

DATA PROCESSING AGREEMENT

Last updated: November 3, 2022

NB! Starting from January 1, 2023, the provider of NordPass Business and NordLocker Business Services changes from nordvpn s.a. (address: PH F&F TOWER, 50th Street & 56th Street, Suite #32-D, Floor 32, Panama City, Republic of Panama) to Nord Security Inc. (address: One Rockefeller Plaza, 11th Floor, New York, NY 10020, United States of America). The current provider, nordvpn s.a., will cease to provide the mentioned Services on December 31, 2022.

By acquiring Services on or after the date indicated by “Effective from” above, Customers explicitly agree and consent to the change of the contracting party on Nord’s side from nordvpn s.a. to Nord Security Inc. and instruct the current data processor nordvpn s.a. to transfer Customers’ Personal Data to the new data processor Nord Security Inc. for further provision of Services, as of January 1, 2023, without any additional notice.

Customers that acquired Services before the date indicated by “Effective from” above have to provide their consent to the mentioned change of contracting party until December 27, 2022, in order to continue using Services after January 1, 2023. If the Customer does not timely provide its consent, the Customer’s (and its end users) access to the Services will be terminated from January 1, 2023 (with the right to request a refund for the unused part of the current Subscription Period by contacting customer support until January 31, 2023).

This Data Processing Agreement (“**DPA**”) is an integral part of the [Terms of Service](#) of Nord Services (“**Terms**”) concluded between the Customer and Nord (hereinafter collectively referred to as the “**Parties**”). The main purpose of this DPA is to define how Nord processes data on behalf and under the Customer’s instructions while providing the Services.

1. DEFINITIONS

- 1.1. Unless expressly stated in this DPA, the capitalized terms shall have the meanings indicated below:

Personal Data means any information relating to an identified or identifiable natural person (“**data subject**”); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Customer’s Personal Data means all Customer’s personal data in whatever form or medium which is (i) supplied to, or in respect of which access to the Nord is granted by the Customer or otherwise in connection with the [Terms](#), or (ii) produced or generated by or on behalf of the Customer in connection with the [Terms](#).

EEA means the European Economic Area.

Data Laws	Protection	means all applicable worldwide legislation relating to data protection and privacy which applies to the respective Party in the role of processing Personal Data in question under this DPA, including, without limitation, European data protection laws: (i) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (hereinafter, the “ GDPR ”); (ii) Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector; and (iii) applicable national implementations of (i) and (ii); (iii) the GDPR as it forms parts of the United Kingdom domestic law by virtue of Section 3 of the European Union (Withdrawal) Act 2018 (hereinafter, the “ UK GDPR ”); regulations of the United States of America, including the California Consumer Privacy Act of 2018, Cal. Civ. Code §1798.100 et. seq., and its implementing regulations (hereinafter, the “ CCPA ”), applicable to the processing of the Personal Data (or an analogous variation of such term); other applicable data protection and privacy laws.
SCCs		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 updated or replaced from time to time. The current version of the SCCs (i.e., applicable at the time of the conclusion of this DPA) is available at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj .
UK SCCs		means an International Data Transfer Addendum to the SCCs approved by the UK as updated or replaced from time to time. The current version of the Addendum to the SCCs (i.e., applicable at the time of the conclusion of this DPA) is available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance/ .

- 1.2. The following lower-case terms used but not defined in this DPA, such as “**controller**”, “**processor**”, “**sub-processor**”, “**processing**”, “**special categories of personal data**”, “**personal data breach**” and “**supervisory authority**” shall have the same meaning as set forth in the GDPR, irrespective of whether the GDPR applies.
- 1.3. Terms and expressions used in this DPA and not defined herein have the meaning assigned to them in the [Terms](#).

2. APPLICATION OF THIS DPA

- 2.1. This DPA applies when Nord processes the Customer’s Personal Data in order to provide Services under the [Terms](#). Nord, as defined in this DPA, acts as the data processor, whereas the Customer acts as the data controller.
- 2.2. The nature, purpose, subject matter, and other details of processing activities performed as part of the Services are set out in Annex I of this DPA.

3. GENERAL OBLIGATIONS

- 3.1. Nord warrants and undertakes to process the Customer’s Personal Data only for the limited and specified purposes set out in the [Terms](#) and/or as otherwise lawfully instructed by the Customer in writing (as specified in the [Terms](#)) and mutually agreed by the Parties, except where otherwise required by the Data Protection Laws. Nord will not process the Customer’s Personal Data for any other purpose or in a way that does not comply with this DPA or the Data Protection Laws.

- 3.2. The Customer's initial instructions to Nord are set forth in this DPA and its Annex I. All the instructions provided are comprehensive and reflect the Customer's will.
- 3.3. Nord shall not evaluate any instructions of the Customer, 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 Nord's reasonable opinion, an instruction undoubtedly infringes the applicable Data Protection Laws, Nord shall notify the Customer. Nord is not responsible for compliance with any Data Protection Laws applicable to the Customer or its industry that are not generally applicable to Nord.
- 3.4. Nord shall not take any action that would cause the Customer to violate the Data Protection Laws.
- 3.5. In particular but without prejudice to the generality of the foregoing, the Customer acknowledges and agrees that it will be solely responsible for: (i) the accuracy, quality, and legality of the Customer's Personal Data and the means by which it acquired Personal Data; (ii) complying with all necessary transparency and lawfulness requirements under applicable Data Protection Laws for the collection and use of the Personal Data, including any necessary notifications, consents, and authorizations that are needed for the Customer's use of Nord's Services; (iii) ensuring it has the right to transfer, or provide access to, the Personal Data to Nord for processing in accordance with the provisions of the [Terms](#) (including this DPA); and (iv) ensuring that its instructions to Nord regarding the processing of Personal Data comply with applicable laws, including Data Protection Laws. The Customer shall also inform Nord without undue delay if the Customer is not able to comply with its responsibilities under this Section.

4. Data Disclosure

- 4.1. Nord undertakes not to disclose the Customer's Personal Data to any third party other than through the use of other data processors as specified in this DPA, 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.
- 4.2. To the fullest extent permissible under the Data Protection Laws, the Customer authorizes Nord to use sub-processors to fulfill its obligations as set forth in this DPA (provides general authorization) provided that Nord maintains a list of sub-processors and, upon receiving a written request from the Customer, provides the Customer with such list.
- 4.3. Nord shall: (i) ensure that any sub-processor is contractually bound in writing to provide at least the same level of protection as is required by this DPA and complies with the Data Protection Laws; (ii) be fully responsible and liable to the Customer for acts and omissions of any sub-processor as if they were Nord's own act or omission.
- 4.4. If required to do so by applicable Data Protection Laws, in case of a new sub-processor: (i) Nord will inform the Customer thereof; and (ii) Nord shall enable the Customer to object, by way of providing Nord with a reasoned, specific and written objection, to changes concerning the addition or replacement of sub-processors to the afore-mentioned list.

5. Data Transfers

- 5.1. The Customer shall transfer the Customer's Personal Data in accordance with the requirements of Data Protection Laws applicable to the Customer.
- 5.2. The Customer acknowledges and agrees that Nord may access and process the Customer's Personal Data on a global basis as necessary to provide the Services in accordance with the [Terms](#).
- 5.3. The Customer's Personal Data from EEA, or UK may only be exported to or accessed by Nord or its sub-processors outside the EEA or the UK ("**European Transfer**"), as applicable:

5.3.1. if the recipient or the country/territory in which it processes or accesses the Customer's Personal Data ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of Personal Data as determined by the European Commission or another regulatory body of competent jurisdiction ("**Adequacy Decision**"); or

5.3.2. in the absence of an Adequacy Decision, the European Transfer only can take place in accordance with Annex II of this DPA.

6. Data Security

6.1. Nord shall make sure to take appropriate technical and organizational measures (hereinafter, the "**TOMs**") to protect the processed Customer's Personal Data. The TOMs must ensure an adequate level of security, taking into account:

6.1.1. context, objectives, and particular risks associated with the processing of Personal Data;

6.1.2. the risks to the rights and freedoms of data subjects arising from the processing of Personal Data;

6.1.3. existing Nord's technical capabilities; and

6.1.4. costs of the measures or their implementation.

6.2. Nord must ensure that the TOMs used to protect the Customer's Personal Data include the following measures/requirements where appropriate:

6.2.1. the ability to ensure the ongoing confidentiality, integrity, availability, and resilience of systems and services of the Customer's Personal Data processing;

6.2.2. the ability to restore the availability and access to the Customer's Personal Data in a timely manner in the event of a physical or technical incident;

6.2.3. regular assessment of the efficiency of TOMs to ensure the security of the processing of Personal Data.

6.3. Nord shall also ensure that sub-processors authorized to process the Customer's Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

6.4. The list of the current Nord's TOMs used to protect the Customer's Personal Data is set out in full in Annex I of this DPA. Notwithstanding any provision to the contrary, Nord may modify or update the TOMs at its discretion provided that such modification or update does not result in a material degradation in the protection offered by the current TOMs.

6.5. Nord, having become aware of any personal data breach affecting the Customer's Personal Data shall: (i) report the breach to the Customer without undue delay, after becoming surely aware of the personal data breach; (ii) make reasonable efforts to assist the Customer in fulfilling its obligation under applicable Data Protection Laws to notify a relevant supervisory authority and/or data subjects about such personal data breach. For the avoidance of doubt, Nord will not notify and/or disclose any information relating to the personal data breach to any third party, including but not limited to data subjects and supervisory authority, unless required to do so by Data Protection Laws.

7. COOPERATION AND DATA SUBJECTS RIGHTS

7.1. The Customer shall process and respond to every enquiry, request, notice, question, complaint or other communication related to the processing of the Customer's Personal Data under this DPA ("**Request**") received from: (i) any natural person whose Personal Data is processed by Nord on behalf of the Customer or (ii) any supervisory authority.

- 7.2. When the Customer is not able to solely process and respond to the Request, the Customer may ask Nord for reasonably required assistance (subject to the nature of the processing and the information available to Nord) to enable the Customer to:
- 7.2.1. comply with (and demonstrate compliance with) its obligations under the Data Protection Laws (including, but not limited to data protection impact assessments, reporting to and consulting with supervisory authorities); and
 - 7.2.2. respond to, comply with, or otherwise resolve the Request. In the event that any such Request under this Section is made directly to Nord, Nord shall promptly inform the Customer by providing full details of such Request. For the avoidance of doubt, Nord will not respond to any Requests, unless Nord is legally compelled to do so.

8. RIGHT TO CARRY OUT AN AUDIT

- 8.1. When reasonably necessary, the Customer shall have the right to take the measures necessary to verify Nord's compliance with this DPA.
- 8.2. The Customer shall also have a right to request an audit performed by the independent, accredited, and reputable third-party audit firm agreed by both Parties. For the avoidance of doubt, neither the Customer nor the appointed auditor shall be a competitor of Nord's business and, under no circumstances may the Customer, or the selected auditor, have access to Nord's confidential information, information of Nord's other clients, nor to any information of third parties to whom Nord owes a duty of confidentiality. Before conducting the audit, the Customer and auditor must execute a written confidentiality agreement acceptable to Nord or otherwise be bound by a statutory confidentiality obligation.
- 8.3. This audit will only take place where there is a specific and well-founded suspicion of misuse of the Customer's Personal Data, and only after the Customer has requested and assessed similar existing reports from Nord and has made reasonable arguments to justify an audit being initiated by the Customer. For the avoidance of doubt, such an audit can be justified only if similar reports (that Nord has available) provide insufficient or inconclusive answers regarding compliance with this DPA by Nord.
- 8.4. An audit shall take place during regular business hours in a manner that is not disruptive to Nord's business, upon reasonable no less than two (2) month advance notice to Nord (unless mandatory applicable Data Protection Laws or the supervisory authority requires a shorter notice) and subject to a maximum capacity of confidentiality undertaking as provided below. Before the commencement of any such audit, the Parties shall mutually agree upon the timing, duration, and scope of an audit, which shall not involve physical access to the servers from which the Customer's Personal Data processing is provided.
- 8.5. The Customer shall notify Nord regarding any non-compliance discovered during the course of an audit. The Customer may not audit Nord more than once during any consecutive twelve (12) month period. The Customer is responsible for all costs and fees related to such audit, including all costs and fees for any and all time Nord expends for any such audit.
- 8.6. All 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](#).

9. TERM

- 9.1. This DPA shall apply as long as the Services are provided to the Customer as set out in the [Terms](#) unless the Parties terminate the [Terms](#) and/or this DPA earlier on the grounds provided therein.
- 9.2. Following termination of the DPA, Nord shall delete or return the Customer's Personal Data to the Customer at its choice. The Customer's Personal Data shall be deleted as determined in the [Terms](#).

10. LIABILITY

- 10.1. Nord's liability, taken together in the aggregate, arising out of or related to this DPA, 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 Nord shall mean the aggregate liability of Nord under the [Terms](#) and this DPA together.

11. OTHER PROVISIONS

- 11.1. All notices between the Parties shall be given following the provisions of the [Terms](#).
- 11.2. Nord shall have the right to any reimbursement of reasonable expenses, costs, and fees which were incurred as a result of Customer's (i) inaccurate, incomplete, or unlawful instructions; and/or (ii) requests for cooperation which are unfounded, excessive, and/or impose unreasonably disproportionate costs to Nord.
- 11.3. This DPA shall be governed and any disputes or claims arising from this DPA shall be settled according to the provisions of the [Terms](#).
- 11.4. Notwithstanding anything to the contrary in the [Terms](#), in the event of any conflict or inconsistency between the terms of this DPA and the [Terms](#), the provisions of this DPA shall prevail.

ANNEX I

Description and Instructions for Processing

Purpose and nature of the processing	To provide the Services to the Customer as provided in the Terms or as instructed by the Customer.	
Categories of the data subjects	Customer's end users of the Services, including Customer's employees, representatives, contractors, customers, and any other natural persons that are authorized by and/or receive access to the Services through the Customer.	
Categories of the Personal Data	NordPass Business	NordLocker Business
	Basic organization contact information, account registration and login information, user emails, information on user roles and status, invites, referrals, passwords' status, health and 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.	Basic organization contact information, account registration and login information, user emails, information on user roles and status, invites, referrals, 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.
Duration and frequency of the processing	The processing is performed on a continuous basis for the period of providing the Services to the Customer.	
The subject matter, nature, and duration of the processing by sub-processors	Sub-processors are an integral part of the Services provided to the Customer. Sub-processors are used in all stages of providing the Service and the Customer's Personal Data is processed for as long as it is needed to provide the Service.	

<p>Description of the TOMs implemented by Nord</p>	<p>Control of Assets in Server Infrastructure</p> <ul style="list-style-type: none"> • Nord's information is kept in secure and physically inaccessible, encrypted servers located in different places around the world. • All regular servers are discless (RAM servers). These allow to create a centrally controlled network where nothing is stored locally. • Nord performs a data center security assessment before onboarding a new vendor. • All infrastructure is protected by firewalls and other security measures. <p>Vulnerability Assessment and Remediation</p> <ul style="list-style-type: none"> • Security of the Customer's Personal Data is ensured by security professionals and outside consultants that perform periodic penetration tests for Nord's websites and applications. <p>Access Management</p> <ul style="list-style-type: none"> • Security, management, and control of access to information are ensured. Access to the Customer's Personal Data is granted only to persons, who require the Customer's Personal Data to carry out their functions (on need-to-know basis). • Nord uses secure jump boxes to access the network infrastructure from remote locations. • Admin level privileges to Nord's infrastructure are restricted to only a limited number of employees. • Nord 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 Nord 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 the configuration. <p>Data Recovery Capability</p> <ul style="list-style-type: none"> • In case of any failures, it is possible to restore the Customer's Personal Data and critical information from back-up copies (if applicable). Back-up copies are encrypted, and data is regularly recorded to data files in different physical places outside Nord's premises. <p>Control of Software and Hardware Assets in HR</p> <ul style="list-style-type: none"> • Nord maintains employee device inventory and is able to detect and block any rogue devices. • Nord maintains employee software inventory and is able to detect unauthorized software. • Computers provided to employees by Nord have mobile device management systems installed that ensure the
---	--

	<p>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.</p> <ul style="list-style-type: none"> • Authorized employees are responsible for the security of Nord's devices – installing and updating anti-virus, firewall, as well as other security measures. • Nord 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 use. The majority of systems containing the Customer's Personal Data are accessible to employees only through whitelisted IP addresses. • All new employees undergo training on information security awareness. <p>Physical Security</p> <ul style="list-style-type: none"> • Nord's premises are accessible only by persons authorized by Nord. • Nord's employees access premises only with key cards that collect information on their use. All premises have operating alarm systems. • To ensure that Nord's premises are accessed only by authorized persons, Nord carries out video surveillance of entrance points and passageways. • Nord'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 TOMs to be taken by sub-processors	<p>Nord implements technical and organizational measures to ensure that security practices upheld by its sub-processors are not less protective than those provided in the DPA with respect to the protection of the Customer's Personal Data (to the extent applicable depending on the nature of the services provided by a sub-processor).</p>

ANNEX II

The SCCs and European Transfers Agreement

1. **EEA Transfers.** In relation to the Customer's Personal Data that is subject to the GDPR: (i) the Customer is the "**data exporter**" and Nord is the "**data importer**"; (ii) the relevant provisions contained in the SCCs are incorporated by reference and are an integral part of this DPA - the **Module Two** terms apply to the extent the Customer is a Controller of Personal Data; (iii) in Clause 7, the optional docking clause applies; (iv) in Clause 9, Option 2 applies and the time period for prior notice of sub-processor changes shall be ten (10) calendar days; (v) in Clause 11, the optional language is deleted; (vi) in Clauses 17 and 18, the Parties agree that the governing law and forum for disputes for the SCCs will be the Netherlands; (vii) the Annexes of the SCCs will be deemed completed with the information set out in Annex I of the DPA; and (viii) if and to the extent the SCCs conflict with any provision of this DPA the SCCs will prevail to the extent of such conflict.
2. **UK Transfers.** In relation to the Customer's Personal Data that is subject to the UK GDPR, the SCCs will apply in accordance with sub-section (a) and the following modifications: (i) the SCCs will be modified and interpreted in accordance with the UK SCCs, which will be incorporated by reference and form an integral part of the DPA; (ii) Tables 1, 2 and 3 of the UK SCCs will be deemed completed with the information set out in Annex I of the DPA and Table 4 will be deemed completed by selecting "neither party"; and (iii) any conflict between the terms of the SCCs and the UK SCCs will be resolved in accordance with Section 10 and Section 11 of the UK SCCs.

ANNEX III

CCPA Data Protection Addendum

1. This CCPA Data Protection Addendum (“**Addendum**”) reflects the requirements of the CCPA and is in effect for so long as Nord maintains Personal Information (as defined in and to the extent protected by the CCPA) provided by the Customer or which is collected on behalf of the Customer by Nord (“**Personal Information**”).
2. This Addendum prevails over any conflicting terms of the [Terms](#) or DPA but does not otherwise modify the [Terms](#) or DPA.
3. The following terms used but not defined in the DPA or this Addendum, such as “**Business**”, “**Service Provider**”, “**Business purpose**”, “**Consumer**” and “**Third party**” will have the same meaning as set forth in the CCPA.
4. **Scope and Applicability of this Addendum**
 - 4.1. This Addendum shall only apply and bind the Parties if and to the extent the Customer is the Business and the Customer appoints Nord as the Service Provider to process the Personal Information on behalf of the Customer.
 - 4.2. This Addendum applies to the collection, retention, use, and disclosure of the Personal Information to provide the Services to the Customer pursuant to the [Terms](#) or to perform a Business purpose.
 - 4.3. Nord’s collection, retention, use, or disclosure of Personal Information for its own purposes independent of providing the Services specified in the [Terms](#) are outside the scope of this Addendum.
5. **Restrictions on Processing**
 - 5.1. Nord is prohibited from retaining, using, selling or disclosing the Personal Information for any purpose other than for the specific purpose of performing the Services specified in the [Terms](#) for the Customer, as set out in this Addendum, or as otherwise permitted by the CCPA.
6. **Consumer Rights**
 - 6.1. If Nord, directly or indirectly, receives a request submitted by a Consumer to exercise a right they have under the CCPA in relation to that Consumer’s Personal Information, it will provide a copy of the request to the Customer.
 - 6.2. Nord shall provide reasonable assistance to the Customer in facilitating compliance with Consumers rights requests.
 - 6.3. Upon direction by the Customer and within a commercially reasonable amount of time, Nord shall delete the Personal Information.
7. **No Sale of Personal Information**
 - 7.1. The Parties acknowledge and agree that the exchange of Personal Information between the Parties does not form part of any monetary or other valuable consideration exchanged between the Parties with respect to the [Terms](#), the DPA, or this Addendum.