Data Protection Addendum

This Data Protection Addendum ("**DPA**") is entered into as of the date of the last signature below, ("**Effective Date**"), by and between the Customer ("***Customer***") and Nintex Global Ltd. and its Affiliates (collectively, "**Company**").

Last Updated: February 2, 2022

RECITALS:

(A) Company provides to Customer certain services (collectively, the "**Services**") pursuant to an agreement between the parties ("**Main Agreement**"). In connection with the Services, the parties anticipate that Company may process certain Personal Data on behalf of Customer.

(B) The parties agree to enter into this DPA in order to ensure that adequate safeguards are put in place with respect to the protection of such Personal Data as required by applicable Data Protection Laws.

1. Definitions and Initial Matters

1.1 The following definitions are used in this DPA:

(a) "**Adequate Country**" means a country or territory that is recognized under the GDPR as providing adequate protection for Personal Data;

(b) "**Affiliate**" means, with respect to a party, any corporate entity that, directly or indirectly, Controls, is Controlled by, or is under Common Control with such party (but only for so long as such Control exists);

(c) "**CCPA**" means the California Consumer Privacy Act of 2018 and any regulations promulgated thereunder, in each case, as amended from time to time;

(d) "**Company Group**" means Company and any of its Affiliates;

"**Controller**" means the entity which determines the purposes and means of the processing of Personal Data;

(e) "**Customer**" means the entity that executed the Main Agreement together with its Affiliates which have signed Order Forms and who, or a member of whose Customer Group, is a data controller of Personal Data under applicable Data Protection Laws;

(f) "**Customer Group**" means a Customer and any of its Affiliates;

(g) "**Data Protection Laws**" means all laws and regulations that apply to the processing of Personal Information and apply to Company or Customer, including the laws of the European Union, the European Economic Area and their member states, Switzerland, the United Kingdom and the United States and its states. For clarity, to the extent Company processes personal information covered by Data Protection Laws: (a) Company serves as a service provider to Customer with respect to the CCPA; and (b) Company serves as a Processor under the GDPR;

(h) "**Data Subject Request**" means a request from or on behalf of a data subject relating to access to, or rectification, erasure or data portability in respect of that person's

Personal Data or an objection from or on behalf of a data subject to the processing of its Personal Data;

(i) "**GDPR**" means, as and where applicable: (a) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation) (the "EU GDPR"); and/or (b) the EU GDPR as it forms part of UK law by virtue of the European Union (Withdrawal) Act 2018, as amended from time to time (the "UK GDPR");

(j) "**Standard Contractual Clauses or SCCs**" means, as and where applicable, the standard contractual clauses: (a) issued by the European Commission under the EU GDPR pursuant to implementing Decision (EU) 2021/914 ("EU SCCs") and set out at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj;and/or (b) the standard contractual clauses (processors) issued by the European Commission pursuant to implementing Decision (EU) 2010/87 ("UK SCCs");

(k) "**Personal Data**" means all data which is defined as '*personal data*' under Data Protection Laws and which is provided by Customer to Company (directly or indirectly), and accessed or otherwise processed by Company as a data processor as part of its provision of the Services to Customer and to which Data Protection Laws apply from time to time;

(l) "**Processo**r" means the entity which processes Personal Data on behalf of the Controller, including as applicable any "service provider" as that term is defined in the CCPA;

(m) "**Data subject**" means the identified or identifiable person to whom the Personal Data relates;

(n) "**Supervisory authority**" shall have the meaning ascribed to it in the GDPR; and

(k) **"Sub-processor"** means any entity engaged by the processor or any further sub-contractor to process Personal Data on behalf of and under the instructions of the controller.

1.2 An entity "**Controls**" another entity if it: (a) holds a majority of the voting rights in it; (b) is a member or shareholder of it and has the right to remove a majority of its board of directors or equivalent managing body; (c) is a member or shareholder of it and controls alone or pursuant to an agreement with other shareholders or members, a majority of the voting rights in it; or (d) has the right to exercise a dominant influence over it pursuant to its constitutional documents or pursuant to a contract; and two entities are treated as being in "**Common Control**" if either controls the other (directly or indirectly) or both are controlled (directly or indirectly) by the same entity.

1.3 Each party warrants in relation to Personal Data that it will comply (and will procure that any of its personnel comply and use commercially reasonable efforts to procure that its sub-processors comply), with Data Protection Laws. As between the parties, Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data.

1.4 Customer is responsible for obtaining all necessary consents, licenses, and approvals for the processing of personal data. Customer's instructions for the processing of Personal Data shall comply with applicable Data Protection Laws. In using the Service Customer shall process Personal Data according to the requirements of applicable Data Protection Laws, including any requirement to provide notice to Data Subjects of Customer's use of Company as a Processor.

1.5 In respect of the parties' rights and obligations under this DPA regarding the Personal Data, the parties hereby acknowledge and agree that Customer is the data controller and Company is the data processor, and accordingly Company agrees that it shall process all Personal Data in accordance with its obligations pursuant to this DPA.

1.6 The individual identified on the front page of this DPA is authorised to respond from time to time to enquiries regarding the Personal Data on behalf of that party and each party shall deal with such enquiries promptly. Each party shall notify the other of any change in the identity of the authorised person.

2. Company obligations

2.1 With respect to all Personal Data, Company shall:

(a) only process Personal Data in order to provide the Service, and shall act only in accordance with: (i) this DPA, (ii) Customer’s instructions as implemented by Customer’s configuration and use of the Service; and (iii) Customer's reasonable written instructions where the instructions are consistent with the Main Agreement;

(b) as soon as reasonably practicable upon becoming aware, inform Customer if, in Company's opinion, any instructions provided by Customer under clause 2.1(a) infringe the GDPR;

(c) implement appropriate technical and organizational measures to ensure a level of security appropriate to the risks that are presented by the processing of Personal Data, in particular protection against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data. Such measures include, without limitation, the security measures set out in Exhibit B;

(d) take reasonable steps to ensure that only authorized personnel have access to such Personal Data and that any persons whom it authorizes to have access to the Personal Data are under obligations of confidentiality;

(e) as soon as reasonably practicable upon becoming aware, notify Customer of any actual incident of unauthorized or accidental disclosure of or access to any Personal Data (a "**Security Breach**"), and take reasonable steps to remediate the Security Breach to the extent that remediation is reasonably within Company’s control;

(f) promptly provide Customer with reasonable cooperation and assistance in respect of a Security Breach and all reasonable information in Company's possession concerning such Security Breach insofar as it affects Customer and/or any member of a Customer Group;

(g) not make any public announcement about a Security Breach without the prior written consent of Customer, unless required by applicable law;

(h) promptly notify Customer if Company receives a Data Subject Request. Company shall not respond to a Data Subject Request without Customer's prior written consent except to confirm that such request relates to Company. Upon Customer's request, Company shall provide reasonable assistance to Customer to facilitate Customer responding to a Data Subject Request within the deadlines set out under applicable Data Protection Laws;

(i) other than to the extent required to comply with applicable law, as soon as reasonably practicable following termination or expiry of the Main Agreement or completion of the Service, Company will delete all Personal Data (including copies thereof) processed pursuant to this DPA;

(j) provide such assistance to Customer as Customer requests in relation to Customer's obligations under applicable Data Protection Laws with respect to:

(i) data protection impact assessments (as such term is defined in the GDPR);

(ii) notifications to the supervisory authority or relevant authorities under the GDPR and applicable Data Protection Laws and/or communications to data subjects by Customer in response to any Security Breach; and

(iii) Customer's compliance with its obligations under the applicable Data Protection Laws with respect to the security of processing.

3. Sub-processing

3.1 Customer grants a general authorization: (a) to Company to appoint other members of the Company Group as sub-processors, and (b) to Company and other members of the Company Group to appoint sub-processors in respect of the sub-processing activities in accordance with this section. Company has entered into a written agreement with each sub-processor containing data protection obligations not less protective than those imposed on the Company in this DPA. Where a sub-processor fails to fulfil its duty Company will be liable for the acts and omissions of its sub-processors to the same extent Company would be liable if performing the services of each sub-processor directly under the terms of this DPA, except as otherwise set forth in the Main Agreement.

3.2 Company will maintain a list of sub-processors, if any, and will add the names of new and replacement sub-processors to the list prior to them starting sub-processing of Personal Data.

3.3 If Customer has a reasonable objection to any new or replacement sub-processor, it shall notify Company of such objections in writing within ten (10) days of the notification and the parties will seek to resolve the matter in good faith. Company may choose to: (i) not use the sub-processor or (ii) take the corrective steps requested by Customer in its objection to the use of the sub-processor. If none of these options are reasonably possible within thirty (30) days, and Customer continues to object for a legitimate reason, then either party may terminate the applicable services or the Main Agreement. If Customer does not provide an objection within ten (10) days, Customer will be deemed to have consented to the sub-processor and waived its right to object.

4. Audit

4.1 **Audits and Records**. Company shall, in accordance with applicable Data Protection Laws make available to Customer such information in Company's possession or control, if any, and provide all assistance in connection with audits of Company's premises, systems and documentation as Customer may reasonably request with a view to demonstrating Company's compliance with the obligations of data processors under applicable Data Protection Law in relation to its processing of Personal Data. For Services that undergo an external audit or certification, then Company shall provide to Customer a copy of the relevant and most recent third-party audit reports or certifications (provided an applicable confidentiality obligation is in place); for Services that are not audited by third-party then such other written documentation as is generally provided by Company; and other additional information in Company's possession or control specifically requested or required by the Supervisory Authority to demonstrate compliance with this DPA.

4.2 **On Site Audit**. If an on-site audit is required, Customer will give Company written notice of at least thirty (30) days of any audit or inspection and must be subject to reasonable confidentiality procedures. The frequency, time frame and scope of any audit will be mutually agreed upon between the parties acting reasonably and in good faith, including the selection of any third-party auditor. Customer will notify Company of any non-conformance discovered during the audit. If an on-site audit is mandatory it shall be conducted in such a manner as not to unreasonably interfere with Company's business operations.

5. Data transfers

5.1 This Section 5 applies to any processing of Personal Data that is subject to the GDPR. Customer acknowledges and accepts that the provision of the Services under the Main Agreement may require the processing of Personal Data by Company or sub-processors in countries outside the EEA.

5.2 For Personal Data that is subject to the GDPR, to the extent any processing of Personal Data by Company takes place in any country outside the EEA or the United Kingdom that is not recognized as an Adequate Country, the parties agree that the Standard Contractual Clauses will apply in respect of that transfer and processing, and Company will comply with the obligations of the 'data importer' in the standard contractual clauses and Customer will comply with the obligations of the 'data exporter'.

5.3 If, in the performance of this DPA and/or the Main Agreement, Company transfers any Personal Data to a sub-processor located, or permits processing of any Personal Data by a sub-processor in a country outside of the EEA, other than to an Adequate Country, (without prejudice to clause 3), Company shall in advance of any such transfer ensure that a legal mechanism to achieve adequacy in respect of that processing is in place, such as:

(a) the requirement for Company to execute or procure that the sub-processor execute the Customer's Standard Contractual Clauses; or

(b) the existence of any other specifically approved safeguard for data transfers (as recognized under the GDPR) and/or a finding of adequacy under the GDPR.

5.4 To the extent consistent with the Standard Contractual Clauses, the following term shall apply to the Standard Contractual Clauses:

Company may appoint sub-processors as set out, and subject to the requirements of, clauses 3 and 5.3 of this DPA.

6. CCPA Provisions

6.1 This Section 7 applies to any processing of Personal Data that is subject to the CCPA. Company agrees that:

6.1.1. Company will not retain, use, or disclose such Personal Data except as permitted in the Main Agreement and under the CCPA; and

6.1.2. Company will not sell Personal Data.

7. General

7.1 This DPA is without prejudice to the rights and obligations of the parties under the Main Agreement, which shall continue to have full force and effect. In the event of any conflict between the terms of this DPA and the terms of the Main Agreement, the terms of this DPA shall prevail so far as the subject matter concerns the processing of Personal Data.

7.2 Without prejudice to clause 17 (Governing Law) and clause 18 (Forum and Jurisdiction) of the EU SCCs and without prejudice to clause 7 (Mediation and Jurisdiction) and 9 (Governing Law) of the UK SCCs , this DPA shall be governed by and construed in accordance with the laws of the country of territory stipulated for this purpose in the Main Agreement and each of the parties agrees to submit to the choice of jurisdiction as stipulated in the Main Agreement in respect of any claim or matter arising under this DPA.

7.3 This DPA is the final, complete and exclusive agreement of the parties with respect to the subject matter hereof and supersedes and merges all prior discussions and agreements between the parties with respect to such subject matter. Other than in respect of statements made fraudulently, no other representations or terms shall apply or form part of this DPA. No modification of, amendment to, or waiver of any rights under the DPA will be effective unless in writing and signed by an authorized signatory of each party. This DPA may be executed in counterparts, each of which shall be deemed to be an original, but all of which, taken together, shall constitute one and the same agreement. Each person signing below represents and warrants that he or she is duly authorized and has legal capacity to execute and deliver this DPA. Each party represents and warrants to the other that the execution and delivery of this DPA, and the performance of such party's obligations hereunder, have been duly authorized and that this DPA is a valid and legally binding agreement on each such party, enforceable in accordance with its terms.

IN WITNESS WHEREOF, the parties have each caused this DPA to be signed and delivered by its duly authorized representative.

[Nintex]

……………………………….

Name:

Title:

[Customer]

……………………………….

Name:

Title:

EXHIBIT A

A. LIST OF PARTIES

Data exporter(s): *Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union*

Name: Customer as provided in the DPA
Address: As described in the DPA
Contact person's name, position and contact details: As described in the DPA

Activities relevant to the data transferred under these Clauses: The provision of the Services to Customer pursuant to the Main Agreement and applicable documentation.

Signature and date:

Role (controller/processor): With respect to Module 2 of the 2021 Standard Contractual Clauses, Customer is the Controller. With respect to Module 3 of the 2021 Standard Contractual Clauses, Customer is a Processor.

Data importer(s): *Identity and contact details of the data importer(s), including any contact person with responsibility for data protection*

Name: Nintex Global Ltd.
Address: 10800 NE 8th St., Suite 400, Bellevue, WA 98004 USA
Contact person's name, position and contact details: Chief Legal Officer, GDPR@nintex.com

Activities relevant to the data transferred under these Clauses: The provision of the Services to Customer pursuant to the Main Agreement and applicable documentation.

Signature and date:

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

1. Categories of data subjects whose personal data is transferred

The data exporter may submit Personal Data to the Services, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

- Employees
- Contractors
- Business Partners
- Other Individuals

2. Categories of personal data transferred

The data exporter may submit Personal Data to the Services, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to:

- Name
- Title
- Position
- Employer
- Phone Number
- Email
- Time Zone
- ID data
- System Access
- Professional Life Data
- Connection Data
- Localization Data

3. Sensitive data transferred (if applicable)

*Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures***.**

The Nintex Process Platform provides business process automation software, and the transfer and processing of sensitive personal data is not intended or required.

Any sensitive data that is submitted to the Services is determined and controlled by the data exporter in its sole discretion, and which is for the sake of clarity Personal Data with information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

4. The frequency of the transfer

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Continuous.

5. Nature of the processing

The collection, analysis, storage, duplication, compute, deletion and disclosure as necessary to provide the Services and as may be further instructed by Company in writing.

6. Purpose(s) of the data transfer and further processing

The objective of the processing is the performance of the Services under the Main Agreement, and as may be further instructed by the Company.

7. Duration

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Nintex will process the Personal Data as described in the Main Agreement, or until the data upon which processing is performed is no longer necessary for the purposes of either party performing its obligations under the Main Agreement (to the extent applicable), unless otherwise agreed between the parties in writing.

8. Sub-processor transfers

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

Details of the sub-processors are available at https://www.nintex.com/legal

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

1. Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer shall act as competent supervisory authority.

2. Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established shall act as competent supervisory authority.

3. Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: Ireland.

EXHIBIT B

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Data importer will maintain administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Personal Data processed by the Services, as described in the Nintex Global Product Sheet, or other applicable documentation made reasonably available by the data importer. Data Importer will not materially decrease the overall security of the Services during a subscription term.

EXHIBIT C

STANDARD CONTRACTUAL CLAUSES

SECTION I
Clause 1
Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)[1] for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2
Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3
Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

(ii) Clause 8 – Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 9 – Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 – Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 – Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4
Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5
Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6
Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7

[Intentionally omitted]

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8
Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

MODULE TWO: Transfer Controller to Processor

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement 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 (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of 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. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point 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. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves 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 (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[2] (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, 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. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

[2] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

Clause 9
Use of sub-processors
MODULE TWO: Transfer controller to processor

(a) The data importer has the data exporter’s general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least thirty (30) days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.[3] The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter’s request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor’s obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10
Data subject rights
MODULE TWO: Transfer controller to processor

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects’ requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II 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 the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11
Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to

[3] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

handle complaints. It shall deal promptly with any complaints it receives from a data subject.

MODULE TWO: Transfer controller to processor

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12
Liability

MODULE TWO: Transfer controller to processor

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer’s responsibility for the damage.

(e) Where 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 an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13
Supervision

MODULE TWO: Transfer controller to processor

(a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] 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 goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer 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. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

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

Clause 14

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This 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 in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(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 in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;[4]

[4] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include 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. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), 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).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

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

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) 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 these Clauses; 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 by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to 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. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall 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. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to 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, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16
Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17
Governing law

MODULE TWO: Transfer controller to processor

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

Clause 18
Choice of forum and jurisdiction

MODULE TWO: Transfer controller to processor

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Ireland.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

ANNEX I

DESCRIPTION OF THE PROCESSING
See Exhibit A to the DPA

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA
See Exhibit B to the DPA

ANNEX III

LIST OF SUB-PROCESSORS
Either provided independently or available at: https://www.nintex.com/legal