Data Processing Agreement

This Data Processing Agreement ("**DPA**") constitutes Schedule 1 to the Agreement applicable to the Order form and/or Quotation acceptance model procedures of Nexus. In this DPA, the Customer is referred to as the "**Controller**" and Nexus is referred to as the "**Processor**". The Controller and the Processor are individually referred to as "**Party**" and jointly as "**Parties**". The respective roles of the Parties are outlined in accordance with EU Regulation 2016/679 ("**GDPR**"), as amended, supplemented and/or varied from time to time.

The Controller is the data controller in relation to the processing of personal data, for which the Controller determines the purposes and means. The Processor is a data processor, processing the personal data on behalf of the Controller. Unless otherwise is explicitly set out in this DPA, the defined terms used elsewhere in the Agreement shall be applicable to this DPA.

The Parties shall negotiate in good faith and agree on any relevant and necessary amendments and updates to this DPA and the processing activities carried out hereunder to ensure that it complies with the GDPR and applicable supplementary rules and regulations to the GDPR ("**Applicable Legislation**") at all times during the term of this DPA.

In addition to this main body of the agreement, this DPA incorporates the following documents:

- **Appendix I** – Categories of personal data and approved sub-processors per product/service (i.e. Delivery Services, Software as a Service, Nexus GO services, Support and/or Maintenance).

- **Appendix II** – Standard contractual clauses of the European Union (where applicable). See www.nexusgroup.com/terms-and-conditions.

POINT OF CONTACT

The Data Protection Officer ("**DPO**") of Nexus can be reached through the following contact details:

Technology Nexus Secured Business Solutions AB
Attn: Data Protection Officer
Telefonvägen 26, 126 26 Hägersten | Sweden
Email: dpo@nexusgroup.com

1. Instructions

1.1 Any processing of personal data carried out by the Processor shall be carried out in accordance with the following instructions:

	Instructions
Purposes of the processing	To deliver the deliverables to the Controller as outlined in the Agreement.
The character of the processing	The processing necessary to enable the use of the deliverables. This includes reading, receiving a request, installing, validating, storing, troubleshooting, providing support and maintenance, as well as other comparable processing activities.
The period of the processing	The earlier of either (i) the termination of the deliverables, or (ii) the Controller's instruction to cease processing.
Categories of data subjects	In accordance with the Controller's instruction, e.g. customers, end customers, suppliers and/or their personnel.

1.2 The Processor may not process the personal data for any other purposes or in any other way than as instructed by the Controller from time to time.

1.3 Notwithstanding the above, the Processor may undertake reasonable day-to-day actions with the personal data without having received specific written instructions from the Controller, provided that the Processor acts for and within the scope of the purposes stated in the instruction.

1.4 In the event that the Processor considers that any instruction violates Applicable Legislation, the Processor shall refrain from acting on such instructions and shall promptly notify the Controller and await amended instructions.

2. The Controller's obligation to process data lawfully

2.1 The Controller shall ensure that a legal ground recognized under Applicable Legislation applies for the processing of the personal data. The Controller shall further meet all other obligations of a controller under Applicable Legislation (including requirements to properly inform the data subjects of the processing activities).

2.2 The Controller's instructions for the processing of the personal data shall comply with Applicable Legislation. The Controller shall have sole responsibility for the accuracy, quality, and lawfulness of the personal data in connection to the purpose of the processing activities, including means by which it acquired the personal data.

3. Use of Sub-Processors

3.1 The Processor may engage third parties to process the personal data or any part thereof on its behalf ("**Sub-Processor**"), provided that the Controller has been informed thereof in writing at least 30 days prior to the engagement of such Sub- Processor. If the Controller does not accept such Sub-Processor, the Controller may terminate the deliverables in accordance with the terms set out in the Agreement.

3.2 The Processor shall enter into a written agreement with every Sub-Processor, in which each Sub-Processor undertakes obligations at least reflecting those undertaken by the Processor under this DPA.

3.3 When the Controller has approved a Sub-Processor, the Controller may no longer object to such Sub-Processor.

Approved Sub-Processors

3.4 The Approved Sub-Processors are listed in the Appendix I. The list shall be updated in the event of changes to the Approved Sub-Processors. The following information regarding each Approved Sub-Processor is included:

(i) name, contact information, company form and geographical location,

(ii) a description of the deliverables provided,

(iii) the location of the data that the Approved Sub-Processor processes.

4. Transfers to third countries

The Processor may not transfer personal data outside the EU/EEA, or engage a Sub-Processor to process personal data outside of the EU/EEA, without at least one of the following prerequisites fulfilled:

(i) the receiving country has an adequate level of protection of personal data as decided by the European Commission,

(ii) the transfer is subject to the European Commission's Standard Contractual Clauses for transfer of personal data to third countries, or

(iii) the Sub-Processor is subject to Binding Corporate Rules and the receiving party in the third country is also subject to the Binding Corporate Rules.

5. Security measures

5.1 The Processor shall maintain adequate security measures to ensure that the personal data is protected against destruction, modification and proliferation. The Processor shall further ensure that personal data is protected against unauthorized access and that access events are logged and traceable. The Controller agrees that these security measures are adequate, sufficient and appropriate.

5.2 The Processor shall ensure (i) that only authorized employees have access to the personal data and only when it is necessary to fulfill the purpose of the deliverable, (ii) that the authorized employees process the personal only in accordance with this DPA and the Controller's instructions and that each authorized employee is bound by a confidentiality undertaking towards the Processor in relation to the personal data, which continues even after their engagement

ends.

Technical and organizational measures

5.3 The Processor has implemented, and will maintain, appropriate technical and organizational measures, internal controls, and information security routines intended to protect personal data, against accidental loss, destruction, or alteration; unauthorized disclosure or access; or unlawful destruction as set forth in the subsections below.

- The Processor has appointed a security officer responsible for coordinating and monitoring the security rules and procedures.
- The Processor (including subcontractors) limits access to facilities where information systems that process personal data are located, to identified authorized individuals.
- The Processor uses a variety of industry standard systems to protect against loss of data due to power supply failure or line interference.
- The data center operating the deliverable includes replication features that facilitate recovery of personal data in the event a particular machine or cluster within a data center fails. The Processor's deliverables include a regular data backup procedure in addition to the data center replication.
- The Processor has anti-malware controls to help avoid malicious software gaining unauthorized access to personal data, including malicious software originating from public networks.
- The Processor logs, or enables the data exporter to log, access and use of information systems containing personal data, registering the access ID, time, authorization granted or denied, and relevant activity.

Authentication

5.4 The Processor uses industry standard practices to identify and authenticate users who attempt to access information systems.

- Where authentication mechanisms are based on passwords, the Processor requires that the passwords are renewed regularly.
- Where authentication mechanisms are based on passwords, the Processor requires the password to be at least eight characters long.

6. Confidentiality

6.1 The Processor undertakes not to disclose or provide any data, or any information related to the data, to any third party. For the avoidance of doubt, any approved Sub-Processor shall not be considered a third party for the purposes of this Section 6.

6.2 Notwithstanding Section 6.1 above, the Processor may disclose such information if the Processor is obliged hereto by law, judgement by court or by decision by a competent authority. When such obligation arises, the Processor shall promptly notify the Controller in writing before disclosure, unless restricted from doing so under Applicable Legislation.

6.3 The confidentiality obligation will continue to apply also after the termination of this DPA without limitation in time.

7. Assistance and Audit obligations

7.1 The Processor shall assist the Controller with the fulfilment of the Controller’s obligation to ensure that the data subjects may exercise their rights under Applicable Legislation by ensuring appropriate technical and organizational measures.

7.2 Upon the Controller’s request, the Processor will provide to the Controller information necessary to demonstrate the Processor’s compliance with its obligations under Applicable Legislation.

7.3 The Controller shall be entitled on 10 days’ written notice to carry out an audit of the Processor’s processing of the data and information relevant in that respect. The Processor shall assist the Controller and disclose any information necessary in order for the Controller to carry out such audit. The Controller shall carry the costs for such audit.

7.4 If a supervisory authority carries out an audit of

the Processor which may involve the processing of the Controller's personal data, the Processor shall promptly notify the Controller thereof.

8. Notification of data breach

The Processor shall notify the Controller without undue delay after becoming aware of a personal data breach. Furthermore, the Processor shall assist the Controller in ensuring compliance with the Controller's obligations to (i) document any personal data breach, (ii) notify the applicable supervisory authority of any personal data breach and (iii) communicate such personal data breach to the data subjects, in accordance with Applicable Legislation.

9. Liability

Each party shall be liable for any administrative fines imposed by a supervisory authority or a competent court on the party in question due to that party's failure to fulfill its obligations under Applicable Legislation or otherwise having processed personal data in breach of Applicable Laws or this DPA. The Processor's liability arising out of or related to this DPA is subject to the provisions on limitation of liability stated in the Agreement.

10. Return and deletion of data

The Controller shall upon termination of the Agreement instruct the Processor in writing whether or not to transfer the personal data processed to the Controller. The Processor 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.

11. Term and termination

This DPA shall, notwithstanding the term of the Agreement, enter into force when the Processor commences to process Data on behalf of the Controller and shall terminate when the Processor has erased the personal data in accordance with Section 10 above.

APPENDIX I – CATEGORIES OF PERSONAL DATA AND APPROVED SUB- PROCESSORS PER PRODUCT/SERVICE

1. DELIVERY SERVICES

For the purpose of delivering Delivery Services, it is not necessary for Nexus to process any personal data. In the event the Controller provides Nexus access to personal data for implementation or other purposes, this data will be processed by Nexus in accordance with this DPA.

1.1 Categories of personal data

Any categories of personal data provided by the Controller in order for Nexus to provide the service.

1.2 Approved sub-processors

Nexus will not engage any third party when processing personal data.

2. SOFTWARE AS A SERVICE

2.1 Categories of personal data

Any categories of personal data provided by the Controller regarding identity, contact, geolocation, vehicle, SSN, images, title/position and authentication.

2.2 Approved sub-processors

Sub-processor	Information
Cleura AB Blekingegatan 1 371 57 Karlskrona Sweden	Data center infrastructure services. CLEURA does not process any personal data.
Orange Business Services AB Gårdsvägen 6 169 70 Solna, Stockholm Sweden	Data center infrastructure services. To perform system administration on an Orange owned equipment, the technicians in Nexus Service Delivery team have access to hard drives containing personal data. Orange's staff do not handle these logs, but per definition they have access to them.
Ida Infront S:t Larsgatan 18 582 24 Linköping Sweden	Software to archive log files. Ida Infront archives on behalf of the customer: The application only handles encrypted logs and for that reason they do not have any access to personal data.

3. NEXUS GO

3.1 Nexus GO Cards

3.1.1 Categories of personal data

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.

3.1.2 Approved sub-processors for Nexus Go Cards 2.0

Sub-processor	Information
Microsoft Finlandsgatan 36 164 74 Kista Sweden	Subsidiary registered in Stockholm, headquarters in Redmond, WA, the United States. The Processor uses Microsoft Azure, in connection to its approved Sub-Processors, as a cloud solution platform service. The datacenter is located in the Netherlands.
Orange Business Services AB Gårdsvägen 6 169 70 Solna, Stockholm Sweden	Company that hosts part of the service and stores customer and personal data for the benefit of cardholders.

3.1.3 Approved sub-processors for Nexus Go Cards 1.0

Sub-processor	Information
Orange Business Services AB Gårdsvägen 6 169 70 Solna, Stockholm Sweden	Company that hosts part of the service and stores customer and personal data for the benefit of cardholders.

3.2 Nexus GO Signing

3.2.1 Categories of personal data

Any personal data provided by the Controller's users in the documents and to identify the signatories of a document. Examples are name, organization, email address and personal identity number.

3.2.2 Approved sub-processors

Sub-processor	Information
Nordea Mästersamuelsgatan 17 105 71 Stockholm Sweden	Company with registered office in Stockholm. The purpose of the processing of persona data by the Sub-Processor is to make and process authentications with Swedish BankID. Only the personal identity number is processed. Data will not be processed in other countries. The sub-processor does not in turn use sub-processors.
Microsoft Finlandsgatan 36 164 74 Kista Sweden	Affiliate with registered office in Stockholm, headquartered in Redmond, WA, United States of America. The Processor uses Microsoft Azure, with their approved sub- processors, as cloud solution for platform as a service. The service processes 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.

4. Support and/or Maintenance

4.1 Categories of personal data

Any categories of personal data provided by the Controller in order for Nexus to provide Support and/or maintenance. Data for this purpose includes information about identity and contact (such as name, telephone number, email address, IP address).

4.2 Approved sub-processors

Sub-processor	Information
Veniture Neuerburgstraße 2 51103 Köln Germany	Hosting of applications on Veniture servers in Germany. The processor uses Veniture's servers to deploy an array of systems as outsourcing partner. As application maintenance is included the sub-processor super administrators have access to data stored in the servers and applications. This data is comprised by name, email, username. IPaddresses are logged into the system sessions as well. In support ticket handling applications, there may be system logs including IP addresses, server names and user names.
Microsoft Finlandsgatan 36 164 74 Kista Sweden	Affiliate with registered office in Stockholm, headquartered in Redmond, WA, United States of America. The Processor uses Microsoft Office 365 for email service and cloud storage. Information handled via email is email address, name, signatures (office, company, position/title etc).
Soluno Lumaparksvägen 9 120 31 Stockholm Sweden	Telephone service in Germany. Soluno provides soft switchboard services to Nexus' employees. Support employees can access a separate queue where support calls are handled. Information handled by Soluna is: name, telephone number. For Nexus agents' office address. For customers calling their telephone number and general location.
Vodafone GmbH Ferdinand-Braun-Platz 1 40549 Düsseldorf Germany	Telephone service for some of our support services. Vodaphone is used in one account for 24x7 services in Germany. Information handled follows the telecom directives in EU. Information shared is telephone number. In telecom logs calling number, time,

	duration, geolocation.
Tele2 Sverige Torshamnsgatan 17 164 40 Kista Sweden	Telephone service for support of SaaS 24/7 Tele2 is a soft switchboard service for all Swedish employees. Nexus has a separate virtual telephone number used on the 24x7 rotation in Sweden. Data handled is telephone number, name, email, address (office/home) and queue for Nexus employees. For callers it's calling number, time, duration. Tele2 follows the telecom directives in EU. Telecom logs save calling number, time, duration, geolocation.