NordPass

DATA PROCESSING AGREEMENT (BUSINESS)

Last updated: 27/09/2021

The Customer ("**Data Controller**") and NordPass ("**Data Processor**");

Data Controller and Data Processor are hereinafter collectively referred to as the "**Parties**";

Whereas

(i) The Data Processor provides Services to the Data Controller under the NordPass Terms of Service (Business) ("**Terms**") available at the Data Processor's website;

(ii) While providing the Services Data Processor Processes the Personal Data on behalf and under instructions of the Data Controller;

(iii) The Parties wish to lay down their rights and obligations related to the above-described Personal Data Processing;

Concluded this data processing agreement (the "**Agreement**").

1. Definitions

1.1 Unless expressly otherwise provided in this Agreement, definitions and (or) capitalized words used in this Agreement shall have the meaning as defined in Terms or as indicated below:

Applicable data protection laws	means all applicable privacy and data protection laws and regulations anywhere in the world, including, where applicable, the GDPR;
EEA	means European Economic Area (all EU Member States, UK and Iceland, Norway and Liechtenstein);
GDPR	means 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, and repealing Directive 95/46/EC (General Data Protection Regulation);
Processing	means any operation or set of operations carried out using Personal Data or Personal Data sets, regardless of whether it is performed by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination and access, coordination, restriction, deletion or destruction;
Person	means a natural person whose Personal Data are processed;

Personal Data	means any information relating to an identifiable Person;
Standard Contractual Clauses (SCC)	means standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (Commission implementing decision 2021/914 of 4 June 2021), as up-dated or replaced from time to time;
Sub-processor	means an entity engaged by the Data Processor which agrees to receive Personal Data from the Data Processor exclusively intended for the Processing activities to be carried out as part of the Services.

2. Application of this Agreement

2.1. This Agreement applies if the Processing of Personal Data is governed by the GDPR. If the Agreement applies, it shall be legally binding between the Parties and constitute an integral part of the Terms.

2.2. Except as otherwise agreed in this Agreement (including the SCC, if applicable) Terms are applied between the Parties in their entirety.

3. General provisions and obligations

3.1 The Data Processor undertakes to only Process Personal Data in accordance with documented instructions communicated from time to time by the Data Controller. The Data Controller's initial instructions to the Data Processor regarding the subject-matter and duration of the Processing, the nature and purpose of the Processing, the type of Personal Data and categories of Persons are set forth in this Agreement.

3.2 When Processing Personal Data under this Agreement, the Data Controller shall comply with all Applicable data protection laws and recommendations of the competent supervisor authorities.

3.3 Data Controller will not take any action that would cause the Data Processor to violate Applicable data protection laws.

3.4 By signing the Agreement Data Controller confirms that:

3.4.1. All the Personal Data Processed under this Agreement is collected lawfully;

3.4.2. All the conditions allowing Personal Data transfers to the Data Processor outside EEA are fulfilled;

3.4.3. All the Persons were properly informed about the use of the Data Processor`s Services and all the information as it is required under the Applicable data protection laws was submitted to the Persons by the Data Controller.

3.5 All the instructions as set out in this Agreement are comprehensive and reflect the Data Controller`s will. Any additional or alternate instructions by the Data Controller shall be agreed between the Parties separately in writing.

3.6 The Data Processor:

3.6.1. Shall not evaluate any instructions of the Data Controller which shall be held responsible and liable for any given instructions to be fully lawful and compliant with the Applicable data protection laws. If in the Data Processor`s reasonable opinion, an instruction undoubtedly infringes the Applicable data protection laws, the Data Processor shall notify the Data Controller;

3.6.2. Taking into account the nature of the Processing, the Data Processor shall assist the Data Controller, at the Data Controller`s costs, to ensure Data Controller`s compliance with the obligations pursuant to the Applicable data protection laws by providing information requested by the Data Controller;

3.6.3. With regard to unlikely security breach the Data Processor shall inform the Data Controller without undue delay after becoming surely aware of any security breaches concerning Personal Data Processed under this Agreement.

4. Instructions for Processing

4.1. The Personal Data under this Agreement shall be Processed in order to provide Services to the Data Controller as per the Terms. The nature, purpose, subject matter and other details of Processing activities performed as part of the Services are set out in the Annex I of this Agreement.

5. Personal Data disclosure

5.1 The Data Processor undertakes not to disclose any Personal Data Processed to any third party, other than through the use of Sub-processors as specified in this Agreement, except if the Personal Data is disclosed under third parties' request of information in accordance with applicable legal acts or under legitimate requests from law enforcement or other competent authorities.

5.2 The Data Controller authorizes the Data Processor to use Sub-processors to fulfil its obligations as set forth in this Agreement (provides general authorization) provided that the Data Processor maintains a list of Sub-processors and, upon receiving a written request from the Data Controller, provides the Data Controller with such list. In case of a new Sub-processor, the Data Processor will inform the Data Controller thereof. The Data Processor shall enable the Data Controller to object, by way of providing the Data Processor with a reasoned, specific and written objection, to changes concerning the addition or replacement of Sub-processors to the afore-mentioned list.

5.3 The Data Processor shall ensure that Sub-processors assume similar obligations in writing as those agreed in this Agreement. Data Processor remains fully liable to the Data Controller for the performance of its Sub-processors' data protection obligations where the Sub-processors fail to fulfil such obligations.

6. Transfer to third countries

6.1. The Data Processor is allowed to transfer the Personal Data to a country outside the EEA as reasonably necessary to provide the Services, provided that the Data Processor ensures an adequate level of protection and complies with other obligations to which it is subject pursuant to this Agreement.

6.2. Where the Parties are required to enter into the SCC under the Applicable data protection laws, the SCC shall be hereby incorporated by this reference to this Agreement as legally binding and duly executed agreement between the Parties, and:

6.2.1. Data Controller shall be considered as the ‘data exporter’ and Data Processor shall be considered as the ‘data importer’;

6.2.2. Parties select "MODULE TWO: Transfer controller to processor" as an applicable module for the relationship under the Terms and the Agreement;

6.2.3. Parties include the optional Docking clause in the SCC. The parties transferring Personal Data to, or receiving Personal Data from the new party shall undertake the obligations of data importer or data exporter, as applicable, in relation to the new party;

6.2.4. Parties select OPTION 2: GENERAL WRITTEN AUTHORISATION for the use of Sub-processors in clause 9 of the SCCs and formulate it as follows: "The data importer has the data exporter's general authorization 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 20 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";

6.2.5. the parties agree that Dutch Data Protection Authority shall be the competent supervisory authority for matters related to Personal Data transfers to third countries in accordance to this Agreement. In all cases where the SCCs require to specify country or a Member State (especially in clauses 17 and 18) parties agree to use the Netherlands as their primary selection;

6.2.6. Annex I of the Agreement shall be considered as Annex I and II to the SCCs.

7. Personal Data security principles

7.1. In order to assist the Data Controller in complying with legal obligations, including but not limited to the implementation of adequate Personal Data security measures, the Data Processor shall take appropriate technical and organizational measures to protect the Personal Data. The measures shall ensure an adequate level of security, taking into account:

7.1.1. particular risks associated with the Processing of Personal Data;

7.1.2. costs of the measures;

7.1.3. existing technical capabilities.

7.2 Data Processor shall implement sufficient technical and organization means to ensure the security level consistent with risks, including, where appropriate:

7.2.1. the ability to ensure the continuing integrity, availability and resilience of systems and services of Personal Data Processing;

7.2.2. the possibility to restore conditions and access to Personal Data in a timely manner in case of a physical or technical incident;

7.2.3. regular assessment of the efficiency of technical and organizational measures to ensure the security, verification, evaluation and performance of the Processing of Personal Data.

7.3 The Data Processor shall ensure that Sub-processors authorized to Process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

8. Processing of the Persons` requests

8.1. Data Controller shall process and respond to every Person's inquiry or request for exercising its rights under the Applicable data protection laws, including but not limited to an access to information held on the Person, and requests to delete or correct the Personal Data or restrict the Processing related to the Person.

8.2. Every Person's inquiry or request for exercising their rights directly addressed to the Data Processor shall be forwarded by the Data Processor to the Data Controller.

8.3. When the Data Controller is not able to exercise Person's rights, the Data Controller may ask the Data Processor for assistance in providing the information related to the Processing of the Personal Data under this Agreement.

9. Right to carry out an audit

9.1. When reasonably necessary, the Data Controller shall have the right to take the measures to verify the Data Processor's compliance with the terms of this Agreement. The Data Controller shall have a right to request for an audit performed by the independent, accredited and reputable third party audit firm agreed by both Parties.

9.2. This audit will only take place where there is a specific and well-founded suspicion of misuse of Personal Data, and only after the Data Controller has requested and assessed similar existing reports from the Data Processor and has made reasonable arguments to justify an audit being initiated by the Data Controller. Such an audit is justified if the similar reports that the Data Processor has available provide insufficient, or inconclusive answers regarding compliance with this Agreement by the Data Processor.

9.3. For the avoidance of doubt, neither Data Controller nor appointed auditor shall be a competitor of Data Processor`s business and, under no circumstances may the Data Controller, or the selected auditor, have access to Data Processor`s confidential information, information of Data Processor's other clients, nor to any information of third-parties to whom the Data Processor owes a duty of confidentiality.

9.4. Any such audit conducted by the Data Controller shall take place during regular business hours in a manner that is not disruptive to the Data Processor`s business, upon reasonable no less than 2-month advance notice to the Data Processor and subject to maximum capacity of confidentiality undertaking as provided below. Data Controller is responsible for all costs and fees related to such audit, including all costs and fees for any and all time Data Processor expends for any such audit, in addition to the rates for support services performed by the Data Processor and any expenses incurred by the Data Processor. Before the commencement of any such audit, the Parties shall mutually agree upon the timing, duration and scope of the audit, which shall not involve physical access to the servers from which the Data Processing Services are provided. The Data Controller shall promptly notify the Data Processor regarding any non-compliance discovered during the course of an audit. The Data Controller may not audit the Data Processor more than once annually.

9.5. Information discovered in the course of an audit shall be treated as "Confidential information" and shall be subject to the 'Confidentiality" Section of the Terms.

10. Term

10.1 This Agreement shall apply for the whole term the Data Processor Processes Personal Data on behalf of Data Controller.

10.2 Following termination of the Agreement, Data Processor shall delete or return to Data Controller the Personal Data as provided in the Terms. Personal Data shall be deleted or otherwise made unrecoverable and/or anonymized, other than such copies, as authorized under the Terms or this Agreement, or required to be retained in accordance with applicable laws.

11. Reimbursement

11.1. The Data Processor shall have the right to any reimbursement of reasonable expenses, costs and fees which were incurred as a result of Data Controller`s inaccurate, incomplete or unlawful instructions or as a result of absence of the Data Controller`s instructions.

12. Liability

12.1. The Data Processor's liability, taken together in the aggregate, arising out of or related to this Agreement, whether contractual, tort, or under any other theory of liability, shall be subject to the limitations and exclusions set out in the Terms. Liability of the Data Processor shall mean the aggregate liability of Data Processor under the Terms and this Agreement together.

13. Other Provisions

13.1. All notices between the Parties shall be given following the provisions of the Terms.

13.2. This Agreement shall be governed and any disputes or claims arising from this Agreement shall be settled according to the provisions of the Terms.

13.3. In case of any discrepancies between this Agreement, Terms and any other contracts which regulate data protection matters between the Parties, the provisions of this Agreement shall prevail over any other contractual provisions.

ANNEX I

Description and Instructions for Processing

Purposes and nature of Processing	To provide Services to the Data Controller as provided in the Terms or as instructed by the Data Controller.
Data subject categories	Data Controller's employees, customers and other persons (who are natural persons) authorized by the Data Controller.
Categories of Personal Data	Data Processor processes information related to the use of the Service, such as basic organization contact information, account registration and login information, user e-mails, information on user roles and status, invites, referrals, password status and health, breach information, basic device information (e.g., device name, device id, IP address, OS, platform), activity and email logs, authentication attempts, metadata about items in the vault (e.g., deleted at, last used at, type, pending shares, access rights), application diagnostics, other information as may be requested by the Data Controller.
Duration and frequency of Processing	The Processing is performed on a continuous basis for the period of providing the Services to the Data Controller.
Subject matter, nature and duration of the processing by Sub-Processors	The Sub-processors are an integral part of the Services provided to the Data Controller. The Sub-processors are used in all stages of providing the Service and the Personal Data is Processed for as long as it is needed to provide the Service.
Description of the technical and organisational measures implemented by the Data Processor	**Control of Assets in Server Infrastructure** • Company's information is kept in secure and physically inaccessible, encrypted servers. • Company performs data center security assessment before onboarding a new vendor. • All infrastructure is protected by firewalls and other security measures. **Vulnerability Assessment and Remediation** • Security of customer data is ensured by in-house security team and outside consultants that perform periodic penetration tests for Company's websites and applications. • Regular automated vulnerability assessments are made and remediation actions are taken. **Access Management** • Access to personal data is granted only to persons, who require personal data to carry out their functions (on need-to-know basis). • ACL software used for fraud detection and prevention, and risk management. This helps to ensure that only the right people have access to sensitive information. • Company uses VPN and secure jumpboxes to access the network infrastructure from remote locations. • Admin level privileges to Company's infrastructure are restricted to only a limited number of employees. • Company uses configuration management software that automates cloud provisioning, configuration management, application deployment, intra-service orchestration, and other IT needs. The software has a role-based access control engine that allows the Company to easily set policies on who can run what automation in what environments, ensuring

	that only the proper people have the ability to access machines and apply configuration. • Company monitors its employees' accounts to remove accounts that are irrelevant or inactive. **Data Recovery Capability** • In case of any failures, it is possible to restore personal data and critical information from back-up copies. Back-up copies are encrypted, and data is regularly recorded to data files in different physical places outside the Company's premises. **Control of Software and Hardware Assets** • Company maintains employee device inventory and is able to detect and block any rogue devices. • Computers provided to employees by the Company have mobile device management systems installed that ensure security of the equipment, appropriate and timely update of software as well as safe destruction of the data in an event of losing the equipment. • Authorized employees are responsible for the security of Company's devices – installing and updating anti-virus, firewall, as well as other security measures. • Data Processor requires the use of unique user IDs, strong passwords, two factor authentication in the majority of applications and carefully monitored access lists to minimize the potential for unauthorized account use. Majority of systems containing Personal data are accessible to employees only through whitelisted IP addresses. • Employees access the network via encrypted tunnels (VPN). Company also uses client isolation that prevents a device that is connected to the network by a wireless connection from accessing resources that are connected to the network by a wired connection. • Software and firmware updates are regularly taken. Identified critical vulnerabilities are remediated immediately. **Physical Security** • Company's premises are accessible only by persons authorized by the Company. Guests, partners and clients when entering main premises of the Company are registered and must sign non-disclosure agreements. All premises of the Company are accessed by third persons only with the escort of the Company employees. • Company's employees access premises only with key cards that collect information on their use. All premises have operating alarm systems monitored by security companies. • To ensure that Company's premises are accessed only by authorized persons, Company carries out video surveillance of entrance points and passageways. • Company's employees must store documents and data files properly, in a secure manner and refrain from making unnecessary copies. Sensitive paper documents are stored in lockers or safes.
The technical and organisational measures to be taken by Sub-processors	The Data Processor implements organisational measures to ensure that security practices upheld by its Sub-processors are not less protective than those provided in the Agreement with respect to the protection of Personal

	Data (to the extent applicable depending on the nature of the services provided by a Sub-processor).