Data Protection Addendum

This Data Protection Addendum ("DPA") is supplemental to, and forms part of, Nintex's Master Subscription Agreement, currently located at https://www.nintex.com/legal/. However, if Customer has entered into some other written agreement with Nintex ("**Company**"), then this DPA forms part of such written agreement (in either case, the "**Main Agreement**"). Unless otherwise defined in this DPA or in the Main Agreement, all capitalized terms used in this DPA will have the meanings given to them in Section 1 of this DPA.

1. Definitions

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

1.2 "**CCPA**" means the California Consumer Privacy Act of 2008, Cal. Civ. Code § 1798.100 *et seq*., as amended by the California Privacy Rights Act, and its implementing regulations;

1.3 "**Company Group**" means Company and any of its Affiliates;

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

1.5 "**Customer**" means the entity that executed the Main Agreement or is listed on the Order Form;

1.6 "**Customer Content**" means what is defined in the Main Agreement as "Customer Content" provided that such data is electronic data and is submitted by, or on behalf of, the Customer to the Service for processing;

1.7 "**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 Processor under the GDPR; and (b) Company serves as a service provider to Customer with respect to the CCPA;

1.8 "**Data Subject**" means the identified or identifiable person to whom Personal Data relates;

1.9 "**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;

1.10 "**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");

1.11 "**Personal Data**" means all data which is defined as '*personal data*' under Data Protection Laws and which is provided by Customer to Company for processing by Company as a data processor as part of its provision of the Service to Customer and to which Data Protection Laws apply from time to time. For the sake of clarity, Customer's business contact information is not by itself deemed to be Personal Data;

1.12 "**Processor**" 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;

1.13 "**Security Incident**" means a breach of Company's security leading to the leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data while being stored or processed by Company;

1.14 "**Standard Contractual Clauses or SCCs**" means (i) the standard contractual clauses: 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;

1.15 "**Supervisory authority**" shall have the meaning ascribed to it in the GDPR;

1.16 **"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;

1.17 **"Swiss FADP"** means the Swiss Federal Act on Data Protection and its implementing regulations as amended, superseded, or replaced from time to time; and

1.18 **"UK Addendum"** means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner, Version B1.0, in force 21 March 2022, as amended, superseded or replaced from time to time.

2. Personal Data Processing

2.1 **Roles**. In respect of the parties' rights and obligations under this DPA regarding the Personal Data, the Customer is the data controller or processor as the case may be, and Company is acting on behalf of the Customer as the data processor. For the avoidance of doubt, to the extent Processing of Personal Data is subject to the CCPA, the parties agree that Customer is the "Business" and Company is the "Service Provider" (as those terms are defined by the CCPA).

2.2 **Details**. The subject-matter of Processing of Personal Data by Company is the performance of the Service pursuant to the Main Agreement. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Exhibit to this DPA.

2.3 **Customer's Processing of Personal Data**. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data. 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.

2.4 **Company's Processing of Personal Data**. In the course of providing the Service, 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) Company will as soon as reasonably practicable upon becoming aware, inform Customer if, in Company's opinion, any instructions provided by Customer infringe the GDPR or other applicable Data Protection Law; and

(c) 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.

2.5 **Business Contact Information**. Company and Customer may process the other's "Business Contact Information" (personal data used to identify or contact an individual in a professional or business capacity, including an individual's name, business e-mail address, physical address, telephone number or like data) as independent Controllers wherever they do business to deliver and receive the Service. The parties are not entering a joint Controller relationship. The Nintex Privacy Statement (available at: https://www.nintex.com/legal/privacy-policy/) provides details on Company's Processing of Business Contact Information. Each of the parties has implemented and follows appropriate technical and organizational measures to protect the other's Business Contact Information.

3. Security of the Processing

Company has implemented and will maintain appropriate technical and organizational measures designed to protect the security, confidentiality, integrity and availability of Customer Data and protect against Security Incidents. Customer is responsible for configuring the Service and using features and functionalities made available by Company to maintain appropriate security in light of the nature of Customer Data.

Company's current technical and organizational measures are described in Exhibit B. Customer acknowledges that the security measures are subject to technical progress and development and that Company may update or modify the security measures from time to time, provided that such updates and modifications do not materially decrease the overall security of the Service during a subscription term.

4. Data Subject Requests

Company shall, to the extent legally permitted, promptly notify Customer if Company receives a Data Subject Request; and Company shall not respond to a Data Subject Request without Customer's prior written consent except to confirm that such request relates to Company.

To the extent it is legally required, and to the extent that the Customer, in its use of the Service, does not have the ability to address a Data Subject Request, upon Customer's request Company shall provide commercially reasonable assistance to Customer in responding to such Data Subject Request within the deadline set by the applicable Data Protection Law.

5. Third Party Access Requests

Company will not access or use, or disclose to any third party, any Personal Data, except, in each case, as necessary to maintain or provide the Service. In the event Company receives an order from any third party for compelled disclosure of any Personal Data processed under this DPA, Company will: (a) redirect the third party to request data directly from Customer; (b) promptly notify Customer, unless prohibited under applicable law, and, if prohibited from notifying Customer, use commercially reasonable efforts to obtain the right to waive the prohibition in order to communicate as much information to Customer as soon as possible; and (c) challenge the order for disclosure on the basis of any legal deficiencies under the laws of the requesting party or any relevant conflicts with applicable law. Company will not disclose the Personal Data requested until required to do so under the applicable procedural rules, and Company agrees it will provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request. For the avoidance of doubt, this DPA shall not require Company to pursue action or inaction that could result in civil or criminal penalty for Company such as contempt of court.

6. Return, Retention, and Deletion of Data

Where applicable and depending on the specific Service, at any time up leading up to termination of the Service, Customer may at its sole discretion and expense, delete or retrieve Customer Content, including any Personal Data contained therein, from the Service as provided in the Main Agreement. As soon as reasonably practicable following termination or expiry of the Main Agreement or completion of the Service, or upon Customer request, will delete all Personal Data (including copies thereof) processed pursuant to this DPA.

Company may retain Customer Personal Data: (i) as required under applicable law; or in accordance with its standard backup or record retention policies, provided that, in either case, until Customer Content is deleted or returned, Company shall continue to comply with this DPA and its schedules.

7. Sub-processing

7.1 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, and when required under applicable Data Protection Law, 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.

7.2 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. Customer hereby consents to these Sub-processors, their locations and processing activities as it pertains to their Personal Data.

7.3 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.

8. Audit

8.1 **Audit Reports**. Company has obtained the third-party certifications and audits set forth in the in the Nintex Platform Security, Privacy and Organizational Overview or other such documentation as Nintex may make available from time to time for each applicable Service; these third-party certifications and audits are also described on the Nintex Security website, https://www.nintex.com/security/ . These audits are performed annually and result in the generation of an audit report ("Audit Report"). At Customer's written request, and provided that the parties have an applicable NDA in place, Company will provide Customer with a copy of the Audit Report so that Customer can reasonably verify Company's compliance with its obligations under this DPA.

8.2 **Data Protection Impact Assessment.** Upon Customer's request, Company shall provide Customer with reasonable cooperation and assistance needed to fulfill Customer's

obligation under Data Protection Laws and Regulations to carry out a data protection impact assessment related to Customer's use of the Service, to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to Company.

8.3 **Onsite Audit.** To the extent Customer's audit requirements under Data Protection Laws, including the Standard Contractual Clauses, cannot reasonably be satisfied through the Audit Report, documentation or compliance information that Company makes available to its customers, and when required under applicable law Customer can request an On-Site Audit. Any On-Site Audits will be limited to Customer Content processing and storage facilities operated by Company or any of Company's Affiliates The timing, duration, scope, evidence requirements, and reimbursement rate for which Customer is responsible 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 , during regular business hours, with reasonable advance notice, of at least 30 days, to Company, and subject to reasonable confidentiality procedures. Neither Customer nor the auditor shall have access to any data from Company's other customers or to Company systems or facilities not involved in providing the applicable Service. Customer is responsible for all costs and fees related to such audit, including all reasonable costs and fees for any and all time Company expends for any such audit, in addition to the rates for services performed by Company. Customer must promptly provide Company with information regarding any non-compliance discovered during the course of an On-Site Audit.

9. Security Incident

9.1 **Security Incident**. Company maintains security incident management policies and procedures, and will notify Customer without undue delay and, where feasible, no later than seventy-two (72) hours after becoming aware of a Security Incident. Company will make reasonable efforts to identify the cause of the Security Incident, mitigate the effects and remediate the cause to the extent within Company's reasonable control. Upon Customer's request and taking into account the nature of the Processing and the information available to Company, Company will assist Customer by providing information reasonably necessary for Customer to meet its Security Incident notification obligations under applicable Data Protection Law. Company's notification of a Security Incident is not an acknowledgment by Company of its fault or liability.

Unsuccessful Security Incidents. Notwithstanding the foregoing, the Customer and Company acknowledge the ongoing existence and occurrence of inconsequential incidents that occur on a daily basis, such as scans, "pings," or other unsuccessful attempts to penetrate computer networks or servers containing Personal Data managed by Company, and the parties agree that no further notification by Company of such unsuccessful Security Incidents is required.

10. Data Transfers - Europe

10.1 If, in the performance of this DPA and/or the Main Agreement, Company transfers any Personal Data, either directly or via onward transfer, to a country outside of the EEA or the United Kingdom that is not subject to an adequacy decision, the transfer mechanisms listed below shall apply:

(a) the Company has executed the Standard Contractual Clauses, and if applicable will 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, such as the Data Privacy Framework).

10.2 **Standard Contractual Clauses**. Where, for purposes of the GDPR, Standard Contractual Clauses are the transfer mechanism, the Standard Contractual Clauses are incorporated by reference as follows:

(a) Customer is the "data exporter" and Company is the "data importer;

(b) Where Customer is a Controller and a data exporter, Module 2, Controller to Processor clauses, as provided in Exhibit C, will apply;

(c) Where Customer is a Processor acting on behalf of a Controller and Company is a Processor, Module 3, Processor to Processor clauses, as provided in Exhibit C, will apply;

(d) The information required for the applicable Annexes is located in the Appendix;

(e) 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 7 and 10.1 of this DPA correct; and

(f) By entering into this DPA, each party is deemed to have signed the Standard Contractual Clauses as of the commencement date of the Main Agreement.

10.3 **Swiss Transfers**. Where Personal Data protected by the Swiss FADP is transferred, either directly or via onward transfer, to any other country that is not subject to an adequacy decision, the EU SCCs apply as stated in in Section 1.2 (European Transfers) above with the following modifications:

(a) All references in the EU SCCs to "Regulation (EU) 2016/679" will be interpreted as references to the Swiss FADP, and references to specific Articles of "Regulation (EU) 2016/679" will be replaced with the equivalent article or section of the Swiss FADP; all references to the EU Data Protection Law in this DPA will be interpreted as references to the FADP.

(b) In Clause 13, the competent supervisory authority is the Swiss Federal Data Protection and Information Commissioner.

(c) In Clause 17, the EU SCCs are governed by the laws of Switzerland.

(d) In Clause 18(b), disputes will be resolved before the courts of Switzerland.

(e) All references to Member State will be interpreted to include Switzerland and Data Subjects in Switzerland are not excluded from enforcing their rights in their place of habitual residence in accordance with Clause 18(c).

10.4 **United Kingdom Transfers**. Where Personal Data protected by the UK GDPR is transferred, either directly or via onward transfer, to a country outside of the United Kingdom that is not subject to an adequacy decision, the following applies:

(a) The Standard Contractual Clauses apply as set forth in Section 10. (Data Transfers) above with the following modifications:

(i) Each party shall be deemed to have signed the UK Addendum.

(ii) For Table 1 of the UK Addendum, the parties' key contact information is located in the Main Agreement and/or relevant Order Form.

(iii) For Table 2 of the UK Addendum, the versions of the SCCs to which the UK Addendum applies are Modules Two and Module Three and as described above in 10.2 above.

(iv) For Table 3 of the UK Addendum:

(A) The information required for Annex 1A is located in the Main Agreement and/or relevant Orders.

(B) The Information required for Annex 1B is located in Section B of Exhibit A (Description of Transfer) of this DPA.

(C) The information required for Annex II is located Exhibit B.

(D) The information required for Annex III is located in Section 4 (Sub-processing) of this DPA.

(b) In Table 4 of the UK Addendum, both the data importer and data exporter may end the UK Addendum.

11. General

11.1 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.

11.2 Without prejudice to clause 17 (Governing Law) and clause 18 (Forum and Jurisdiction) of the Standard Contractual Clauses and without prejudice to clause 7 (Mediation and Jurisdiction) and 9 (Governing Law) of the UK Addendum, 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.

11.3 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] **[Customer]**

……	……..
Name:	Name:
Title:	Title:

CCPA Addendum

This CCPA Addendum ("CCPA Addendum") supplements the Main Agreement available at https://www.nintex.com/legal/ or other agreement between Customer and the Company governing the use of the Service (the "Main Agreement") when the California Consumer Privacy Act of 2018 as amended, including as amended by the California Privacy Rights Act of 2020, together with any implementing regulations (collectively the "CCPA") applies to Customer's use of the Service to process personal information.

For purposes of this CCPA Addendum, "commercial purpose," "personal information," "process," "sell," and "share" shall have the meaning ascribed to them in the CCPA. Unless otherwise defined in this CCPA Addendum, all capitalized terms will have the meanings given to them in the Main Agreement.

Company agrees that Company will: (a) process Personal Information pursuant to the Main Agreement for the purposes specified in Section B of Exhibit A of the DPA; (b) not retain, use, or disclose Personal Information for any purpose, including any commercial purpose, except as permitted in the Main Agreement or under the CCPA; (c) not retain, use, or disclose Personal Information outside the direct business relationship between Company and Customer, including by not combining any Personal Data with other personal information collected or received from another source, except as permitted by CCPA; and (d) not sell or share Personal Information. Company will notify Customer if it determines that Company can no longer meet its obligations under the CCPA. If Company is engaged in unauthorized use of Personal Information, Customer may, upon reasonable notice to Company, take reasonable and appropriate steps to stop and remediate the unauthorized use of Personal Information.

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 Service to Customer pursuant to the Main Agreement and applicable documentation.

Signature and date:

Role (controller/processor): With respect to Module 2 of the Standard Contractual Clauses, Customer is the Controller. With respect to Module 3 of the 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
Address: 411 106th Ave., Suite 600, 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 Service 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 Service, 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 Service, 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 Service 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 Service and as may be further instructed by Customer in writing.

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

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

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 either provided independently, in this DPA or 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.

Nintex maintains an Information Security Program and Information Security Team that is responsible for the security of the Nintex Process Platform, including the confidentiality, availability and integrity of the processed data. The technical and organizational measures described here apply to the Nintex Process Platform. As security threats change, Nintex continues to update its security program and strategy to protect the Nintex Process Platform. The Information Security Program at a minimum includes the technical and organizational measures described below.

1. **Audits and Certifications**: the Nintex Process Platform maintains the following audits and certifications:
    a. SOC2: Nintex Automation Cloud, Nintex DocGen, Nintex eSign, Nintex K2 Cloud, Nintex Process Discovery, Nintex Process Manager, Nintex RPA, Nintex Skuid.
    b. ISO 27001: Nintex K2 Cloud, Nintex Process Discovery and Nintex RPA.
    c. PCI SAQ: Nintex eSign.
    d. HITRUST: Nintex Skuid.
2. **Access Control**. Nintex has an Access Management Policy that outlines security practices to prevent unauthorized access to Nintex corporate systems and the Nintex Process Platform. The Access Policy and related guidelines and practices define the rules necessary to achieve this protection, and to ensure a secure and reliable operation, and include:
    a. Unique credentials to access Nintex systems;
    b. User provisioning for the access to Nintex systems, applications and infrastructure based on the relevant job role and on the least privilege principle that is enforced through the authentication processes;
    c. Quarterly review of privileged users; and where necessary, revocation of access privileges in a timely manner;
    d. For Nintex cloud based services: Privileged access to the production environment is restricted to privileged accounts used solely for the purpose of monitoring and maintaining the production environment. Each person's privileged account is held separately from their primary domain account and for additional security multifactor authentication is also required to log into the platform.
    e. Nintex maintains a corporate Password Policy with the following requirements: (i) minimum length of 8 characters; (ii) complexity enabled; and (iii) expires every 90 days. Privileged passwords must meet higher requirements.
3. **Confidentiality**. All Nintex employees are bound by Nintex's internal policies and procedures regarding maintaining the confidentiality of customer data and are contractually obligated to comply with these obligations.
4. **Encryption**. Nintex has Cryptography Guidelines that provide a framework for the proper use of cryptography in Nintex Process Platform capabilities, as well as guidance for software development where there may be a choice of available implementation functions such as transport layer security, symmetric and asymmetric algorithms, and hash function requirements. Nintex encryption requirements include:

a. **Encryption of data in transit.** Data is encrypted when in transit between Customer's software application and the Nintex Process Platform using TLS; and
b. **Encryption of data at rest**. Data at rest is encrypted using industry-accepted encryption.

5. **Hosting Architecture and Data Segregation**.
    a. **Hosting Providers**. The Nintex Process Platform utilizes Microsoft Azure and Amazon Web Services (AWS) to host its cloud-based capabilities. Security is a shared responsibility between Nintex and its hosting providers Microsoft Azure and AWS. Microsoft Azure and AWS are responsible for the security of its platform, including middleware, the servers and physical security within its data centers.
    b. **Multi-tenant**. The services that make up the Nintex Process Platform are operated in a multitenant architecture. The architecture provides a logical data separation for each different customer via a unique ID.
6. **Change Management**. Nintex has Enterprise Change Management guidelines that provide direction and support for performing consistent production level changes, including for routine, scheduled, and emergency changes. The guidelines cover the planning stages, approval or rejection of the change, and implementing the change, and with any rollbacks. Changes are reviewed and evaluated in a test environment before being deployed into the production environment.
7. **Testing and Vulnerability Assessments**. Nintex has Vulnerability Management Guidelines that outline the security requirements to perform regular external vulnerability assessments and testing of the Nintex Process Platform, identifying issues and tracking them to resolution in line with Nintex internal remediation timeframes. The vulnerability management program includes:
    a. **Static scanning**. Static vulnerability scans performed via a third party tool prior to each release to check for vulnerabilities such as those found in the OWASP top 10.
    b. **Infrastructure scanning.** Nintex conducts vulnerability scans via a third party tool to regularly assess vulnerabilities in Nintex's cloud infrastructure and corporate systems.
    c. **Penetration testing**. All Nintex cloud based products undergo third party penetration tests on an annual basis.
8. **Logging and Monitoring**. Nintex maintains policies and procedures for monitoring of certain security events related to its SaaS product infrastructure and information systems, such as privileged user logins. Nintex collects and consolidates security relevant logs and data from the corporate environment and its cloud services using a Security Information and Event Management System (SIEM).
9. **Security Training**. Nintex provides mandatory annual security and privacy awareness training annually and at time of hiring. This provides employees the knowledge and tools that maintain the safety and integrity of the Nintex IT infrastructure, cloud-based capabilities, data network, intellectual property and physical locations. Nintex tracks who has completed the training and provides testing at the end of each module. All Nintex developers are also required to participate in additional annual interactive web-based Cybersecurity training for software engineers to maintain and enhance their skills in writing secure code.
10. **Security Incident Management.** Nintex has a Security Incident Response Policy and a formal Security Incident Response Plan that establishes a standard operating procedure for the incident response process during a security event. The Security Response Plan governs the notification process of the security incidents to the customers. The Nintex Incident Response Team communicates the Security Incidents involving customer information or information systems within 72 hours of the incident. Nintex also provides an externally facing status page to customers: http://status.nintex.com. This site provides a history of incidents, which includes timelines.
11. **Business Continuity and Disaster Recovery**. Nintex has an overarching Business Continuity Management (BCM) Plan for internal enterprise operations. The plan

establishes the Nintex BCM function and outlines requirements for the response to, and recovery of, all critical business processes in the event of an unplanned business disruption to any portion of Nintex's normal operations.

12. **Physical Security**. Nintex maintains a comprehensive set of policies, controls, and practices for the physical and environmental protection of the processed data, which include:
    a. **Offices**. Nintex offices are located in fit for purpose buildings with building access via key card only. Visitors must sign in and sign out and are accompanied by an employee when onsite. No customer data is hosted within Nintex offices.
    b. **Data Centers**. The Nintex Process Platform utilizes Microsoft Azure and Amazon Web Services to host its cloud-based capabilities. Security is a shared responsibility between Nintex and its hosting provider Microsoft Azure. Microsoft Azure is responsible for the security of its platform, including middleware, the servers and physical security within its data centers.
        i. For more information on Microsoft Azure security, please see "Microsoft Azure Security, Privacy, and Compliance" available at: https://www.microsoft.com/en-us/download/details.aspx?id=26647
        ii. For more information on AWS security, please see: https://aws.amazon.com/security/ and https://aws.amazon.com/compliance/shared-responsibility-model/
13. **Supply Chain Management**. Nintex may use third party vendors to provide the Nintex Process Platform.
    a. **Assessment**. Nintex carries out a security risk-based assessment of prospective critical vendors before working with them to validate they meet Nintex's security requirements. Nintex periodically reviews its critical vendors in light of security and business continuity standards, including the type of access and classification of data being accessed (if any), controls necessary to protect data, and legal or regulatory requirements.
    b. **Contracts**. Nintex enters into written agreements with its vendors which include confidentiality, privacy, and security obligations that provide an appropriate level of protection for data that these vendors may process.
14. **Network Security**. Nintex implements measures in its corporate and product network such as firewall, Segmentation, DDoS protection and DNS security.

EXHIBIT C

MODULE 2: CONTROLLER TO PROCESSOR

Costumer and Company hereby agree that they will comply with the EU Standard Contractual Clauses which are incorporated herein by reference, a copy of which can be found at https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en as amended by this Annex 2A. The parties agree to Standard Contractual Clauses using Module 2 with the following terms:

Clause 7 (Docking Clause)-not used

Clause 9 (Use of Subprocessors): "Option 2" applies; and subsection (a) shall state: OPTION 2 GENERAL WRITTEN AUTHORISATION: 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 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.

Clause 11 (Redress) subsection (a) shall state: 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 authorized to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

Clause 13 (Supervision) Clause 13 shall apply as follows:

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.

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.

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 Data Protection Commission of Ireland.

Clause 17 (Governing law): "Option 1" applies and shall state: 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) subsection (b) shall state: The Parties agree that those shall be the courts of Ireland.

MODULE 3: PROCESSOR TO PROCESSOR

Customer and Company hereby agree that they will comply with the EU Standard Contractual Clauses which are incorporated herein by reference, a copy of which can be found at https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en as amended by this Annex 2A. The parties agree to Standard Contractual Clauses using Module 3 with the following terms:

Clause 7 (Docking Clause)-not used

Clause 9 (Use of Subprocessors): "Option 2" applies; and subsection (a) shall state: OPTION 2 GENERAL WRITTEN AUTHORISATION: The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub- processors at least 30 days in advance, thereby giving the controller 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 controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).

Clause 11 (Redress) subsection (a) shall state: 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 authorized to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

Clause 13 (Supervision) Clause 13 shall apply as follows:

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.

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.

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 Data Protection Commission of Ireland.

Clause 17 (Governing law): "Option 1" applies and shall state: 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) subsection (b) shall state: The Parties agree that those shall be the courts of Ireland.

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