CONTRACTUAL CLAUSES FOR SUBCONTRACTING THE PROCESSING OF PERSONAL DATA - ARTICLE 28 - DATA PROCESSING AGREEMENT

What is the purpose of this agreement?

Article 28(4) of the GDPR requires the conclusion of a subcontracting contract for the processing of personal data between the Controllers of personal data (our clients) and the Processor of personal data (Nexus). The purpose of the present Data Processing Agreement (DPA) is to fulfil this requirement. To ensure a high level of compliance and facilitate its adoption by our clients, the present DPA is based entirely on the EU standardized contractual clauses (SCCs).

Why did Nexus choose Standard Contractual Clauses?

To facilitate the conclusion of contracts required under Article 28 of the GDPR, the European Commission adopted on June 4, 2021 standardized contractual clauses (SCCs).

Nexus has chosen to use the SCCs published by the European Commission because they are “ready-made”: they avoid having to negotiate individual contracts while providing the best level of compliance to all the parties involved. Moreover, contrary to SCCs adopted by national data protection authorities, the SCCs published by the European Commission can be relied upon throughout the entire European Economic Area (EEA) and are binding on all EEA data protection authorities. The validity of the SCCs adopted by the European Commission can be contested only before the Court of Justice of the European Union. As a result, they provide for a harmonized approach across the EEA with the legal certainty of an EU act.

You can find more information about the SCCs at the following link: Standard contractual clauses for controllers and processors in the EU/EEA

N.B: These SCCs are different from the SCCs dedicated to transfers of personal data outside the EU/EEA.

Has Nexus made any changes to the SCCs?

The SCCs are “ready-made” by the European Commission: they are not meant to be modified by the parties. As a result, this data processing agreement incorporating the SCCs does not present any modification to the SCCs published by the European Commission.

On specific points, the SCCs require to mention practical information (e.g. which data is being processed, who are the eventual subcontractors, etc.). For transparency, we have made additions to the original text of the SCCs in blue.

How to conclude this data processing agreement?

The present DPA is an integral part of Nexus’ Terms and Conditions. If you sign a contract with Nexus and a data processing agreement is required under the GDPR, you will automatically enter into the present DPA.

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance with Article 28(3) and (4) 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.

(b) The controllers and processors listed in Annex I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 and/or Article 29 (3) and (4) Regulation (EU) 2018/1725.

(c) These Clauses apply to the processing of personal data as specified in Annex II.

(d) Annexes I to IV are an integral part of the Clauses.

(e) These Clauses are without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

Clause 2

Invariability of the Clauses

(a) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.

(b) This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

Clause 3

Interpretation

(a) Where these Clauses use the terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively, 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 or Regulation (EU) 2018/1725 respectively.

(c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

Clause 4

Hierarchy

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

Clause 5 - Optional

Docking clause

(a) Any entity that is not a Party to these Clauses may, with the agreement of all the Parties, accede to these Clauses at any time as a controller or a processor by completing the Annexes and signing Annex I.

(b) Once the Annexes in (a) are completed and signed, the acceding entity shall be treated as a Party to these Clauses and have the rights and obligations of a controller or a processor, in accordance with its designation in Annex I.

(c) The acceding entity shall have no rights or obligations resulting from these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 6

Description of processing(s)

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Annex II.

Clause 7

Obligations of the Parties

7.1. Instructions

(a) The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.

(b) The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or the applicable Union or Member State data protection provisions.

7.2. Purpose limitation

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex II, unless it receives further instructions from the controller.

7.3. Duration of the processing of personal data

Processing by the processor shall only take place for the duration specified in Annex II.

7.4. Security of processing

(a) The processor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (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 purposes of processing and the risks involved for the data subjects.

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

7.5. Sensitive data

If the processing 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 ("sensitive data"), the processor shall apply specific restrictions and/or additional safeguards.

7.6 Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.

(c) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. At the controller's request, the processor shall also permit 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 an audit, the controller may take into account relevant certifications held by the processor.

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

(e) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

7.7. Use of sub-processors

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

(b) Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

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

(d) The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub-processor to fulfil its contractual obligations.

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

7.8. International transfers

(a) Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfil a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.

(b) The controller agrees that where the processor engages a sub-processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

Clause 8

Assistance to the controller

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

(b) The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the controller's instructions

(c) In addition to the processor's obligation to assist the controller pursuant to Clause 8(b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:

(1) the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

(2) the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;

(3) the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;

(4) the obligations in Article 32 Regulation (EU) 2016/679.

(d) The Parties shall set out in Annex III the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

Clause 9

Notification of personal data breach

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 Regulation (EU) 2016/679 or under Articles 34 and 35 Regulation (EU) 2018/1725, where applicable, taking into account the nature of processing and the information available to the processor.

9.1 Data breach concerning data processed by the controller

In the event of a personal data breach concerning data processed by the controller, the processor shall assist the controller:

(a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

(b) in obtaining the following information which, pursuant to Article 33(3) Regulation (EU) 2016/679, shall be stated in the controller's notification, and must at least include:

(1) the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(2) the likely consequences of the personal data breach;

(3) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this 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.

(c) in complying, pursuant to Article 34 Regulation (EU) 2016/679, with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

9.2 Data breach concerning data processed by the processor

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

(a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

(b) the details of a contact point where more information concerning the personal data breach can be obtained;

(c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this 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.

The Parties shall set out in Annex III all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under Articles 33 and 34 of Regulation (EU) 2016/679.

SECTION III – FINAL PROVISIONS

Clause 10

Non-compliance with the Clauses and termination

(a) Without prejudice to any provisions of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725, in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.

(b) The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:

(1) the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;

(2) the processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725;

(3) the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(c) The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the controller insists on compliance with the instructions.

(d) Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or, return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.

ANNEX I LIST OF PARTIES

Controller(s): [*Identity and contact details of the controller(s), and, where applicable, of the controller's data protection officer]*

Identity	The client, as identified in the contract concluded between the client and Nexus.
Contact	The contact details of the client for GDPR-related matters shall be mentioned in the main contract.

Processor(s): [*Identity and contact details of the processor(s) and, where applicable, of the processor's data protection officer]*

Identity	Technology Nexus Secured Business Solutions AB ("Nexus") Telefonvägen 26, 126 26 Hägersten | Sweden
Contact	Data protection officer: dpo@nexusgroup.com

ANNEX II: DESCRIPTION OF THE PROCESSING

Categories of data subjects whose personal data is processed: Mentioned in Annex IV

Categories of personal data processed: Mentioned in Annex IV

Sensitive data processed (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: Nexus is not processing sensitive personal data.

Nature of the processing: Mentioned in Annex IV

Purpose(s) for which the personal data is processed on behalf of the controller: Mentioned in Annex IV

Duration of the processing: The table below ("*Data retention periods of Nexus' products*") explains in detail which of our products use default retention periods and when the Controller has the possibility to set such duration. When there is no retention period set, personal data is kept by Nexus for the time necessary for the execution of the contract with the Controller, i.e. the duration of the contractual relationship, and in order to fulfill its legal and regulatory obligations. Upon termination of the main agreement, the Controller shall instruct Nexus in writing if it wishes to have the personal data transferred to the Controller. Nexus will erase the data from its systems no earlier than 30 days and no later than 40 days after the effective date of termination of the service or as otherwise agreed.

Data retention periods	
GO WorkForce, GO Workplace, GO IoT	Certificate Manager • Certificate Manager stores two types of data: (i) the certificates themselves and (ii) the data used to generate the certificates. By default, there is no default retention period for either type of data. Each client may delete the data at any time, via two options. • The first option is to delete the data on the client's side. The client can ask Nexus to activate the "*GDPR removal*" functionality. Please note that this function is not visible by default for security reasons. When the functionality is activated, the certificate manager officer sees this functionality on its client device. Clicking on the "*GDPR removal*" button will delete the certificates, and the data used to generate the certificates. • The second option is to delete the data on Nexus' side. The deletion of the data can be done by Nexus' teams directly. In such a case, the client must make a request to Nexus to delete the data. Identity Manager (where applicable) • IDM stores two types of data: (i) tables, which is the usual data needed for the software and (ii) object related data, which are logs of the events of the workflows. • By default, there is no duration period, and the data is kept for the duration of the main agreement. However, there is a built-in functionality to delete data on a periodic basis: this functionality needs to be activated and configured by Nexus' teams. The client can request such activation: in such case, the client must provide Nexus its preferred retention period. • For more specific information, please read our Identity Manager documentation. SIS Cards: • SIS Cards stores the following categories of personal data: (i) identification data (last name, first name, email adress, employee number, date of birth, photo, signature, home adress, social security number), (ii) professional life data (company, title), (iii) order data (card order history and production data, shipping company, shipping adress, and (iv) connection data (cookies). • Purposes of the personal data processing are to deliver all types of corporate cards (ID badges), and to enable issuance, tracking, and management of access credentials. Data subjects concerned are the customer's end users • Data retention period is 5 years + 1 year
GO Cards 2.0	• The Controller has the possibility to set up a retention period for its organization. He can have his order data removed or anonymized after 3, 6, 12, 24 or 36 months. The default value is 36 months. If the organization was onboarded before 2024-08-12, the default value is set to no retention period. • For more information, please read our GO Cards documentation.
GO Cards 1.0	• There is no default retention period: the data is kept for the duration of the main agreement.
GO Signing	• Users that are using their Smart ID-account for signing have their email and name stored in PDF Signs database. • Signed documents are stored 30-60 days. This period is the same for all clients.

GO Authentication / Digital Access	• GO Authentication and Digital Access store the logs generated by the software. • By default, there is no duration period, and the data is kept for the duration of the contract. A specific retention period can be set globally upon request by the client.
E-Signing	• Signed documents are stored for 90 days. • Transactions based on BankID, NemID and MitID are stored for 3 months. Transactions based on Nets NPS are stored for 5 years. • Users of the E-Signing Portal are stored as long as user is active + 3 months. Their transaction data is stored for 6 months.

For processing by (sub-) processors, also specify subject matter, nature and duration of the processing: Nexus will ensure that the duration of processing with sub-processors does not exceed the duration mentioned in the present agreement.

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

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

Nexus has an information security policy. For confidentiality and security reasons, we only provide all or part of this policy on demand on a case-by-case basis. Please contact us if you wish to have more detailed information.

This policy covers the following elements:

- Confidentiality
  - Access control to premises and facilities
  - Access control to systems
  - Access control to data
  - Segregation control

- Integrity
  - Disclosure control
  - Input control

- Availability, Resilience, Recoverability
  - Availability control

- Procedures for regular review, assessment & evaluation
  - Job control
  - Data protection management
  - Privacy-friendly default settings

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller:

Nexus has a policy in place for the choice and monitoring of sub-processors. This policy includes the conduct of an information security and GDPR requirements questionnaire (“Nexus Security Requirements”). For confidentiality and security reasons, we only provide all or part of this procedure on demand on a case-by-case basis. Please contact us if you wish to have more detailed information.

This policy includes the review with our suppliers of the following elements:

- Information Security requirements
  - Information security policies
  - Confidentiality undertaking
  - Subcontractor control
  - Network security
  - Encryption
  - Access control
  - Incident and change notifications
  - Segregation of data
  - Business continuity
  - Backup
  - Malware
  - Update and patch
  - Logging and monitoring
  - Hardening practices
  - Remote access
  - Training
  - Production data and environment
  - Physical security
  - Communication with Nexus

- GDPR-specific requirements
  - Processing of data
  - Privacy documentation
  - GDPR incident handling
  - Storage of personal data
  - Protection of personal data
  - Prior injunctions or condemnations for GDPR breaches
  - Corrective undertaking in case of non-compliance

Description of the specific technical and organisational measures to be taken by the processor to be able to provide assistance to the controller.

Nexus undertakes to cooperate with its clients to assist them in GDPR-related matters. Nexus has appointed a data protection officer and an information security officer.

ANNEX IV: LIST OF SUB-PROCESSORS

The controller has authorised the use of the following sub-processors.

The following list is a complete list of our sub-processors for our products and services. As a result, for the avoidance of doubt, the Controller's authorisation shall apply only to the sub-processors which are necessary for the performance of the main contract between Nexus and the Controller.

Sub-processor	Address	Localization of the services	Purpose of the processing	Transfer to third country	Categories of data subjects, categories of data, and nature of processing	Sensitive data
PRODUCTS						
GO Workforce, GO Workplace, GO IoT						
Cleura AB	Blekingegatan 1 Karlskron Sweden	Sweden	Data center infrastructure services	N/A	Personal data processed may include any categories of personal data provided by the Controller regarding identity, contact, geolocation, vehicle identification number, SSN, images, title/position and authentication. Nexus does not control what kind of personal information is inserted by the Controller in the certificates.	N/A
Redbridge AB	Gamla Brogatan 26 111 20 Stockholm Sweden	Sweden	Load balancer	N/A	Handling streaming data load balancing to Nexus datacenters. Redbridge does not view or read the personal data, but only forwards it to the recipient. The personal data is end to end encrypted and therefore Redbridge cannot view the content. Only upon the Controller's written request, IP addresses may be processed by Redbridge for troubleshooting purposes. Streaming data concerns mostly contact information of the Controller's employees. Redbridge does not retain any personal data.	N/A
Sotera AS	Strandveien 37, 1366 Lysaker Norway	Norway	Service Provider	N/A	Sotera acts as a Sub-processor solely in connection with the SIS Cards product. Sotera develops and operates the Breeze Portal, an ordering portal for physical and virtual ID and access cards, keyfobs, and accessories. Sotera processes personal data solely for the purpose of providing, operating, and administering the Breeze Portal and related ordering and management services.	N/A
GO Cards 2.0						
Microsoft AB	Regerings-gatan 25 111 53 Stockholm Sweden	Nether-lands (main server) Ireland (redun-dant server)	Microsoft Azure is used as cloud solution for platform as a service	N/A	Any categories of data provided by the Controller to produce authenticators for identification and access control. Data for this purpose includes information such as first name, surname, personal identity number/social security number, personal photo,	N/A

					employee number, gender, nationality, home address, etc.	
Canva Austria GmbH	Ungargasse 37/BT1/3.3 1030 Vienna Austria	Nether-lands (main server)	Optional background removal feature within GO Cards, applicable only to customers who actively use this specific feature (not to all GO Cards users)	Personal data may be transferred to the U.S. by the sub-processor to its sub-processors, all of whom are certified under EU-U.S. Data Privacy Framework	The personal data processed consists solely of the image uploaded by cardholders who use the optional feature for the purpose of automated background removal. The processing is primarily carried out within the EU. The sub-processor may involve sub-processors located in the U.S. These sub-processors are certified under the EU-U.S. Data Privacy Framework, which constitutes an adequacy decision under GDPR.	N/A
GO Cards 1.0						
Orange Business Sweden AB	Gårdsvägen 6 169 70 Solna Sweden	Sweden	Data center infrastructure services	N/A	Any categories of data provided by the Controller to produce authenticators for identification and access control. Data for this purpose includes information such as first name, surname, personal identity number/social security number, personal photo, employee number, gender, nationality, home address etc.	N/A
GO Signing						
Nordea Bank AB		Sweden	Authentication provider	N/A	Swedish BankID. Only the personal identity number is processed.	N/A
Microsoft AB	Regeringsgata n 25 111 53 Stockholm Sweden	Netherlan ds (main server) Ireland (redundan t server)	Microsoft Azure is used as cloud solution for platform as a service	N/A	Contents of documents for signing, as well as name, email address or other user data registered in the service, of users for the purpose of generating digital signatures on documents. In the case where users sign documents with Swedish BankID, personal identity numbers are processed.	N/A
GO Auth / Digital Access						
Orange Business Sweden AB	Gårdsvägen 6 169 70 Solna Sweden	Sweden	Data center infrastructure services	N/A	Email and social security number	N/A

SUPPORT AND MAINTENANCE						
Imprimerie Nationale S.A (IN Groupe)	38, avenue de New-York 75116 Paris	France	Hosting of applications on servers in France (Douai). We use IN Groupe's servers to deploy an array of systems as outsourcing partner	N/A	Names, work email addresses and IP addresses of administrators are stored in the system sessions. We save them in the following systems: Nexus IDP, OpenLDAP and Jira. We create accounts for customers in our system. We use the data to communicate with customers in support tickets. During handling of support tickets, we receive logs from the customer which may contain personal numbers, names, certificate data, IP addresses, etc.	N/A

Orange Business Services AB	Gårdsvägen 6 169 70 Solna Sweden	Sweden	Hosting of Identity solution	N/A	Customer accounts are created via OpenLDAP. We use this to control the user administration of the customers (customer name and email address).	N/A

TRAINING					
Training with 360Learning					
Microsoft	France	Hosting of 360Learning's infrastructure	N/A	Last Name, First Name, Email, Employment, Photo. Login, Usage Stats, and in general, all data processed in the context of the services.	N/A
Scaleway	France	Hosting test environments for customers who requested it for their own needs	N/A	Last Name, First Name, Email, Employment, Photo, Login, Usage Stats and in general all data processed in the context of the tests.	N/A
OVH	France	Hosting	N/A	Media files (upload)	N/A
Amazon SES	Ireland	Sending notification mails	N/A	Email, Email Content and Email Opt-in	N/A
Amplitude	US	Usage statistics for reporting	Yes Signed DPA with Standard Contractual Clauses (SCCs)	ID (pseudonymisation)	N/A
Pendo Inc.	EU	Platform notifications, guides, and other in-app communication	N/A	ID (pseudonymisation)	N/A
Gainsight Inc.	Germany	Usage statistics for reporting	N/A	ID (pseudonymisation)	N/A
Datadog	EU	Observability	N/A	ID (pseudonymisation)	N/A
Snowflake Computing Netherlands B.V.	EU	Usage statistics for reporting. Ship data-processing features (e.g: platform search)	N/A	Last Name, First Name, Email (to make them available in the Search Not used for statistics) - For statistics : ID (pseudonymisation)	N/A
Elastic App Search	EU	Search engine to power platform search; usage analytics for recommendations	N/A	Last Name, First Name, Email	N/A
Workato Inc.	EU	iPaaS provider for automations	N/A	For workato's connectors : personal data uploaded to the Service. which may include but is	N/A

			and 3rd party integrations		not limited to Last Name, First Name, Email. The data is provided by the 3rd party application, licenced and configured by the customer	
Zendesk		US and EU	Managing customer support requests	Yes Signed DPA with Standard Contractual Clauses (SCCs) Zendesk Internal BCRs	Last Name, First Name, Email, Photo (if added). This subcontractor may only have access to a limited number of authorized users having a specific role: Author, Administrator, Owner	N/A
Training with Rise						
Rise (Articulate Global LLC.)	244 5th Avenue, Suite 2960, NY 10001 New-York USA	US	Training SaaS Provider	Yes Certified under the Data Privacy Framework	Usage Data when users access and use the Services, including Internet Protocol (IP) address, access times, browser type and language, Internet Service Provider (ISP), the web pages that users visit, behavior during the visit, the content you use, and the URL of the web page you visited before navigating to our Services.	N/A

Important notice: When Nexus makes available a Rise webpage to its clients for training purposes, Nexus does not process directly any personal data. Nexus shall not be considered a Processor. The customer is the Controller and Rise is the Processor. The mention of Rise in the present DPA is provided for information purposes only and shall not mean that Nexus has any GDPR obligation in this processing. It is the responsibility of the Controller to make sure the relevant legal obligations are addressed directly with Rise. Additional information about Rise privacy may be found in Rise's documentation.