Data processing agreement for Nexus GO PDF Signing

This Data Processing Agreement (the “DPA”), constitutes Schedule 1 to the Agreement. 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 Controller is the data controller in relation to the processing of the Data. The Processor is a data processor, processing the 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.

1. Documents

This DPA consists of this main document and the following appendices:

Appendix 1: Instructions to the Processor
Appendix 2: Security Measures
Appendix 3: Approved Sub-Processors

2. Definitions and interpretation

2.1 In this DPA, capitalized terms shall have the meanings set out below or if not defined herein, the meanings set forth in Applicable Legislation.

<table>
<thead>
<tr>
<th>Applicable Legislation</th>
<th>means (i) until and including 24 May 2018, the PDA or equivalent in another state than Sweden, (ii) from and including 25 May 2018, the GDPR and (iii) any applicable supplementary legislation to the PDA or the GDPR.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data</td>
<td>means the personal data (as defined in Applicable Legislation), specified in Appendix 1 hereto.</td>
</tr>
<tr>
<td>GDPR</td>
<td>means Regulation (EU) 2016/679 of the European Parliament and the Council as amended, supplemented and/or varied from time to time.</td>
</tr>
</tbody>
</table>

2.2 The Parties shall negotiate in good faith and agree on any relevant and necessary amendments and updates to this DPA and the processing carried out hereunder to ensure that it complies with Applicable Legislation at all times during the term of this DPA.

3. Instructions

3.1 The Processor shall process the Data in accordance with the Controller’s written instructions set forth in Appendix 1. The instructions shall at least include the following information:

(i) The purpose of the processing;
(ii) The character of the processing;
(iii) The duration of the processing, or how the duration will be decided;
(iv) Categories of personal data included in the Data; and
(v) Categories of data subjects included in the processing.

3.2 The Processor may not process the Data for any other purposes or in any other way than as instructed by the Controller from time to time. The Parties shall update Appendix 1 in the event of new or amended instructions. The Processor is entitled to charge any work carried out by it to comply with the Controller’s instructions on a time and material basis in accordance with its standard consultancy rates.
3.3 Notwithstanding the above, the Processor may undertake reasonable day-to-day actions with the 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 Appendix 1.

3.4 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.

4. The Controller's obligation to process data lawfully

4.1 The Controller shall obtain explicit and legally valid consents from each data subject for the processing of the Data or ensure that another legal ground recognized under Applicable Legislation applies for processing of the 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 of the Data).

4.2 The Controller’s instructions for the processing of the Data shall comply with Applicable Legislation. The Controller shall have sole responsibility for the accuracy, quality, and legality of the Data and the means by which it acquired the Data.

5. Security measures

5.1 The Processor shall maintain adequate security measures to ensure that the Data is protected against destruction, modification and proliferation. The Processor shall further ensure that Data is protected against unauthorized access and that access events are logged and traceable. The security measures are described in Appendix 2. 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 Data, (ii) that the authorized employees process the Data only in accordance with this DPA and the Controller’s instructions and (iii) that each authorized employee is bound by a confidentiality undertaking towards the Processor in relation to the Data.

5.3 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.

6. The Processor’s obligations to assist

6.1 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. The data subjects’ rights include (i) rights to object to the processing and have the Data erased, (ii) rights to request information about and access to the Data, (iii) if technically viable, rights to move Data from one controller to another, and (iv) rights to request correction of Data.

6.2 The Processor shall further assist the Controller in relation to the Controller’s obligations under Articles 32-36 of the GDPR (such obligations include (i) ensuring security of the processing, (ii) impact assessments regarding data protection and (iii) prior consultations).

7. Sub-Processors

7.1 The Processor may engage third parties to process the Data or any part thereof on its behalf (“Sub-Processor”), provided that the Controller has been informed thereof in writing at least 45 days prior to the engagement of such Sub-Processor. If the Controller does not accept such Sub-Processor, the Controller may terminate the Agreement in accordance with the terms set out in the Agreement. Approved Sub-Processors are listed in Appendix 3 hereto (which shall be updated in the event of changes to the Approved Sub-Processors). Appendix 3 shall list the following information regarding each Approved Sub-Processor:
name, contact information, company form and geographical location,

(ii) a description of the services provided,

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

7.2 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.

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

8. Transfers to third countries

The Processor may not transfer personal data outside the EU/EEA, or engage a Sub-Processor to process Data outside of the EU/EEA, without the Controller’s consent and upon such consent only if at least one of the following prerequisites is fulfilled:

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

(ii) the Controller confirms that the data subject has given his/her consent to the transfer,

(iii) the transfer is subject to the European Commission’s standard contractual clauses for transfer of personal data to third countries,

(iv) the Processor is subject to Binding Corporate Rules and the receiving party in the third country is also subject to the Binding Corporate Rules, or

(v) for transfers to the United States, the receiving legal entity is certified under the EU-U.S. Privacy Shield.

9. Audit

9.1 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.

9.2 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.

9.3 If a Data Protection Authority carries out an audit of the Processor which may involve the processing of Data, the Processor shall promptly notify the Controller thereof.

10. Costs

10.1 Unless otherwise has been agreed, the Processor shall be entitled to remuneration for its processing of the Data in accordance with prices on http://go.nexusgroup.com

10.2 The Controller shall bear all additional costs for any altered or additional instructions to the Processor regarding the processing of the Data and for any additional costs incurred by the Processor due to any changes of Applicable Legislation or other relevant regulations. The Controller shall further be entitled to compensation for any and all actions undertaken by it on behalf of or as instructed by the Controller.

11. Limitation of liability

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.
12. Confidentiality

12.1 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 12.

12.2 Notwithstanding Section 12.1 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.

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

13. Return and deletion of data

The Controller shall upon termination of the Agreement instruct the Processor in writing whether or not to transfer the Data to the Controller (such transfer to be made in a common machine readable format). 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 Agreement.

14. Term

This DPA shall, notwithstanding the term of the Agreement, enter into effect when the Processor commences to process Data on behalf of the Controller and shall terminate when the Controller has erased the Data in accordance with Section 13 above.

Appendix 1 - Instructions to the Processor

Any processing carried out by the Processor shall be carried out in accordance with the following instructions. If the Processor processes Data in violation with these instructions, the Processor will be deemed data controller.

<table>
<thead>
<tr>
<th>INSTRUCTION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Purposes of the processing</strong></td>
</tr>
<tr>
<td>To enable the Controller to use the Services.</td>
</tr>
<tr>
<td><strong>The character of the processing</strong></td>
</tr>
<tr>
<td>The processing necessary to enable the use of the Services, mainly temporary storage.</td>
</tr>
<tr>
<td><strong>The period of the processing</strong></td>
</tr>
<tr>
<td>The earlier of (i) the termination of the Agreement, or (ii) the Controller’s instruction to the Processor to cease processing of the Data.</td>
</tr>
<tr>
<td><strong>Categories of Data</strong></td>
</tr>
<tr>
<td>Any 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 national identification number (“personnummer”).</td>
</tr>
<tr>
<td><strong>Categories of data subjects</strong></td>
</tr>
<tr>
<td>1. Any categories of data subjects provided by the Controller’s Users in the Documents.</td>
</tr>
<tr>
<td>2. Users which shall or have signed a Document.</td>
</tr>
<tr>
<td><strong>Any other instructions</strong></td>
</tr>
<tr>
<td>-</td>
</tr>
</tbody>
</table>
Appendix 2 - Security Measures

The Processor will implement and maintain the security measures set out in this Appendix 2.

1. Personnel

The Processor's personnel will not process the Controller's Data without authorization and only when this is necessary to fulfill the purpose of the service. Personnel are obligated to maintain the confidentiality of any Data and this obligation continues even after their engagement ends.

2. Data privacy contact

The Information security officer of the data importer can be reached at the following address:

**Technology Nexus AB**

Attn: Chief Security Officer

Telefonvägen 26, 126 26 Hägersten | Sweden

Email: peter.hellstrom@nexusgroup.com

3. Technical and organizational measures

The Processor has implemented, and will maintain for the service, appropriate technical and organizational measures, internal controls, and information security routines intended to protect Data, as defined in the Agreement, 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 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 service includes replication features that facilitate recovery of Data in the event a particular machine or cluster within a data center fails. The Processor's services 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 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 Data, registering the access ID, time, authorization granted or denied, and relevant activity.

4. Authentication

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.

Appendix 3 - Approved Sub-Processors
<table>
<thead>
<tr>
<th>Sub-Processor</th>
<th>Information</th>
</tr>
</thead>
</table>
| Nordea        | Company with registered office in Stockholm.  
               | The purpose of the processing of Data by the Sub-Processor is to make and process authentications with Swedish BankID. Only the national identification number "personnummer" is processed.  
               | Data will not be processed in other countries.  
               | The Sub-Processor does not in turn use Sub-Processors. |
| Microsoft     | 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, national identification numbers, "personnummer", are processed. |
| Coegi AB      | Company with registered office in Göteborg.  
               | The purpose of the processing is to generate certificates that identify the user that has performed a signing operation. Any data about the user, that has been registered in the service, may be submitted in a certificate request. |