wire or electronic communications	☐ Yes	☒ No

If no, please specify the nature of the services provided to NAVEX Global by the data importer: Provision of regulatory screening services GRID, Client Review, AI Review and Analyst Review.

C. Details of Data Transfers

Data transfer mechanism

Appropriate Processor to Processor SCCs between RDC and NAVEX Global.

Scope of personal data covered by the data transfer mechanism in place

The SCCs cover transfers of EU personal data from the EEA/UK to third countries, including the following categories of data subjects:

- Clients, business partners and vendors of customer Data Controller (who are natural persons)
- Employees or contact persons of customer Data Controller's third-party suppliers, business partners and vendors

D. Transfer Risk Assessment

The table below aids identification and evaluation of risk factors in relation to the specific data transfer. The assessment of each risk factor is recorded in appropriate detail.

#	Factor	Response
Scope of the transfers		
1.	What is the type of transfer?	NAVEX Global's customer submits certain personal data within the RiskRate system which is provided to RDC to utilize in its due diligence screening and ongoing monitoring. The processing by RDC is limited to the performance of the given screen or monitoring request.
2.	Is the transfer necessary?	Yes. The transfer is critical and necessary to provide the services to NAVEX Global, on behalf of NAVEX Global's customers.
3.	Is the transfer proportionate?	Yes. The transfer is strictly limited to screening and monitoring the information provided from the customer.
4.	Is the transfer occasional/non-routine or frequent/routine?	The transfer is non-routine to RDC on a per request basis.
5.	Will the transferred personal data be processed for a relatively long or short period of time?	Personal data is processed for a relatively short period of time to support the applicable due diligence requests.
6.	Is the transferred data encrypted and/or pseudonymized?	Yes, both Encryption in transit and at rest and Obfuscation as follows: In storage, the data is contained within unique database tables assigned to each "firm" in the application, Firm identifiers are not client name but rather a unique two alphabetical character + a 6-character alphanumeric string. Clients can set this firm ID. In processing there is anonymization between RDC and its sub processors, i.e. it is never disclosed to offshore analysts which client submitted inquiry data for which they review, this is done through role based views within he analytics application.

#	Factor	Response
Specific circumstances of the transfer		
7.	What are the purposes for which the data are transferred and processed?	To provide the best publicly available information regarding adverse media alerts, sanctions watchlists, and politically exposed alerts.
8.	What are the types of entities involved in the processing?	RDC is a data sub-processor and a private company. NAVEX Global's customers are the data controllers and may consist of both private and public companies.
9.	In which sector does the transfer occur?	NAVEX Global provides risk and compliance management SaaS based software. ***This factor is especially important as the purposes of our services is to enable organizations support their risk, ethics, and compliance programs.*** * Many of our customers are required by law to conduct appropriate due diligence on third parties. As such, our customers request certain data to be screened and provided back to them, to allow them to conduct this due diligence.
10.	What are the categories of personal data transferred?	Customers can send the following categories of data to RDC via NAVEX Global's RiskRate services: • name, address information (street, city, state/province, country, zip code), date of birth ***No sensitive data, as defined under the GDPR, is sent to RDC from customer to the RiskRate services. ***
11.	What is the format of the personal data to be transferred?	When personal data is provided to RDC for the purposes described in this TRA, such personal data must be accessible in the clear to fulfill the request.
12.	What is the storage location of the data transferred?	The United States for NAVEX Global's US hosted customers.
13.	What are the sub-sub-processing activities?	AWS: cloud hosting. United States for customers who elect US hosting WNS: Remote customer support (all Review products); Analyst review (applicable for Analyst Review only).

#	Factor	Response
		SEBPO: Analyst review (applicable for Analyst Review only).
Importer's exposure to government surveillance and practical application of Section 702 FISA		
14.	Is the data importer's sector or business directly subject to such laws in its jurisdiction that permit government access to personal data, or require the assistance of data importer to disclose personal data to public authorities, for surveillance and intelligence gathering purposes?	No, RDC's business is currently not directly subject to such laws.
	a. What is data importer's analysis regarding applicable third country surveillance and intelligence laws under the SCCs and EDPB Guidance?	NAVEX Global and RDC have conducted an analysis and the risk is very low, given the nature of our business. The same conclusions as set forth in this TRA apply to any transfers in non-U.S. countries.
	b. Specifically, what is data importer's analysis regarding third country surveillance laws, especially Section 702 FISA, under the SCCs and EDPB Guidance?	1) Data exporters may decide to proceed with the transfer without supplementary measures, if they consider there to be no reason to believe that the relevant and problematic legislation (for example, those in the U.S.) will be applied, in practice, to the transferred data and/or RDC. a. In our reasonable opinion upon internal and outside counsel review, we do not find third country surveillance laws, including Section 702 FISA from the U.S., to practically apply to these transfers. b. It is important to note that given the broad definitions of these laws, the vast majority of organizations are going to have to acknowledge their potential application. However, this does not mean they directly apply or practically apply in practice. c. We believe RDC is generally out of scope and that these laws are overall not going to apply to the services we provide, as the intent is for surveillance of certain telecom and internet service providers for targeted information. This typically involves to surveillance of real time emails, texts, and chat conversations. The foregoing is not what RDC nor NAVEX Global provides and to obtain this sought for information, authorities would pursue those providers directly as it would be impractical to make a request through RDC. 2) Data exporters may also take into consideration documented practical

#	Factor	Response
		experience of data importer with relevant prior instances of requests for access received from public authorities, including those in the U.S. a. ***To this point, RDC has never received a Section 702 FISA request, an EO 12.333 request or order, or any other country access request.** * b. The EDPB Guidance implies that the lack of requests received in the past plus no prohibition on providing information about such requests, could be sufficient to conclude Section 702 FISA does not apply in practice. Note there is no prohibition on RDC to provide information about these requests. 3) If you conclude Section 702 FISA, or any other potential similar types of surveillance laws, does not apply in practice to the particular transfer, it is possible to proceed with the transfer without any supplementary measures. **a. While NAVEX Global and RDC take the approach that Section 702 FISA does not apply in practice, we still have elected to provide for supplementary measures with regard to these transfers. Please see Section IV (D).**
15	Within the last three (3) years, has the data importer received requests/demands from public authorities in its jurisdiction to disclose EU personal data?	Based on available information, RDC does not receive requests/demands for disclosure of, or access to, EU personal data.
	a. Approximately how many requests/demands from public authorities has the data importer received in that time period concerning EU personal data?	None, to the best of our knowledge.
	b. Approximately how many of these requests/demands are pursuant to criminal law procedure in the destination country? *[Regular court proceedings are not the issue under Schrems II, but intelligence programs are scrutinized.]*	None, to the best of our knowledge.
	c. Approximately how many of these requests/demands are pursuant to national security or intelligence agencies in the destination country?	None, to the best of our knowledge. The data importer can represent that it has not received requests/demands from intelligence agencies.
	d. Has the data importer been able to contest/minimize such disclosure of EU personal data, where appropriate?	Not applicable.
	e. What types of EU personal data has the	

#	Factor	Response
	data importer been required to disclose to public authorities in its jurisdiction?	Not applicable
16	How likely is it that the data importer will receive bulk data surveillance requests to disclose EU personal data to public authorities in its jurisdiction in the future (e.g., based on factors such as the type of services provided and sector in which the data importer operates, its size, number of customers and reputation)?	Unlikely. RDC's entities do not receive requests/demands by public authorities for disclosure of, or access to, EU personal data, and have no reason to believe that they might receive such in the future.
17	Does the data importer maintain annual reports or statistics regarding requests/demands received from law enforcement or intelligence agencies (e.g., number/type of requests/demands, requesting authority, etc.)?	Not applicable. RDC has not received requests from public authorities for EU personal data under the SCCs or otherwise. As a result, if RDC gets such requests in the future, it will notify NAVEX Global and this TRA will be updated accordingly.
18	Does the data importer maintain a written procedure(s) for: 1. Responding to or challenging requests/demands of law enforcement or intelligence agencies that apply to EU personal data? 18. Informing customers of requests/demands from law enforcement or intelligence agencies where permitted by applicable law?	RDC does not maintain a written policy because no requests have ever been received. However, in the event of any request, these would be reviewed by the Privacy Team within Legal and NAVEX Global will be duly notified where required. RDC and NAVEX Global entered into a contractual agreement requiring RDC to cooperate and mutually agree on any appropriate actions, to notify NAVEX Global of any requests unless explicitly required otherwise under applicable law, to put any access request on hold, and to use reasonable efforts to obtain the right to waive any notice prohibitions and oppose any such request and contest its legal validity where possible and permitted. The contract additionally ensures RDC will not make any disclosures that are determined to be massive, disproportionate, and indiscriminate in a manner that would go beyond what is necessary in a democratic society. RDC is obliged to document and demonstrate to the assessments made and the actions taken. RDC undertakes to regularly review, assess, and continuously monitor the scope of the access to personal data by public authorities in the countries where RDC is processing personal data, as well as the safeguards and recourses in place to protect data subjects, and to immediately inform NAVEX Global in the case of a change in applicable law that would materially impact such access by public authorities or recourses available to data subjects.
19	Are the data importer's commitments enabling data subjects to exercise their rights as provided in the SCCs thwarted by	No. Data subjects' rights can be effectively applied in practice. RDC has never

#	Factor	Response
	the laws and/or practices in the U.S. and any other third countries involved, or can these rights be effectively applied in practice?	encountered a situation where it felt it could not enable data subject rights, including judicial redress. We do not believe the laws subject to us prevent us from enabling, supporting, and fulfilling data subject rights under the SCCs.
Onward transfers and exposure to government surveillance		
20	Does the data importer share EU personal data further with third-party data recipients in [the U.S./other jurisdiction]?	Yes, RDC utilizes AWS: cloud hosting. United States for NAVEX Global customers who elect US hosting WNS: Analyst review (applicable for Analyst Review only). SEBPO: Analyst review (applicable for Analyst Review only).
21	What measures does the third-party data recipient take to ensure the protection of EU personal data transferred to it?	Where RDC engages sub-processors that have access to EU personal data, RDC enters into written agreements with sub-processors that include safeguards for EU personal data in accordance with the GDPR requirements.
22	What assurances has the data importer received from third-party data recipients with respect to requests/demands for EU personal data from [U.S./other jurisdiction] public authorities?	RDC will update written agreements with sub-processorsto include additional measures for the protection of EU personal data, where required. Existing data processing addendums are in place under applicable law.
23	Is the vendor's (or its sub-processor's) sector or business directly subject to such laws in its jurisdiction that permit government access to personal data, or require the assistance of data importer to disclose personal data to public authorities, for surveillance and intelligence gathering purposes?	No, RDC does not believe in its reasonable opinion that it or its sub-processors are directly subject to such laws in their jurisdiction.

Conclusion/Risk of transfers

Very limited-risk data transfer

In particular, RDC and NAVEX Global identified the following factors (based on the assessment documented above and any additional information), that are likely to indicate a limited-risk transfer:

No further processing outside of a given screen and/or monitoring request takes place.

The data importer has never received requests/demands from intelligence services for disclosure of EU personal data.

The data importer has received limited requests/demands from public authorities for disclosure of EU personal data (such as for disclosure of employee data), but the requests related to regular criminal law procedure and did not go beyond what is necessary and proportionate to meet the purpose of the

request.

The data importer has a process in place for handling and contesting public authority access requests, if received.

Based on the nature of its services and data processing activities, the data importer does not expect to be the target of requests/demands pursuant to national security or intelligence agencies for disclosure of EU personal data.

Such data transfers are not directly nor practically in scope of requests/demands from national security or intelligence agencies for disclosure of EU personal data.

E. Supplementary Measures

Notwithstanding the Conclusion set forth in the above TRA, RDC has also adopted the following supplemental measures. We believe that by implementing such supplemental measures, we are following best practices and are demonstrating our serious commitment to the protection of customer data.

Contractual safeguards	RDC and NAVEX Global have entered into supplementary contractual assurances as an amendment to the data processing addendum.
	The SCCs themselves contain a number of contractual commitments by RDC and NAVEX Global, aimed at serving as safeguards for EU personal data. We have also entered into a robust general data processing addendum.
Organizational safeguards	RDC would maintain internal record of requests made by public authorities concerning EU personal data.
	RDC would take steps to limit the volume of disclosed data, where possible and applicable.
	RDC would take data minimization measures such as redacting unnecessary identifiable personal data or personal data that may be of increased interest to intelligence agencies before complying with a request to disclosure EU personal data.
Technical safeguards	Encrypt personal data in transit.
	Encrypt personal data at rest.
	Appropriate access controls.

	Enhance data minimization (e.g., store the least amount of data necessary).
	Limit timespan for using personal data "in the clear" (i.e., in identifiable form).
	Obfuscate stored personal data.
	Enable only remote access or view-only access where applicable.

Conclusion

Having regard to the level of risk of the data transfer (**limited risk**), RDC and NAVEX Global considers that the measures identified above are **sufficient and effective** in light of the circumstances of the transfers, in conjunction with the supplementary measures and safeguards provided by the SCCs, to allow the data importer to comply with its obligations under the SCCs and provide an appropriate level of protection for the transfer.

RiskRate US Hosted Sub-processing Activity: Due Diligence with Pacific Strategies & Assessments

NAVEX GLOBAL SUB-PROCESSING ACTIVITY

US HOSTED RISKRATE- PACIFIC STRATEGIES & ASSESSMENTS TRANSFER RISK ASSESSMENT

I. SCOPE

This TRA applies to NAVEX Global's US Hosted RiskRate customers. This TRA applies specifically to the services provided by NAVEX Global's sub-processor, Pacific Strategies & Assessments Limited (PSA).

As part of NAVEX Global's RiskRate services, our customers provide certain personal data in NAVEX Global's systems to be received and processed by PSA as part of the enhanced due diligence screenings. PSA's network is located in the Philippines. PSA logs into NAVEX Global's RiskRate services, hosted in the EU, to view the customer's request. During this viewing, PSA personnel extract relevant details including the level of research required, jurisdiction of research, and names of designated subject entities. An analyst in the Philippines will be assigned to process the provided information. In addition to the Philippines, material relating to a NAVEX Global customer RiskRate request may be processed by PSA staff located in China, the UAE and occasionally, in the Czech Republic. The information required for these offices to process the case element will be sent by internal email to ensure data security is maintained. The staff will conduct the local language or other research required and on completion will return the result over the same secure internal email system.

II. ASSESSING THE ADEQUACY OF EU/UK DATA TRANSFERS –

In assessing the adequacy of transfers of personal data from the EU/UK to NAVEX Global's sub-processor pursuant to the PSA services, we have taken the following steps:

1. **STEP 1:** Identified the relevant data transfers and the legal mechanism that NAVEX Global and sub-processor is relying on for such transfers (e.g., SCCs).

2. **STEP 2:** Conducted due diligence and collected information about the scope of the transfers, the exposure of the sub-processor to local law that may require disclosure of EU personal data about individuals, and any other relevant information.

3. **STEP 3:** Completed the "Transfer Risk Assessment" in **Section IV** to assess whether the SCCs is effective in light of all circumstances of the transfer.

4. **STEP 4:** Included additional "Supplementary Measures" as set forth in **Section IV (D)**.

5. **STEP 5:** Documented the assessment for accountability purposes. We encourage our customers to do the same.

6. **STEP 6:** NAVEX Global and its sub-processor is responsible for the periodic review of the assessment, which should take place at least annually, to ensure that the transfer of the EU personal data continues to be afforded an adequate level of protection.

III. TRANSFER RISK ASSESSMENT

Name Of Data Importer: Pacific Strategies & Assessments Limited ("PSA") (NAVEX Global's sub-processor)

Completed By: NAVEX Global's Privacy Team and PSA's Privacy Team

Date: 25 September 2021

The Processor to Processor SCCs between NAVEX Global and PSA is part of a master services agreement between NAVEX Global and PSA.

A. Does PSA provide the following services to NAVEX Global:

	Data Importer	
Telecommunications	☐ Yes	☒ No
Other electronic communications (such as an Internet Service Provider or a provider of email, text message, VoIP, remote desktop or VPN services)?	☐ Yes	☒ No
Remote computing services	☐ Yes	☒ No
Other communications service where there may be access to wire or electronic communications	☐ Yes	☒ No

If no, please specify the nature of the services provided to NAVEX Global by the data importer: PSA provide Due Dilligence reports uploaded at the customer Data Controller's request into the NAVEX Global service portal.

B. Details of Data Transfers

Data transfer mechanism

Appropriate Processor to Processor SCCs between PSA and NAVEX Global.

Scope of personal data covered by the data transfer mechanism in place

The SCCs cover transfers of EU personal data from the EEA/UK to third countries, including the following categories of data subjects:

- Clients, business partners and vendors of customer Data Controller (who are natural persons)
- Employees or contact persons of customer Data Controller's third-party suppliers, business partners and vendors

C. Transfer Risk Assessment

The table below aids identification and evaluation of risk factors in relation to the specific data transfer. The assessment of each risk factor is recorded in appropriate detail.

#	Factor	Response
Scope of the transfers		
1.	What is the type of transfer?	NAVEX Global's customer submits certain personal data within the RiskRate system which is provided to PSA to utilize for the enhanced due diligence request. The processing by PSA is limited to the performance of the given request.
2.	Is the transfer necessary?	Yes. The transfer is critical and necessary to provide the services to NAVEX Global, on behalf of NAVEX Global's customers.
3.	Is the transfer proportionate?	Yes. The transfer is strictly limited to the due diligence request information provided from the customer.
4.	Is the transfer occasional/non-routine or frequent/routine?	The transfer is non-routine to PSA on a per request basis.
5.	Will the transferred personal data be processed for a relatively long or short period of time?	Personal data is processed for a relatively short period of time to support the applicable due diligence requests.
6.	Is the transferred data encrypted, pseudonymized or otherwise processed in an unintelligible form??	Yes, encryption in transit and at rest during all stages of processing.
Specific circumstances of the transfer		
7.	What are the purposes for which the data are transferred and processed?	The data is directly used to construct an Enhanced Due Diligence report and so contains information in the request including who the report is on, and any supporting details needed to carry out the report.
8.	What are the types of entities involved in the processing?	PSA is a data sub-processor and a private company. NAVEX Global's customers are the data controllers and may consist of both private

#	Factor	Response
		and public companies.
9.	In which sector does the transfer occur?	NAVEX Global provides risk and compliance management SaaS based software. ***This factor is especially important as the purposes of our services is to enable organizations support their risk, ethics, and compliance programs. *** Many of our customers are required by law to conduct appropriate due diligence on third parties. As such, our customers request certain data to be screened and provided back to them, to allow them to conduct this due diligence.
10.	What are the categories of personal data transferred?	Customers can send various categories of data to PSA for processing using NAVEX Global's RiskRate services. This can include company name and details used to identify a company or individual as required by the scope of the work. ***No sensitive data, as defined under the GDPR, is transferred from the customer Data Controller to NAVEX Global nor PSA as part of the RiskRate services. ***
11.	What is the format of the personal data to be transferred?	When personal data is provided to PSA for the purposes described in this TRA, such personal data must be accessible in the clear to fulfill the request.
12.	What is the storage location of the data transferred?	The United States via NAVEX Global's secure servers.
13.	What are the sub-sub-processing activities?	Only where it is essential based on the requirements of the customer request/task (for example where a physical site visit or attendance at court in a separate country is required) will PSA take some of the relevant information and provide it to a sub-sub-processor to complete this section of the tasking. This information is provided through encrypted email, password protected excel sheet or password protected zip folder. All sub-sub-processors agree to and are subject to PSA's data protection and retention policies. Sub-sub-processors agree to delete all record of

#	Factor	Response
		the matter from their system within 60 days of completion of their tasking under the secondary sub processor allocation.
Importer's exposure to government surveillance and practical application of such laws		
14.	Is the data importer's sector or business directly subject to such laws in its jurisdiction that permit government access to personal data, or require the assistance of data importer to disclose personal data to public authorities, for surveillance and intelligence gathering purposes?	No, in our reasonable opinion, PSA's business is currently not directly subject to such laws. As a Philippines registered business PSA must comply with all relevant laws, for example the Expanded Anti-Trafficking in Persons Act of 2012, the Anti-Child Pornography Act of 2009, the Cybercrime Prevention Act of 2012, and the Anti-Terrorism Act of 2020 which may require data access, however, our business sector is not directly subject to these laws.
	a. What is data importer's analysis regarding applicable third country surveillance and intelligence laws under the SCCs and EDPB Guidance?	1) Data exporters may decide to proceed with the transfer without supplementary measures, if they consider there to be no reason to believe that the relevant and problematic legislation will be applied, in practice, to the transferred data and/or PSA. a. Philippines law mandates a court order for surveillance or data access to support an active investigation and supports the international laws on data privacy however in practice we do not believe that the laws are focused on our industry or sector, and so do not apply to these transfers between PSA and NAVEX Global in practice. b. It is important to note that given the broad definitions of these laws, the vast majority of organizations are going to have to acknowledge their potential application. However, this does not mean they directly apply or practically apply in practice. c. We believe PSA is generally out of scope and that these laws are overall not going to apply to the services provided, as the intent is for surveillance of certain telecom and internet service providers for targeted information. This typically involves to surveillance of real time emails, texts, and chat conversations. The foregoing is not what PSA nor NAVEX Global provides and to obtain this sought

#	Factor	Response
		for information, authorities would pursue those providers directly as it would be impractical to make a request through PSA. 2) Data exporters may also take into consideration documented practical experience of data importer with relevant prior instances of requests for access received from public authorities. a. **To this point, PSA has never received a public authority access request.*** b. The EDPB Guidance implies that the lack of requests received in the past plus no prohibition on providing information about such requests, could be sufficient to conclude relevant problematic legislation does not apply in practice. Note there is no prohibition on PSA to provide information about these requests. 3) If you conclude such surveillance laws do not apply in practice to the particular transfer, it is possible to proceed with the transfer without any supplementary measures. **While NAVEX Global and PSA take the approach that such laws don't apply in practice, we still have elected to provide for supplementary measures with regard to these transfers. Please see Section IV (D).**
15.	Within the last three (3) years, has the data importer received requests/demands from public authorities in its jurisdiction to disclose EU personal data?	PSA has not received requests/demands for disclosure of, or access to, EU personal data in the last 3 years.
	a. Approximately how many requests/demands from public authorities has the data importer received in that time period concerning EU personal data?	None, to the best of our knowledge.
	b. Approximately how many of these requests/demands are pursuant to criminal law procedure in the destination country? *[Regular court proceedings are not the issue under Schrems II, but intelligence programs are scrutinized.]*	None, to the best of our knowledge.
	c. Approximately how many of these requests/demands are pursuant to national security or intelligence agencies	None, to the best of our knowledge. The data importer can represent that it has not received

#	Factor	Response
	in the destination country?	requests/demands from intelligence agencies.
	d. Has the data importer been able to contest/minimize such disclosure of EU personal data, where appropriate?	Not applicable.
	e. What types of EU personal data has the data importer been required to disclose to public authorities in its jurisdiction?	Not applicable.
16.	How likely is it that the data importer will receive bulk data surveillance requests to disclose EU personal data to public authorities in its jurisdiction in the future (e.g., based on factors such as the type of services provided and sector in which the data importer operates, its size, number of customers and reputation)?	Unlikely. PSA does not store bulk data on individuals nor provide resources that law enforcement would not be able to get internally without going through PSA.
17.	Does the data importer maintain annual reports or statistics regarding requests/demands received from law enforcement or intelligence agencies (e.g., number/type of requests/demands, requesting authority, etc.)?	Yes. Collected by relevant personnel and reported directly to the management team. Records kept for reporting and review by management team in a dedicated log.
18.	Does the data importer maintain a written procedure(s) for: 1. Responding to or challenging requests/ demands of law enforcement or intelligence agencies that apply to EU personal data? 19. Informing customers of requests/demands from law enforcement or intelligence agencies where permitted by applicable law?	Yes. Covered by "Data Request Policy". Inform customers within 24 hours of receiving authenticated request where possible within the law.
19.	Are the data importer's commitments enabling data subjects to exercise their rights as provided in the SCCs thwarted by the laws and/or practices in the U.S. and any other third countries involved, or can these rights be effectively applied in practice?	PSA has not yet encountered a situation where it felt it could not enable data subject rights, including judicial redress. We do not believe the laws we are subject to prevent us from enabling, supporting, and fulfilling data subject rights under the SCCs.
Onward transfers and exposure to government surveillance		
20.	Does the data importer share EU personal data further with third-party data recipients in [the U.S./other jurisdiction]?	Yes, only where it is essential based on the requirements of the customer request/task (for example where a physical site visit or attendance at court in a separate country is required) will PSA take some of the relevant information and provide it to a sub-sub-processor to complete this section of the tasking. This information is provided through encrypted email, password protected excel sheet or password protected zip folder.

#	Factor	Response
		All sub-sub-processors agree to and are subject to PSA's data protection and retention policies. Sub-sub-processors agree to delete all record of the matter from their system within 60 days of completion of their tasking under the secondary sub processor allocation.
21.	What measures does the third-party data recipient take to ensure the protection of EU personal data transferred to it?	Where PSA engages sub-processors that have access to EU personal data, PSA enters into written agreements with sub-processors that include safeguards for EU personal data in accordance with the GDPR requirements. These include strict requirements on how data can be transferred, and on how long data can be kept before mandatory deletion.
22.	What assurances has the data importer received from third-party data recipients with respect to requests/demands for EU personal data from [U.S./other jurisdiction] public authorities?	PSA has signed policies in place with sub-sub-processors to ensure their compliance and regularly carries out audits to ensure compliance. No sub-sub-party holds significant amounts of data and is obligated to inform PSA in the event of any data request where possible by law so that PSA can inform the relevant parties.
23.	Is the vendor's (or its sub-processor's) sector or business directly subject to such laws in its jurisdiction that permit government access to personal data, or require the assistance of data importer to disclose personal data to public authorities, for surveillance and intelligence gathering purposes?	No. As a Philippines registered business we must comply with all relevant laws, for example the Expanded Anti-Trafficking in Persons Act of 2012, the Anti-Child Pornography Act of 2009, the Cybercrime Prevention Act of 2012, and the Anti-Terrorism Act of 2020 which may require data access however our business sector is not directly subject to these laws and would not fall under any known surveillance or intelligence gathering assistance requests.

Conclusion/Risk of transfers

Very limited-risk data transfer

In particular, PSA and NAVEX Global identified the following factors (based on the assessment documented above and any additional information), that are likely to indicate a limited-risk transfer:

No further processing outside of a given enhanced due diligence request takes place.

The data importer has never received requests/demands from intelligence services for disclosure of EU personal data.

The data importer has received limited requests/demands from public authorities for disclosure of EU

#	Factor	Response
		personal data (such as for disclosure of employee data), but the requests related to regular criminal law procedure and did not go beyond what is necessary and proportionate to meet the purpose of the request. The data importer has a process in place for handling and contesting public authority access requests, if received. Based on the nature of its services and data processing activities, the data importer does not expect to be the target of requests/demands pursuant to national security or intelligence agencies for disclosure of EU personal data. Such data transfers are not directly nor practically in scope of requests/demands from national security or intelligence agencies for disclosure of EU personal data.

D. Supplementary Measures

Notwithstanding the Conclusion set forth in the above TRA, PSA has also adopted the following supplemental measures. We believe that by implementing such supplemental measures, we are following best practices and are demonstrating our serious commitment to the protection of customer data.

Contractual safeguards	PSA and NAVEX Global have entered into supplementary contractual assurances as an amendment to the data processing addendum.
	The SCCs themselves contain a number of contractual commitments by PSA and NAVEX Global, aimed at serving as safeguards for EU personal data. We have also entered into a robust general data processing addendum.
	PSA agrees to audit and monitor its obligations, and to support its customers auditing and monitoring obligations, regarding the level of government access to data.
Organizational safeguards	PSA maintains written processes and procedures to provide for review of and limit the scope of EU personal data disclosed by PSA in response to requests from public authorities.
	PSA maintains internal record of requests made by public authorities concerning EU personal data.
	PSA takes steps to limit the volume of disclosed data, where possible.

	PSA would take data minimization measures such as redacting unnecessary identifiable personal data or personal data that may be of increased interest to intelligence agencies before complying with a request to disclosure EU personal data.
Technical safeguards	PSA ensures that any personal data must be encrypted in transit and at rest with at least AES-128bit encryption.
	Logging of all access with unique identifiers for all actors to ensure audit trails and data confidentiality.
	PSA enforces appropriate strong access controls including 'minimum necessary access' for all work, ensuring that no more access is granted than is necessary to complete the work.
	PSA Implements data minimization (e.g., store the least amount of data necessary including using an alias to refer to projects where possible to ensure data subjects are kept 'need to know'.
	Timespan for any access to personal data "in the clear" is limited to the specific function.
	Personal data is ultimately stored in the US via NAVEX Global's secure data centre.
	Data kept in PSA is held only long enough to collate, present and transfer the requested data, once the transfer is confirmed all copies are wiped from PSA systems. This provides considerably security and reduces any risks or responsibilities brought on by storing the data in PSA systems.

Conclusion

Having regard to the level of risk of the data transfer (**very limited risk**), PSA and NAVEX Global considers that the measures identified above are **sufficient and effective** in light of the circumstances of the transfers, in conjunction with the supplementary measures and safeguards provided by the SCCs, to allow the data importer to comply with its obligations under the SCCs and provide an appropriate level of protection for the transfer.

Disclosures: US Hosted

US HOSTED COI DISCLOSURES - EU/UK DATA TRANSFER RISK ASSESSMENTS

I. INTRODUCTION

NAVEX Global must conduct Transfer Risk Assessments ("TRA" or "TRAs") for transfers of personal data from the European Economic Area ("EEA")[11] or the United Kingdom ("UK") (collectively "EU personal data") to third countries that are not deemed to provide an adequate level of data protection.

II. SCOPE

These TRAs apply to NAVEX Global's US Hosted Disclosures customers.

This TRA process applies to personal data transferred to NAVEX Global pursuant to the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council. This TRA is specifically designed to address Clause 14 of the foregoing set of Standard Contractual Clauses. Personal data from the UK is also in scope and shall be assessed pursuant to the European Commission's decision (C(2010)593) of 5 February 2010 on Standard Contractual Clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection. We collectively refer to the sets of Standard Contractual Clauses as the "SCCs." NAVEX Global agrees and acknowledges the UK will be issuing its own set of standard contractual clauses and related Schrems II guidance. We will update this TRA on an ongoing basis as needed.

This TRA process takes into account the European Data Protection Board's Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data adopted on 18 June 2021 (the "EDPB Guidance").

This TRA is not intended for transfers (i) within the EEA, (ii) between the EEA and the UK, or (iii) from the EEA or UK to a country recognized by the European Commission or UK law as adequate at this time (i.e., Andorra, Argentina, Canada (commercial organizations subject to PIPEDA), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, UK, and Uruguay).

The TRA is completed by the NAVEX Global Privacy Team, which consists of the Data Privacy Officer & Senior Counsel, Deputy Data Privacy Officer & Senior Counsel, and Privacy Counsel.

III. ASSESSING THE ADEQUACY OF EU/UK DATA TRANSFERS – TO NAVEX GLOBAL IN THE U.S.

In assessing the adequacy of transfers of personal data from the EU/UK to NAVEX Global in the U.S. we have taken the following steps:

1. **STEP 1:** Identified the relevant data transfers and the legal mechanism that NAVEX Global is relying on for such transfers (e.g., SCCs).

2. **STEP 2:** Conducted due diligence and collected information about the scope of the transfers, the exposure of NAVEX Global to local law that may require disclosure of EU personal data about individuals, and any other relevant information.

3. **STEP 3:** Completed the "Transfer Risk Assessment" in **Section IV** to assess whether the SCCs is effective in light of all circumstances of the transfer.

[11] The European Economic Area consists of the Member States of the EU (Austria, Belgium, Bulgaria, Croatia, Cyprus, Czechia, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain and Sweden), plus Iceland, Liechtenstein and Norway.

4. **STEP 4:** Included additional "Supplementary Measures" as set forth in **Section IV (D)**.

5. **STEP 5:** Documented the assessment for accountability purposes. We encourage our customers to do the same.

6. **STEP 6:** NAVEX Global is responsible for the periodic review of the assessment, which should take place at least annually, to ensure that the transfer of the EU personal data continues to be afforded an adequate level of protection.

IV. TRANSFER RISK ASSESSMENT

Name Of Data Importer: NAVEX Global

Scope of TRA: Transfers to NAVEX Global in the United States as part of the Disclosures Services provided to US Hosted Customers

****Our customers elect the hosting and storage location. As a result, NAVEX Global has many customers subject to the GDPR on our US hosted and storage configuration, as chosen by the customer.****

Completed By: NAVEX Global's Privacy Team

Date: 25 September 2021

A. Type of Data Importer

Name of data importer: NAVEX Global. The SCCs between customer and NAVEX Global is part of a master services agreement between customer and NAVEX Global, Inc., a Delaware corporation, having its principal place of business at 5500 Meadows Road, Suite 500, Lake Oswego, Oregon 97035.

Upon reviewing the broad definitions set forth within U.S. surveillance laws under scrutiny pursuant to the CJEU ruling in the Schrems II case, NAVEX Global identifies itself as follows:

NAVEX Global does not consider itself a "telecommunications carrier" as defined in 47 U.S.C. 152.

NAVEX Global acknowledges that certain of its services could be viewed by U.S. government authorities as an "electronic communication service" as defined in 18 U.S.C. 2510.

NAVEX Global acknowledges that certain of its services could be viewed by U.S. government authorities as a "remote computing service" as defined in 18 U.S.C. 2711.

NAVEX Global acknowledges that certain of its services could be viewed by U.S. government authorities as other communication services where there may be access to wire or electronic communications.

B. Details of Data Transfers

Data transfer mechanism
Appropriate Controller to Processor SCCs between customer and NAVEX Global.

Scope of personal data covered by the data transfer mechanism in place

The SCCs cover transfers of EU personal data from the EEA/UK to the U.S., including the following categories of data subjects:

- Employees of data exporter
- Clients, business partners and vendors of data exporter (who are natural persons)
- Employees or contact persons of data exporters' third-party suppliers, business partners and vendors
- Data exporter's users authorized by data exporter to use the relevant Service(s)

C. Transfer Risk Assessment

The table below aids identification and evaluation of risk factors in relation to the specific data transfer. The assessment of each risk factor is recorded in appropriate detail.

#	Factor	Response
Scope of the transfers		
1.	What is the type of transfer?	EU personal data is stored and hosted within the U.S. NAVEX Global's hosting providers either cannot or do not access EU personal data. Select NAVEX Global personnel have access to provision the services in accordance with our agreements, subject to the principle of least privilege and our access control policies and processed.
2.	Is the transfer necessary?	Yes. NAVEX Global's customers elect their storage and hosting location. Many customers choose and prefer the U.S. For NAVEX Global to securely store the data in the U.S. as elected by the customer, they must transfer the data to this location via the services. For NAVEX Global to be able to provide the services, our personnel must be able to access the systems to provide support, administrative functions, technical work, and IT/Hosting support.

#	Factor	Response
		Without the above, we wouldn't be able to provide the services or meet our service level commitments.
3.	Is the transfer proportionate?	Yes. The data is securely stored and NAVEX Global processes data to maintain the services and in accordance with its customer's instructions.
4.	Is the transfer occasional/non-routine or frequent/routine?	The transfer is frequent/routine. This is necessary in order to host, store, and provide the services from the U.S. as requested.
5.	Will the transferred personal data be processed for a relatively long or short period of time?	During the life of the agreement, the customer decides how long to maintain the personal data in the system in accordance with their own policies and processes. NAVEX Global maintains the personal data within the services, as elected by the customer, for the duration of the agreement.
6.	Is the transferred data encrypted and/ or pseudonymized?	Yes. NAVEX Global employs encryption at rest using either full-disk encryption or within the database using TDE. Data at rest will be encrypted using AES 256 or better, data in flight will be accomplished using TLS 1.2 or higher on public untrusted networks. Upon reviewing pseudonymization in the context of this transfer, it is inapplicable to the services we need to support.
Specific circumstances of the transfer		
7.	What are the purposes for which the data are transferred and processed?	To securely store the data in the U.S. as requested by our customers. To provide the best support, maintenance, and services as committed to in our agreements with our customers.
8.	What are the types of entities involved in the processing?	NAVEX Global is a data processor and a private company. Our customers are the data controllers and may consist of both private and public companies.
9.	In which sector does the transfer occur?	

#	Factor	Response
		NAVEX Global provides risk and compliance management SaaS based software. ***This factor is especially important as the purposes of our services is to enable organizations support their risk, ethics, and compliance programs. ***
10.	What are the categories of personal data transferred?	• Name (first and last), email address, job site, job title, department, supervisor, log-in credentials, completion status, details about the reported conflicts, time and date of disclosure. ****No sensitive data, as defined under the GDPR, is transferred as part of the Disclosures services.****
11.	What is the format of the personal data to be transferred?	NAVEX Global employs encryption at rest using either full-disk encryption or within the database using TDE. Data at rest will be encrypted using AES 256 or better, data in flight will be accomplished using TLS 1.2 or higher on public untrusted networks. When access is provided to NAVEX Global personnel in the U.S. for the purposes described in this TRA, customer data must be accessible in the clear to provide the requisite support or service function.
12.	What is the storage location of the data transferred?	The United States.
13.	What are the sub-processing activities?	Please see details here: https://www.navexglobal.com/en-us/service-hosting-providers. All requirements are flown down to each sub-processor.
Importer's exposure to government surveillance and practical application of Section 702 FISA		
14.	Is the data importer's sector or business directly subject to such laws in its jurisdiction that permit government access to personal data, or require the assistance of data importer to disclose personal data to public authorities, for surveillance and intelligence gathering purposes?	No. In our reasonable opinion upon internal and outside counsel review, we do not find NAVEX Global to be directly subject to such laws. As a practical matter based on the nature of NAVEX Global's services, the types of personal data processed, and the absence of any prior requests received in the past, NAVEX Global believes it is extremely unlikely to receive requests from U.S. government agencies to obtain customer data for national security purposes or to participate in the types of U.S. bulk surveillance programs scrutinized by the

#	Factor	Response
		CJEU in its recent ruling on data transfer mechanisms.
	a. Specifically, what is data importer's analysis regarding Section 702 FISA under the SCCs and EDPB Guidance?	1) Data exporters may decide to proceed with the transfer without supplementary measures, if they consider there to be no reason to believe that the relevant and problematic legislation (those in the U.S. in this instance) will be applied, in practice, to the transferred data and/or NAVEX Global. a. In our reasonable opinion upon internal and outside counsel review, we do not find U.S. surveillance laws, including Section 702 FISA, to practically apply to these transfers. b. It is important to note that given the broad definitions of these laws, the vast majority of organizations are going to have to acknowledge their potential application. However, this does not mean they directly apply or practically apply in practice. c. We believe NAVEX Global is generally out of scope and that these laws are overall not going to apply to the services we provide, as the intent is for surveillance of certain telecom and internet service providers for targeted information. This typically involves to surveillance of real time emails, texts, and chat conversations. The foregoing is not what NAVEX Global provides and in order to obtain this sought for information, authorities would pursue those providers directly as it would be impractical to make a request through NAVEX Global. 2) Data exporters may also take into consideration documented practical experience of data importer with relevant prior instances of requests for access received from public authorities in the U.S. a. ***To this point, NAVEX Global has never received a Section 702 FISA request or an EO 12.333 request or order. Please see our Public Authority Disclosure Request Policy for more details.** * b. The EDPB Guidance implies that the lack of requests received in the past plus no prohibition on providing information about such requests, could be sufficient to conclude Section 702 FISA does not apply in

#	Factor	Response
		practice. Note there is no prohibition on NAVEX Global to provide information about these requests. 3) If you conclude Section 702 FISA does not apply in practice to the particular transfer, it is possible to proceed with the transfer without any supplementary measures. **a. While NAVEX Global takes the approach that Section 702 FISA does not apply in practice, we still have elected to provide for supplementary measures with regard to these transfers. Please see Section IV (D).**
15.	Within the last three (3) years, has the data importer received requests/demands from public authorities in its jurisdiction to disclose EU personal data pursuant to the SCCs?	No, not to the best of our knowledge.
	a. Approximately how many requests/demands from public authorities has the data importer received in that time period concerning EU personal data pursuant to the SCCs?	None, to the best of our knowledge.
	b. Approximately how many of these requests/demands are pursuant to criminal law procedure in the destination country? *[Regular court proceedings are not the issue under Schrems II, but intelligence programs are scrutinized.]*	While NAVEX Global has not received a Section 702 FISA request, an EO 12.333 request or order, or a public authority request specifically targeting EU personal data under the SCCs, we have received a limited number of formal requests or demands from U.S. government authorities concerning customer data. These requests have been made in the context of criminal and civil actions in the form of a subpoena issued to NAVEX Global as a third party, by a state or federal court. In each instance, we've notified the customer straight away and they have directed us to comply with the subpoena. We've only fulfilled such requests with full customer clearance and direction on how to handle.
	c. Approximately how many of these requests/demands are pursuant to national security or intelligence agencies in the destination country?	None, to the best of our knowledge. The data importer can represent that it has not received requests/demands from intelligence agencies. NAVEX Global offers signed contracts, warranting it has not received such requests, via either a data processing addendum or amendment to data processing addendum.
	d. Has the data importer been able to contest/minimize such disclosure of EU personal data, where appropriate?	Not applicable
	e. What types of EU personal data has the data importer been required to disclose to public authorities in its jurisdiction?	Not applicable
16.	How likely is it that the data importer will	

#	Factor	Response
	receive bulk data surveillance requests to disclose EU personal data to public authorities in its jurisdiction in the future (e.g., based on factors such as the type of services provided and sector in which the data importer operates, its size, number of customers and reputation)?	Unlikely. As a practical matter based on the nature of NAVEX Global's services, the types of personal data processed, and the absence of any prior requests received in the past, NAVEX Global believes it is extremely unlikely to receive requests from U.S. government agencies to obtain customer data for national security purposes or to participate in the types of U.S. bulk surveillance programs scrutinized by the CJEU in its recent ruling on data transfer mechanisms. We have no reason to believe we may receive such requests in the future.
17.	Does the data importer maintain annual reports or statistics regarding requests/demands received from law enforcement or intelligence agencies (e.g., number/type of requests/demands, requesting authority, etc.)?	Not applicable. NAVEX Global has not received a Section 702 FISA request, an EO 12.333 request or order, or a public authority request specifically targeting EU personal data under the SCCs. As a result, if we get such requests in the future, we will provide such statistics and update our TRA process and Public Authority Disclosure Policy accordingly.
18.	Does the data importer maintain a written procedure(s) for: 1. Responding to or challenging requests/demands of law enforcement or intelligence agencies that apply to EU personal data? 20. Informing customers of requests/demands from law enforcement or intelligence agencies where permitted by applicable law?	Yes, please see our Public Authority Disclosure Request Policy.
19.	Are the data importer's commitments enabling data subjects to exercise their rights as provided in the SCCs thwarted by the laws and/or practices in the U.S. or can these rights be effectively applied in practice?	NAVEX Global has never encountered a situation where it felt it could not enable data subject rights, including judicial redress. We do not believe the laws subject to us prevent us from enabling, supporting, and fulfilling data subject rights under the SCCs.
Onward transfers and exposure to government surveillance		
20.	Does the data importer share EU personal data further with sub-processors whose processing takes place in third countries?	No.
Conclusion/Risk of transfers **Likely limited-risk data transfer** **In particular, NAVEX Global identified the following factors (based on the assessment**		

#	Factor	Response
	documented above and any additional information), that are likely to indicate a limited-risk transfer: The data importer has never received requests/demands from intelligence services for disclosure of EU personal data. The data importer has received limited requests/demands from public authorities for disclosure of EU personal data (such as for disclosure of employee data), but the requests related to regular criminal law procedure and did not go beyond what is necessary and proportionate to meet the purpose of the request. The data importer has a process in place for handling and contesting public authority access requests, if received. Based on the nature of its services and data processing activities, the data importer does not expect to be the target of requests/demands pursuant to national security or intelligence agencies for disclosure of EU personal data. Such data transfers are not directly nor practically in scope of requests/demands from national security or intelligence agencies for disclosure of EU personal data.	

D. Supplementary Measures

Notwithstanding the Conclusion set forth in the above TRA, NAVEX Global has also adopted the following supplemental measures. We believe that by implementing such supplemental measures, we are following best practices and are demonstrating our serious commitment to the protection of customer data.

Contractual safeguards	The SCCs themselves contain a number of contractual commitments by NAVEX Global and its customer, aimed at serving as safeguards for EU personal data.
	Supplementary contractual assurances are offered via our standard data processing addendum or an amendment to the data processing addendum. Please reach out to privacy@navexglobal.com in order to get this in place.
	NAVEX Global agrees to audit and monitor its obligations, and to support its customers auditing and monitoring obligations, regarding the level of government access to data.
	NAVEX Global provides a data processing agreement to support GDPR compliance, which includes the SCCs. As the data processor/importer, we process personal data strictly in accordance with your instructions and to provide the services. Our customers are the owners of the personal data within our service applications.

	NAVEX Global offers a Data Security Addendum, providing for contractual commitments to its information security program.
Organizational safeguards	NAVEX Global maintains written processes and procedures which provide for review of and limit the scope of EU personal data disclosed by NAVEX Global in response to requests from public authorities. Please see our Public Authority Disclosure Request Policy.
	NAVEX Global maintains internal records of requests made by public authorities concerning EU personal data.
	NAVEX Global takes steps to limit the volume of disclosed data, where possible.
	NAVEX Global would take data minimization measures such as redacting unnecessary identifiable personal data or personal data that may be of increased interest to intelligence agencies before complying with a request to disclosure EU personal data.
	NAVEX Global has developed a Standard Contractual Clauses Assurance Guide, which details our commitment to compliance with the SCCs. NAVEX Global remains a participant and has certified its compliance with the EU-U.S. Privacy Shield Framework and the Swiss- U.S. Privacy Shield Framework. NAVEX Global, Inc. is committed to subjecting all personal information received from the European Economic Area, United Kingdom, and Switzerland, respectively, in reliance on each Privacy Shield Framework, to the Frameworks' applicable Principles. To learn more about the Privacy Shield program, and to view our certification, please visit https://www.privacyshield.gov. NAVEX Global provides an independent recourse mechanism to EU individuals, currently TrustArc.
Technical safeguards	Encrypt personal data in transit.
	Encrypt personal data at rest.
	Appropriate access controls.

	Customers can implement data minimization (e.g., store the least amount of data necessary).
	Timespan for any access to personal data "in the clear" is limited to the specific function.
	NAVEX Global equips its services with self-servicing functionality, allowing you to manage the personal data on your own through the use of the services. NAVEX Global engages a recognized, independent third party to conduct a Statement on Standards for Attestation Engagements No. 16, Service Organization Control 2, Type 2 ("SSAE 18 SOC 2 Type 2") audit (or its equivalent or successor) of its information security program and its administrative, technical, and physical safeguards for all facilities used to deliver the Services, which specifically includes privacy controls. NAVEX Global maintains an annual Standardized Information Gathering Questionnaire ("SIG"), which details our robust security program with supporting documentation.

Conclusion

Having regard to the level of risk of the data transfer (**limited risk**), NAVEX Global considers that the measures identified above are **sufficient and effective** in light of the circumstances of the transfers, in conjunction with the supplementary measures and safeguards provided by the SCCs, to allow the data importer to comply with its obligations under the SCCs and provide an appropriate level of protection for the transfer.

Lockpath: US Hosted

NAVEX GLOBAL

US HOSTED LOCKPATH - EU/UK DATA TRANSFER RISK ASSESSMENTS

I. INTRODUCTION

NAVEX Global must conduct Transfer Risk Assessments ("TRA" or "TRAs") for transfers of personal data from the European Economic Area ("EEA")[12] or the United Kingdom ("UK") (collectively "EU personal data") to third countries that are not deemed to provide an adequate level of data protection.

[12] The European Economic Area consists of the Member States of the EU (Austria, Belgium, Bulgaria, Croatia, Cyprus, Czechia, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain and Sweden), plus Iceland, Liechtenstein and Norway.

II. SCOPE

These TRAs apply to NAVEX Global's US Hosted Lockpath customers.

This TRA process applies to personal data transferred to NAVEX Global pursuant to the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council. This TRA is specifically designed to address Clause 14 of the foregoing set of Standard Contractual Clauses. Personal data from the UK is also in scope and shall be assessed pursuant to the European Commission's decision (C(2010)593) of 5 February 2010 on Standard Contractual Clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection. We collectively refer to the sets of Standard Contractual Clauses as the "SCCs." NAVEX Global agrees and acknowledges the UK will be issuing its own set of standard contractual clauses and related Schrems II guidance. We will update this TRA on an ongoing basis as needed.

This TRA process takes into account the European Data Protection Board's Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data adopted on 18 June 2021 (the "EDPB Guidance").

NAVEX Global has separate TRAs for its non-affiliate sub-processing activities, where NAVEX Global utilizes such sub-processors for the processing of personal data who receive customer EU personal data in third countries that have not been deemed adequate by the European Commission. These are available as part of our compliance documentation and on request.

This TRA is not intended for transfers (i) within the EEA, (ii) between the EEA and the UK, or (iii) from the EEA or UK to a country recognized by the European Commission or UK law as adequate at this time (i.e., Andorra, Argentina, Canada (commercial organizations subject to PIPEDA), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, UK, and Uruguay).

The TRA is completed by the NAVEX Global Privacy Team, which consists of the Data Privacy Officer & Senior Counsel, Deputy Data Privacy Officer & Senior Counsel, and Privacy Counsel.

III. ASSESSING THE ADEQUACY OF EU/UK DATA TRANSFERS – TO NAVEX GLOBAL IN THE U.S.

In assessing the adequacy of transfers of personal data from the EU/UK to NAVEX Global in the U.S. we have taken the following steps:

1. **STEP 1:** Identified the relevant data transfers and the legal mechanism that NAVEX Global is relying on for such transfers (e.g., SCCs).

2. **STEP 2:** Conducted due diligence and collected information about the scope of the transfers, the exposure of NAVEX Global to local law that may require disclosure of EU personal data about individuals, and any other relevant information.

3. **STEP 3:** Completed the "Transfer Risk Assessment" in **Section IV** to assess whether the SCCs is effective in light of all circumstances of the transfer.

4. **STEP 4:** Included additional "Supplementary Measures" as set forth in **Section IV (D)**.

5. **STEP 5:** Documented the assessment for accountability purposes. We encourage our customers to do the same.

6. **STEP 6:** NAVEX Global is responsible for the periodic review of the assessment, which should take place at least annually, to ensure that the transfer of the EU personal data continues to be afforded an adequate level of protection.

IV. TRANSFER RISK ASSESSMENT

Name Of Data Importer: NAVEX Global

Scope of TRA: Transfers to NAVEX Global in the United States as part of the Lockpath Services provided to US Hosted Customers

****Our customers elect the hosting and storage location. As a result, NAVEX Global has many customers subject to the GDPR on our US hosted and storage configuration, as chosen by the customer.****

Completed By: NAVEX Global's Privacy Team

Date: 25 September 2021

Type of Data Importer

Name of data importer: NAVEX Global. The SCCs between customer and NAVEX Global is part of a master services agreement between customer and NAVEX Global, Inc., a Delaware corporation, having its principal place of business at 5500 Meadows Road, Suite 500, Lake Oswego, Oregon 97035.

Upon reviewing the broad definitions set forth within U.S. surveillance laws under scrutiny pursuant to the CJEU ruling in the Schrems II case, NAVEX Global identifies itself as follows:

NAVEX Global does not consider itself a "telecommunications carrier" as defined in 47 U.S.C. 152.

NAVEX Global acknowledges that certain of its services could be viewed by U.S. government authorities as an "electronic communication service" as defined in 18 U.S.C. 2510.

NAVEX Global acknowledges that certain of its services could be viewed by U.S. government authorities as a "remote computing service" as defined in 18 U.S.C. 2711.

NAVEX Global acknowledges that certain of its services could be viewed by U.S. government authorities as other communication services where there may be access to wire or electronic communications.

A. Details of Data Transfers

Data transfer mechanism
Appropriate Controller to Processor SCCs between customer and NAVEX Global.

Scope of personal data covered by the data transfer mechanism in place

The SCCs cover transfers of EU personal data from the EEA/UK to the U.S., including the following categories of data subjects:

- Employees of data exporter
- Clients, business partners and vendors of data exporter (who are natural persons)
- Employees or contact persons of data exporters' third-party suppliers, business partners and vendors
- Data exporter's users authorized by data exporter to use the relevant Service(s)

B. Transfer Risk Assessment

The table below aids identification and evaluation of risk factors in relation to the specific data transfer. The assessment of each risk factor is recorded in appropriate detail.

#	Factor	Response
Scope of the transfers		
1.	What is the type of transfer?	EU personal data is stored and hosted within the U.S. NAVEX Global's hosting providers either cannot or do not access EU personal data. Select NAVEX Global personnel have access to provision the services in accordance with our agreements, subject to the principle of least privilege and our access control policies and processed.
2.	Is the transfer necessary?	Yes. NAVEX Global's customers elect their storage and hosting location. Many customers choose and prefer the U.S. For NAVEX Global to securely store the data in the U.S. as elected by the customer, they must transfer the data to this location via the services. For NAVEX Global to be able to provide the services, our personnel must be able to access the systems to provide support, administrative functions, technical work and product management, and IT/Hosting support.

#	Factor	Response
		Without the above, we wouldn't be able to provide the services or meet our service level commitments.
3.	Is the transfer proportionate?	Yes. Customer elects the U.S. for storage. The data is securely stored and NAVEX Global processes data to maintain the services and in accordance with its customer's instructions.
4.	Is the transfer occasional/non-routine or frequent/routine?	The transfer is frequent/routine. This is necessary in order to host, store, and provide the services from the U.S. as requested.
5.	Will the transferred personal data be processed for a relatively long or short period of time?	During the life of the agreement, the customer decides how long to maintain the personal data in the system in accordance with their own policies and processes. NAVEX Global maintains the personal data within the services, as elected by the customer, for the duration of the agreement.
6.	Is the transferred data encrypted and/ or pseudonymized?	Yes. NAVEX Global employs encryption at rest using either full-disk encryption or within the database using TDE. Data at rest will be encrypted using AES 256 or better, data in flight will be accomplished using TLS 1.2 or higher on public untrusted networks. Upon reviewing pseudonymization in the context of this transfer, it is inapplicable to the services we need to support.
Specific circumstances of the transfer		
7.	What are the purposes for which the data are transferred and processed?	To securely store the data in the U.S. as requested by our customers. To provide the best support, maintenance, and services as committed to in our agreements with our customers.
8.	What are the types of entities involved in the processing?	NAVEX Global is a data processor and a private company. Our customers are the data controllers and may consist of both private and public companies.

#	Factor	Response
9.	In which sector does the transfer occur?	NAVEX Global provides risk and compliance management SaaS based software. ***This factor is especially important as the purposes of our services is to enable organizations support their risk, ethics, and compliance programs. ***
10.	What are the categories of personal data transferred?	• Name (first and last), email address, log-in credentials, and other categories such as job title. ****No sensitive data, as defined under the GDPR, is transferred as part of the Lockpath services.****
11.	What is the format of the personal data to be transferred?	NAVEX Global employs encryption at rest using either full-disk encryption or within the database using TDE. Data at rest will be encrypted using AES 256 or better, data in flight will be accomplished using TLS 1.2 or higher on public untrusted networks. When access is provided to NAVEX Global personnel in the U.S. for the purposes described in this TRA, customer data must be accessible in the clear to provide the requisite support or service function.
12.	What is the storage location of the data transferred?	The United States.
13.	What are the sub-processing activities?	Please see details here: https://www.navexglobal.com/en-us/service-hosting-providers. These are temporary and limited sub-processing activities. All requirements are flown down to each sub-processor.
Importer's exposure to government surveillance and practical application of Section 702 FISA		
14.	Is the data importer's sector or business directly subject to such laws in its jurisdiction that permit government access to personal data, or require the assistance of data importer to disclose personal data to public authorities, for surveillance and intelligence gathering purposes?	No. In our reasonable opinion upon internal and outside counsel review, we do not find NAVEX Global to be directly subject to such laws. As a practical matter based on the nature of NAVEX Global's services, the types of personal data processed, and the absence of any prior requests received in the past, NAVEX Global believes it is extremely unlikely to receive requests from U.S. government agencies to obtain customer data for national security

#	Factor	Response
		purposes or to participate in the types of U.S. bulk surveillance programs scrutinized by the CJEU in its recent ruling on data transfer mechanisms.
	a. Specifically, what is data importer's analysis regarding Section 702 FISA under the SCCs and EDPB Guidance?	1) Data exporters may decide to proceed with the transfer without supplementary measures, if they consider there to be no reason to believe that the relevant and problematic legislation (those in the U.S. in this instance) will be applied, in practice, to the transferred data and/or NAVEX Global. a. In our reasonable opinion upon internal and outside counsel review, we do not find U.S. surveillance laws, including Section 702 FISA, to practically apply to these transfers. b. It is important to note that given the broad definitions of these laws, the vast majority of organizations are going to have to acknowledge their potential application. However, this does not mean they directly apply or practically apply in practice. c. We believe NAVEX Global is generally out of scope and that these laws are overall not going to apply to the services we provide, as the intent is for surveillance of certain telecom and internet service providers for targeted information. This typically involves to surveillance of real time emails, texts, and chat conversations. The foregoing is not what NAVEX Global provides and in order to obtain this sought for information, authorities would pursue those providers directly as it would be impractical to make a request through NAVEX Global. 2) Data exporters may also take into consideration documented practical experience of data importer with relevant prior instances of requests for access received from public authorities in the U.S. a. ***To this point, NAVEX Global has never received a Section 702 FISA request or an EO 12.333 request or order. Please see our Public Authority Disclosure Request Policy for more details.** * b. The EDPB Guidance implies that the lack of requests received in the

#	Factor	Response
		past plus no prohibition on providing information about such requests, could be sufficient to conclude Section 702 FISA does not apply in practice. Note there is no prohibition on NAVEX Global to provide information about these requests. 3) If you conclude Section 702 FISA does not apply in practice to the particular transfer, it is possible to proceed with the transfer without any supplementary measures. **a. While NAVEX Global takes the approach that Section 702 FISA does not apply in practice, we still have elected to provide for supplementary measures with regard to these transfers. Please see Section IV (D).**
15.	Within the last three (3) years, has the data importer received requests/demands from public authorities in its jurisdiction to disclose EU personal data pursuant to the SCCs?	No.
	a. Approximately how many requests/demands from public authorities has the data importer received in that time period concerning EU personal data pursuant to the SCCs?	None.
	b. Approximately how many of these requests/demands are pursuant to criminal law procedure in the destination country? *[Regular court proceedings are not the issue under Schrems II, but intelligence programs are scrutinized.]*	****NAVEX Global has never received <u>ANY</u> requests for data pertaining to its Lockpath services. *** While NAVEX Global has not received requests from public authorities for EU personal data under the SCCs or otherwise, we have received a limited number of formal requests or demands from U.S. government **authorities concerning customer data pertaining to its hotline and incident management services**. These requests have been made in the context of criminal and civil actions in the form of a subpoena issued to NAVEX Global as a third party, by a state or federal court. In each instance, we've notified the customer straight away and they have directed us to comply with the subpoena. We've only fulfilled such requests with full customer clearance and direction on how to handle.
	c. Approximately how many of these requests/demands are pursuant to national security or intelligence agencies in the destination country?	None, to the best of our knowledge. The data importer can represent that it has not received requests/demands from intelligence agencies. NAVEX Global offers signed contracts, warranting it has not received such requests, via either a data processing addendum or

#	Factor	Response
		amendment to data processing addendum.
	d. Has the data importer been able to contest/minimize such disclosure of EU personal data, where appropriate?	Not applicable
	e. What types of EU personal data has the data importer been required to disclose to public authorities in its jurisdiction?	Not applicable
16.	How likely is it that the data importer will receive bulk data surveillance requests to disclose EU personal data to public authorities in its jurisdiction in the future (e.g., based on factors such as the type of services provided and sector in which the data importer operates, its size, number of customers and reputation)?	Unlikely. As a practical matter based on the nature of NAVEX Global's services, the types of personal data processed, and the absence of any prior requests received in the past, NAVEX Global believes it is extremely unlikely to receive requests from U.S. government agencies to obtain customer data for national security purposes or to participate in the types of U.S. bulk surveillance programs scrutinized by the CJEU in its recent ruling on data transfer mechanisms. We have no reason to believe we may receive such requests in the future.
17.	Does the data importer maintain annual reports or statistics regarding requests/demands received from law enforcement or intelligence agencies (e.g., number/type of requests/demands, requesting authority, etc.)?	Not applicable. NAVEX Global has not received requests from public authorities for EU personal data under the SCCs or otherwise. As a result, if we get such requests in the future, we will provide such statistics and update our TRA process and Public Authority Disclosure Policy accordingly.
18.	Does the data importer maintain a written procedure(s) for: 1. Responding to or challenging requests/demands of law enforcement or intelligence agencies that apply to EU personal data? 21. Informing customers of requests/demands from law enforcement or intelligence agencies where permitted by applicable law?	Yes, please see our Public Authority Disclosure Request Policy.
19.	Are the data importer's commitments enabling data subjects to exercise their rights as provided in the SCCs thwarted by the laws and/or practices in the U.S. or can these rights be effectively applied in practice?	NAVEX Global has never encountered a situation where it felt it could not enable data subject rights, including judicial redress. We do not believe the laws subject to us prevent us from enabling, supporting, and fulfilling data subject rights under the SCCs.
Onward transfers and exposure to government surveillance		
20.	Does the data importer share EU personal data further with sub-processors whose	Yes.

#	Factor	Response
	processing takes place in third countries?	
21.	What measures does the third-party data recipient take to ensure the protection of EU personal data transferred to it?	NAVEX Global enters into written agreements with sub-processors that include safeguards for EU personal data in accordance with the GDPR requirements.
22.	What assurances has the data importer received from third-party data recipients with respect to requests/demands for EU personal data from [U.S./other jurisdiction] public authorities?	NAVEX Global has updated, or is in the process of updating, all written agreements with sub-processors to include additional measures for the protection of EU personal data, where required.

Conclusion/Risk of transfers

Likely limited-risk data transfer

In particular, NAVEX Global identified the following factors (based on the assessment documented above and any additional information), that are likely to indicate a limited-risk transfer:

The data importer has never received requests/demands from intelligence services for disclosure of EU personal data.

The data importer has received limited requests/demands from public authorities for disclosure of EU personal data (such as for disclosure of employee data), but the requests related to regular criminal law procedure and did not go beyond what is necessary and proportionate to meet the purpose of the request.

The data importer has a process in place for handling and contesting public authority access requests, if received.

Based on the nature of its services and data processing activities, the data importer does not expect to be the target of requests/demands pursuant to national security or intelligence agencies for disclosure of EU personal data.

Such data transfers are not directly nor practically in scope of requests/demands from national security or intelligence agencies for disclosure of EU personal data.

C. Supplementary Measures

Notwithstanding the Conclusion set forth in the above TRA, NAVEX Global has also adopted the following supplemental measures. We believe that by implementing such supplemental measures, we are following best practices and are demonstrating our serious commitment to the protection of customer data.

Contractual safeguards	The SCCs themselves contain a number of contractual

	commitments by NAVEX Global and its customer, aimed at serving as safeguards for EU personal data.
	Supplementary contractual assurances are offered via our standard data processing addendum or an amendment to the data processing addendum. Please reach out to privacy@navexglobal.com in order to get this in place.
	NAVEX Global agrees to audit and monitor its obligations, and to support its customers auditing and monitoring obligations, regarding the level of government access to data.
	NAVEX Global provides a data processing agreement to support GDPR compliance, which includes the SCCs. As the data processor/importer, we process personal data strictly in accordance with your instructions and to provide the services. Our customers are the owners of the personal data within our service applications. NAVEX Global offers a Data Security Addendum, providing for contractual commitments to its information security program.
Organizational safeguards	NAVEX Global maintains written processes and procedures which provide for review of and limit the scope of EU personal data disclosed by NAVEX Global in response to requests from public authorities. Please see our Public Authority Disclosure Request Policy.
	NAVEX Global maintains internal records of requests made by public authorities concerning EU personal data.
	NAVEX Global takes steps to limit the volume of disclosed data, where possible.
	NAVEX Global would take data minimization measures such as redacting unnecessary identifiable personal data or personal data that may be of increased interest to intelligence agencies before complying with a request to disclosure EU personal data.
	NAVEX Global has developed a Standard Contractual Clauses Assurance Guide, which details our commitment to compliance with the SCCs. NAVEX Global remains a participant and has certified its compliance with the EU-U.S. Privacy Shield Framework and the Swiss- U.S. Privacy Shield Framework. NAVEX Global, Inc. is committed to subjecting all personal information received from the European Economic Area, United Kingdom, and Switzerland, respectively, in reliance on each Privacy Shield Framework, to the Frameworks' applicable Principles. To learn more about the Privacy

	Shield program, and to view our certification, please visit https://www.privacyshield.gov. NAVEX Global provides an independent recourse mechanism to EU individuals, currently TrustArc.
Technical safeguards	Encrypt personal data in transit.
	Encrypt personal data at rest.
	Appropriate access controls.
	Customers can implement data minimization (e.g., store the least amount of data necessary).
	Timespan for any access to personal data "in the clear" is limited to the specific function.
	NAVEX Global equips its services with self-servicing functionality, allowing you to manage the personal data on your own through the use of the services. NAVEX Global engages a recognized, independent third party to conduct a Statement on Standards for Attestation Engagements No. 16, Service Organization Control 2, Type 2 ("SSAE 18 SOC 2 Type 2") audit (or its equivalent or successor) of its information security program and its administrative, technical, and physical safeguards for all facilities used to deliver the Services, which specifically includes privacy controls. NAVEX Global maintains an annual Standardized Information Gathering Questionnaire ("SIG"), which details our robust security program with supporting documentation.

Conclusion

Having regard to the level of risk of the data transfer (**limited risk**), NAVEX Global considers that the measures identified above are **sufficient and effective** in light of the circumstances of the transfers, in conjunction with the supplementary measures and safeguards provided by the SCCs, to allow the data importer to comply with its obligations under the SCCs and provide an appropriate level of protection for the transfer.

Lockpath US Hosted Sub-processing Activity: IPaaS Connector Services with Workato

NAVEX GLOBAL SUB-PROCESSING ACTIVITY

US HOSTED LOCKPATH SERVICES – WORKATO SERVICES

I. SCOPE

This TRA applies to NAVEX Global's US Hosted Lockpath customers. This TRA applies specifically to the services provided by Workato.

As part of NAVEX Global's Lockpath services, Workato provides software products and services relating to enterprise integration platforms to integrate and automate tasks across on-premise, cloud apps and databases.

Workato's capabilities and functions are more fully described at docs.workato.com and specifically include:

1. A low-code/no-code online editor for visually designing and editing integration processes ("recipes").
2. Connection facilities to a wide range of 3rd-party applications, systems and services.
3. The ability to execute recipes and thus enable data flow between applications.
4. Monitoring and management facilities including a history of jobs processed on the platform.
5. Management facilities for controlling user access and permissions.
6. The ability to embed Workato functionality within data exporter's own applications.

II. ASSESSING THE ADEQUACY OF EU/UK DATA TRANSFERS – WORKATO SERVICES

In assessing the adequacy of transfers of personal data from the EU/UK to NAVEX Global's sub-processor pursuant to the services provided by said sub-processor, we have taken the following steps:

1. **STEP 1:** Identified the relevant data transfers and the legal mechanism that NAVEX Global and sub-processor is relying on for such transfers (e.g., SCCs).

2. **STEP 2:** Conducted due diligence and collected information about the scope of the transfers, the exposure of the sub-processor to local law that may require disclosure of EU personal data about individuals, and any other relevant information.

3. **STEP 3:** Completed the "Transfer Risk Assessment" in **Section IV** to assess whether the SCCs is effective in light of all circumstances of the transfer.

4. **STEP 4:** Included additional "Supplementary Measures" as set forth in **Section IV (D)**.

5. **STEP 5:** Documented the assessment for accountability purposes. We encourage our customers to do the same.

6. **STEP 6:** NAVEX Global and its sub-processor is responsible for the periodic review of the assessment, which should take place at least annually, to ensure that the transfer of the EU personal data continues to be afforded an adequate level of protection.

III. TRANSFER RISK ASSESSMENT

Name Of Data Importer: Workato, Inc. **(**NAVEX Global's sub-processor)
Completed By: NAVEX Global's Privacy Team and Workato's Chief Information Security Officer
Date: 25 September 2021

A. Type of Data Importer

Name of data importer: Workato, Inc. ("Workato"). The Processor to Processor SCCs between NAVEX Global and Workato is part of a master services agreement between NAVEX Global and Workato.

Does Workato provide the following services to NAVEX Global:

	Data Importer	
Telecommunications	☐ Yes	☒ No
Other electronic communications (such as an Internet Service Provider or a provider of email, text message, VoIP, remote desktop or VPN services)?	☐ Yes	☒ No
Remote computing services	☒ Yes	☐ No
Other communications service where there may be access to wire or electronic communications	☐ Yes	☒ No

B. Details of Data Transfers

Data transfer mechanism

Appropriate Processor to Processor SCCs between Workato and NAVEX Global.

Scope of personal data covered by the data transfer mechanism in place

The SCCs cover transfers of EU personal data from the EEA/UK to the U.S., including the following categories of data subjects:

- Employees of customer Data Controller
- Clients, business partners and vendors of customer Data Controller (who are natural persons)
- Employees or contact persons of customer Data Controllers' third-party suppliers, business partners and vendors
- Customer Data Controller's users authorized to use the relevant Service(s)

C. Transfer Risk Assessment

The table below aids identification and evaluation of risk factors in relation to the specific data transfer. The assessment of each risk factor is recorded in appropriate detail.

#	Factor	Response
Scope of the transfers		
1.	What is the type of transfer?	Data is processed in accordance with the Data exporter's or controller's instructions, generally delivered via online configuration options and APIs provided to authorized users of the Data importer's platform.
2.	Is the transfer necessary?	Yes, in order to deliver the services requested by the customer Data Controller.
3.	Is the transfer proportionate?	Yes, data is transferred and processed solely for the specified service and in accordance with Processor's instructions.
4.	Is the transfer occasional/non-routine or frequent/routine?	This is dependent upon the customer Data Controller's use of the services and for the term of the commercial agreement between Navex and Workato.
5.	Will the transferred personal data be processed for a relatively long or short period of time?	Retention is limited and under NAVEX Global and Data Controller control: 30 days default.
6.	Is the transferred data encrypted, pseudonymized or otherwise processed in an unintelligible form, during all stages of the processing (i.e., in transit, in rest and while in use)?	Yes, All data is encrypted both in transit and at rest using industry-standard encryption technologies. In addition, the data importer provides as an option the ability to mask sensitive data from display and to restrict its retention on the platform. Display masking is applied automatically to certain data including passwords and keys.
Specific circumstances of the transfer		
7.	What are the purposes for which the data are transferred and processed?	Workato provides a flexible business integration and automation service. Data submitted by NAVEX Global's customers may be transferred onwards to one or more business applications or systems, under the control of NAVEX Global and Data Controller.
8.	What are the types of entities involved in the processing?	Workato is a data sub-processor and a private company. NAVEX Global is a data processor and private company. NAVEX Global's customers are the data controllers and may consist of both private and public companies.

#	Factor	Response
9.	In which sector does the transfer occur?	NAVEX Global provides risk and compliance management SaaS based software. ***This factor is especially important as the purposes of our services is to enable organizations support their risk, ethics, and compliance programs. ***
10.	What are the categories of personal data transferred?	• name, job title, job position, location, employer, relationship with the organization, e-mail address, telephone number; • Third party application data provided at the customer Data Controller's election depending on the Services' use case, as detailed in an agreement between Data exporter and the customer Data Controller • Other categories of data may be processed at the customer Data Controller's election depending on the Services' use case, as detailed in an agreement between Data exporter and the customer Data Controller • In the event customer Data controller whistle-blower hotline and incident management report data is processed, strictly as elected by the customer Data Controller, the following may also be captured: o facts reported by a reporter about a suspected violation, including how and where the suspected violation occurred and how the reporter learned about the suspected violation; o identity, function and contact details of individuals allegedly involved in the suspected violation; and o identity, function and contact details of individuals who could provide information relating to the suspected violation. Given the nature of incident management services, reporters may submit sensitive categories of data in a report. NAVEX Global recommends its customers have strict policies around the management of such report data in their use of the services, in accordance with the laws subject to them.
11.	What is the format of the personal data to be transferred?	Under the control of the customer Data Controller and may be in various formats.

#	Factor	Response
12.	What is the storage location of the data transferred?	The United States. Ultimately stored in NAVEX Global's secure data centres in the United States.
13.	What are the sub-sub-processing activities?	See https://www.workato.com/legal/sub-processors.
Importer's exposure to government surveillance and practical application of Section 702 FISA		
14.	Is the data importer's sector or business directly subject to such laws in its jurisdiction that permit government access to personal data, or require the assistance of data importer to disclose personal data to public authorities, for surveillance and intelligence gathering purposes?	No. Workato's business is currently not directly subject to such laws.
	a. Specifically, what is data importer's analysis regarding Section 702 FISA under the SCCs and EDPB Guidance?	1) Data exporters may decide to proceed with the transfer without supplementary measures, if they consider there to be no reason to believe that the relevant and problematic legislation (those in the U.S. in this instance) will be applied, in practice, to the transferred data and/or Workato. a. In our reasonable opinion upon internal and outside counsel review, we do not find U.S. surveillance laws, including Section 702 FISA, to practically apply to these transfers. b. It is important to note that given the broad definitions of these laws, the vast majority of organizations are going to have to acknowledge their potential application. However, this does not mean they directly apply or practically apply in practice. c. We believe Workato is generally out of scope and that these laws are overall not going to apply to the services we provide, as the intent is for surveillance of certain telecom and internet service providers for targeted information. This typically involves to surveillance of real time emails, texts, and chat conversations. The foregoing is not what Workato provides and in order to obtain this sought for information, authorities would pursue those providers directly as it would be impractical to make a request through Workato.

#	Factor	Response
		2) Data exporter may also take into consideration documented practical experience of data importer with relevant prior instances of requests for access received from public authorities in the U.S. a. To this point, Workato has never received a Section 702 FISA request or an EO 12.333 request or order. b. The EDPB Guidance implies that the lack of requests received in the past plus no prohibition on providing information about such requests, could be sufficient to conclude Section 702 FISA does not apply in practice. Note there is no prohibition on Workato to provide information about these requests. 3) If you conclude Section 702 FISA does not apply in practice to the particular transfer, it is possible to proceed with the transfer without any supplementary measures. While NAVEX Global and Workato take the approach that Section 702 FISA does not apply in practice, we still have elected to provide for supplementary measures with regard to these transfers. Please see Section IV (D).
15.	Within the last three (3) years, has the data importer received requests/demands from public authorities in its jurisdiction to disclose EU personal data?	Based on available information, Workato entities do not receive requests/demands for disclosure of, or access to, EU personal data in the US or elsewhere.
	a. Approximately how many requests/demands from public authorities has the data importer received in that time period concerning EU personal data?	None, to the best of our knowledge.
	b. Approximately how many of these requests/demands are pursuant to criminal law procedure in the destination country? *[Regular court proceedings are not the issue under Schrems II, but intelligence programs are scrutinized.]*	None, to the best of our knowledge.
	c. Approximately how many of these requests/demands are pursuant to national security or intelligence agencies in the destination country?	None, to the best of our knowledge. The data importer can represent that it has not received requests/demands from intelligence agencies.
	d. Has the data importer been able to contest/minimize such disclosure of EU personal data, where appropriate?	Not applicable

#	Factor	Response
	e. What types of EU personal data has the data importer been required to disclose to public authorities in its jurisdiction?	Not applicable
16.	How likely is it that the data importer will receive bulk data surveillance requests to disclose EU personal data to public authorities in its jurisdiction in the future (e.g., based on factors such as the type of services provided and sector in which the data importer operates, its size, number of customers and reputation)?	Unlikely. Workato is a SaaS provider. We are not in the types of businesses, such as telecommunication providers, which are commonly subject to such requests.
17.	Does the data importer maintain annual reports or statistics regarding requests/demands received from law enforcement or intelligence agencies (e.g., number/type of requests/demands, requesting authority, etc.)?	Workato maintains records but not annual statistics. Workato has not received any requests thus far. We anticipate that we'll receive them on rare occasions given the nature of our business.
18.	Does the data importer maintain a written procedure(s) for: 1. Responding to or challenging requests/ demands of law enforcement or intelligence agencies that apply to EU personal data? 22. Informing customers of requests/demands from law enforcement or intelligence agencies where permitted by applicable law?	Workato does not currently have a written policy because no requests have been received. We fully commit to evaluate such requests on a case by case basis in accordance with our agreements with NAVEX Global. Workato and NAVEX Global entered into a contractual agreement requiring Workato to cooperate and mutually agree on any appropriate actions, to notify NAVEX Globalof any requests unless explicitly required otherwise under applicable law, to put any access request on hold, and to use reasonable efforts to obtain the right to waive any notice prohibitions and oppose any such request and contest its legal validity where possible and permitted. The contract additionally ensures Workato will not make any disclosures that are determined to be massive, disproportionate, and indiscriminate in a manner that would go beyond what is necessary in a democratic society. Workato is obliged to document and demonstrate to the assessments made and the actions taken. Workato undertakes to regularly review, assess, and continuously monitor the scope of the access to personal data by public authorities in the countries where Workato is processing personal data, as well as the safeguards and recourses in place to protect data subjects, and to immediately inform NAVEX Global in the case of a change in applicable law that would materially impact such access by public authorities or recourses available to data subjects.
19.	Are the data importer's commitments enabling data subjects to exercise their rights as provided in the SCCs thwarted by the laws and/or practices in the U.S. and any other third countries involved, or can these rights	Workato does not believe that U.S. laws limit its ability to fulfill such requests.

#	Factor	Response
	be effectively applied in practice?	
Onward transfers and exposure to government surveillance		
20.	Does the data importer share EU personal data further with third-party data recipients in [the U.S./other jurisdiction]?	Yes. See https://www.workato.com/legal/sub-processors.
21.	What measures does the third-party data recipient take to ensure the protection of EU personal data transferred to it?	Where Workto engages sub-processors that have access to EU personal data, Workato enters into written agreements with sub-processors that include safeguards for EU personal data in accordance with the GDPR requirements.
22.	What assurances has the data importer received from third-party data recipients with respect to requests/demands for EU personal data from [U.S./other jurisdiction] public authorities?	Workato will update written agreements with sub-processors to include additional measures for the protection of EU personal data, where required by applicable law or regulation(s). Workato has current agreements in place with such sub-processors for the protection of EU personal data under applicable law.
23.	Is the vendor's (or its sub-processor's) sector or business directly subject to such laws in its jurisdiction that permit government access to personal data, or require the assistance of data importer to disclose personal data to public authorities, for surveillance and intelligence gathering purposes?	Generally no, but we may be considered a "remote computing service" under 18 U.S. Code § 2711 given the broad definition.

Conclusion/Risk of transfers

Very limited-risk data transfer

In particular, Workato and NAVEX Global identified the following factors (based on the assessment documented above and any additional information), that are likely to indicate a very limited-risk transfer:

The data importer has never received requests/demands from intelligence services for disclosure of EU personal data.

In the unlikely event that Workato receives such request(s), the Privacy team will review them with the Legal team and to seek counsel on how to respond and will coordinate the response with all stakeholders and the requesting legal authorities.

Based on the nature of its services and data processing activities, the data importer does not expect to be the target of requests/demands pursuant to national security or intelligence agencies for disclosure of EU personal data.

Such data transfers are not directly nor practically in scope of requests/demands from national security or intelligence agencies for disclosure of EU personal data.

D. Supplementary Measures

Notwithstanding the Conclusion set forth in the above TRA, Workato has also adopted the following supplemental measures. We believe that by implementing such supplemental measures, we are following best practices and are demonstrating our serious commitment to the protection of customer data.

Contractual safeguards	Workato and NAVEX Global have entered into supplementary contractual assurances as part of the data processing addendum.
	The SCCs themselves contain a number of contractual commitments by Workato and NAVEX Global, aimed at serving as safeguards for EU personal data. We have also entered into a robust general data processing addendum.
Organizational safeguards	Workato maintains written processes and procedures provide for review of and limit the scope of EU personal data disclosed by Workato in response to requests from public authorities.
	Workato maintains internal record of requests made by public authorities concerning EU personal data.
	Workato takes steps to limit the volume of disclosed data, where possible.
	Workato take data minimization measures such as redacting unnecessary identifiable personal data or personal data that may be of increased interest to intelligence agencies before complying with a request to disclosure EU personal data.
Technical safeguards	Encrypt personal data in transit.
	Encrypt personal data at rest.
	Appropriate access controls.
	Limit timespan for using personal data "in the clear" (i.e., in identifiable form).
	Mask stored personal data.
	Enable only remote access or view-only access.

Conclusion

Having regard to the level of risk of the data transfer (**very limited risk**), Workato and NAVEX Global consider that the measures identified above are **sufficient and effective** in light of the circumstances of the transfers, in

conjunction with the supplementary measures and safeguards provided by the SCCs, to allow the data importer to comply with its obligations under the SCCs and provide an appropriate level of protection for the transfer.

PUBLIC AUTHORITY DISCLOSURE REQUEST POLICY

Overview

NAVEX Global takes the privacy of our customers' data seriously, as it is a critical component of our business and our success as a leading provider in the governance, risk, and compliance marketplace. As part of our continued commitment to transparency, NAVEX Global has created this policy to help our customers understand how we respond to public authority requests for any customer data, or any direct access by public authorities to customer data.

This policy specifically applies to any public authority requests for, or public authority direct access to, personal data: (i) pursuant to (or transferred under) the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (the "SCCs"); (ii) pursuant to the General Data Protection Regulation ("GDPR"); (iii) pursuant to the Clarifying Lawful Overseas Use of Data Act ("CLOUD Act"); (iv) or pursuant to any other applicable legally binding requests or direct access by public authorities.

Disclosure Requests by Public Authorities

In theory, U.S. public authorities have broad statutory authority under the Foreign Intelligence Surveillance Act of 1978 ("FISA") or Executive Order 12333 of Dec. 4, 1981 (46 FR 59941, 3 CFR, 1981 Comp., p. 200) ("EO 12333") and other federal laws and orders to obtain information from U.S. companies, including NAVEX Global, for national security or foreign intelligence purposes. However, based on the nature of our services, the types of personal data we process, and our history of requests received in the past, we believe we are unlikely to receive requests from U.S. public agencies to obtain customer data for national security purposes or to participate in bulk surveillance programs**. To this point, NAVEX Global has never received a FISA, EO 12333, or CLOUD Act request.**

In recent years, NAVEX Global has received a limited number of formal requests for customer data from courts and agencies with investigatory authority. These requests have been made in the context of criminal investigations and civil actions and primarily by subpoena issued to NAVEX Global as a third party. In each instance, we review the requests for lawfulness and appropriate handling. Please note, NAVEX Global has never received a request for disclosure from a public authority specifically targeting personal data transferred pursuant to the SCCs from the European Economic Area (EEA).

NAVEX Global has processes in place to carefully review and promptly address requests it receives from public authorities, including subpoenas. All such requests are escalated internally to the NAVEX Global Legal Department for review. The NAVEX Global Legal Department, in consultation with outside counsel as appropriate, evaluates the request to determine its scope, NAVEX Global's responsibilities to respond and inform the relevant customer, and applicable nondisclosure restrictions. As appropriate, NAVEX Global will work with the relevant customer in taking steps to challenge the request.

Direct Access by Public Authorities

NAVEX Global will never voluntarily assist a public authority where applicable, specifically the US government in conducting any operations under EO 12333. NAVEX Global shall, where possible, take such measures as it, in its sole discretion, deems reasonable to prevent data from being intercepted in transmission.

NAVEX Global has not and will not intentionally create back doors, alternative means or similar programming for use by public authorities to access the system and/or personal data. NAVEX Global has not and will not purposefully create or change its business processes in a manner that facilitates access by public authorities to personal data or systems. NAVEX Global is not aware of any requirement under applicable national law or government policy requiring NAVEX Global to create or maintain back doors or to facilitate access to personal data or systems or for NAVEX Global to hand over the encryption key.

General Process for Notification

If NAVEX Global receives from a governmental or judicial body a lawful request for a customer's data, we will promptly contact the customer whose data is implicated and provide a copy of the request, if permitted under controlling law.

We will then use best efforts to refer the authority directly to the customer for the requested information. If we determine we remain under a legal obligation to act, we will ask if the customer's counsel plans to move to quash, seek a protective order, or otherwise challenge or modify the request. If the customer challenges the request, it is NAVEX Global's preference and practice to await resolution of such a challenge prior producing any data.*

While transparency is our number one objective, we may sometimes be compelled by law not to disclose the request. In such a scenario, we will use reasonable efforts to obtain a waiver of the prohibition in order to communicate as much information to the customer as is allowed. We will document these efforts, as well as any efforts to oppose any such request for access and contest its legal validity.

In any event, NAVEX Global will not make any disclosures of customer data to any law enforcement, national security or any other authority that are determined to be massive, disproportionate or indiscriminate in a manner that it would go beyond what is necessary under the law.

**Please note, NAVEX Global can never provide advice on how a customer should respond to a request for information and they should always consult their own attorney.*

Specific Notification Process for Personal Data Transferred Pursuant to the SCCs

(a) NAVEX Global will notify the customer and, where possible, the data subject promptly (if necessary with the help of the customer) if it:
   i. receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to the SCCs; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
   ii. becomes aware of any direct access within our hosting environment by public authorities to personal data transferred pursuant to the SCCs in accordance with the laws of the country of destination; such notification will include all information available to NAVEX Global.

(b) If we are prohibited from notifying our customer and/or the data subject under the laws of the country of destination, NAVEX Global will use best efforts to obtain a waiver of the prohibition and will communicate as much information to our customer as possible, as soon as possible. We will document these best efforts so that we can demonstrate them on customer request.

(c) NAVEX Global agrees to provide its customer, where permissible under the laws of the country of destination and at regular intervals for the duration of our agreement, with as much relevant information as possible on the requests we have received. Specifically, we have made available the number of requests, the type of data requested, the requesting authorities, whether the requests have been challenged and the outcome of such challenges.

We are committed to updating this information at regular intervals and agree to provide customers on request with as much relevant information as possible regarding our receipt of such requests.

(d) We agree to retain the information pursuant to paragraphs (a) to (c) above for at least the duration of our applicable agreements and will make it available to competent supervisory authorities on request.

(e) NAVEX Global agrees and understands that paragraphs (a) to (c) are without prejudice to our obligations under Clause 14 (e) and Clause 16 of the SCCs to inform our customers promptly in a situation where we are unable to comply with the SCCs.

Review of Legality and Data Minimization Specific to the SCCs

If NAVEX Global receives a public authority request for customer data pursuant to the SCCs, we will ensure our Legal Department has been engaged. Any request not directly received by the Legal Department is immediately sent to them and all individuals that need to know are notified. Our General Counsel, Senior Counsel, and Privacy Counsel review every request for disclosure to ensure that each is handled properly.

(a) NAVEX Global will review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. NAVEX Global will, under the same conditions, pursue possibilities of appeal. When challenging a request, NAVEX Global will seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules.

(b) NAVEX Global will document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination and subject to the preservation of privilege, make the documentation available to the customer. It shall also make it available to the competent supervisory authority on lawful request.

(c) NAVEX Global will only provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

General Policy for Producing Information

If we move forward with production, we begin by compiling and reviewing the data to ensure it is responsive to the request and to determine whether to withhold it from production based on any legal basis, including the attorney-client privilege and the work-product doctrine. Only those non-privileged documents that fall within the scope of the request will be produced. Once compiled, we will send all the responsive data to the customer for their review and approval. We will only use secure file-sharing methods to share data.

Once the customer has reviewed the data, we will confirm whether the customer is asserting a legal basis to withhold any data. Once confirmed, we will either send the responsive, non-privileged data to the requesting party, or wait until any challenge to the request made by the customer is resolved.

* * * * *

CONTACT US

Should you have any additional questions please contact; Jessica Wilburn, NAVEX Global Data Privacy Officer & Senior Counsel, CIPP/US, CIPP/E, CIPM. She is supported by our data privacy team which consists of CIPP/E certified Privacy Counsel. To contact our privacy team please e-mail privacy@navexglobal.com.