Data Processing Agreement

Personal data processed by Nord Node on behalf of its customers (Article 28 GDPR)

Version 1.0 · Effective: 24 September 2026

This document forms part of the Agreement between Nord Node AB and the Customer. It applies where an Order Form has been signed and does not apply to use of Nord Node's website.

1. Background and scope

1.1 This Data Processing Agreement (the **"DPA"**) forms part of the Agreement between Nord Node AB, reg. no. 559493-4936 (**"Nord Node"** or the **"Processor"**), and the Customer (the **"Controller"**). It applies whenever Nord Node processes personal data on the Customer's behalf when providing the Services.

1.2 This DPA meets the requirements of Article 28(3) of Regulation (EU) 2016/679 (the **"GDPR"**) and applies together with the Swedish Act containing supplementary provisions to the GDPR (lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning).

1.3 This DPA does not apply to personal data that Nord Node processes as a controller for its own purposes, such as customer relationship management, invoicing and its own security logging. That processing is described in Nord Node's Privacy Policy.

2. Definitions

2.1 Terms such as "personal data", "processing", "controller", "processor", "data subject", "personal data breach" and "supervisory authority" have the meanings given in Article 4 of the GDPR. **"Data Protection Law"** means the GDPR and supplementary national legislation applicable to the processing. **"Sub-processor"** means another processor engaged by Nord Node to process Customer personal data. Other terms have the meanings given in the General Terms of Service.

3. Roles and the Customer's responsibilities

3.1 The Customer is the controller, and Nord Node is the processor, of the personal data described in Annex 1. Where the Customer is itself a processor for another controller, Nord Node acts as the Customer's sub-processor, and the Customer is responsible for ensuring that its instructions are consistent with the instructions of that controller.

3.2 The Customer is responsible for ensuring that the processing it instructs Nord Node to carry out has a lawful basis, that data subjects have been informed as required, and that the personal data it provides has been collected lawfully.

3.3 The Customer's own agreements with Vendors of Third-Party Services, such as the Microsoft Customer Agreement and Microsoft's Products and Services Data Protection Addendum, govern the Vendor's processing of personal data in the Customer's own cloud tenant. When Nord Node administers such a tenant, Nord Node is a processor only in respect of its own administrative access and activities.

4. Instructions

4.1 Nord Node will process the personal data only on the Customer's documented instructions, including with regard to transfers to third countries, unless Union or Member State law to which Nord Node is subject requires otherwise. In that case, Nord Node will inform the Customer of the legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

4.2 The Customer's instructions at the date of this DPA are set out in the Agreement, including this DPA and Annex 1. The Customer may give additional or changed instructions in writing through an Authorised Contact. If new instructions change the scope or cost of the Services, section 4.2 of the General Terms applies.

4.3 Nord Node will inform the Customer immediately if, in its opinion, an instruction infringes Data Protection Law. Nord Node may suspend the relevant processing until the Customer confirms or changes the instruction.

5. Confidentiality and personnel

5.1 Nord Node will ensure that persons authorised to process the personal data are bound by confidentiality, either contractually or by law, and receive appropriate training in data protection and information security.

5.2 Nord Node will limit access to the personal data to personnel who need it to provide the Services.

6. Security

6.1 Nord Node will implement and maintain the technical and organisational measures described in Annex 2 to ensure a level of security appropriate to the risk, in accordance with Article 32 of the GDPR.

6.2 Nord Node may update the measures in Annex 2 over time to reflect technical developments, provided that the updates do not reduce the overall level of protection.

6.3 The Customer is responsible for the security of the parts of the Customer Environment that Nord Node does not manage, and for assessing whether the measures in Annex 2 are appropriate for its processing.

7. Sub-processors

7.1 The Customer gives Nord Node general authorisation to engage Sub-processors. The Sub-processors engaged on the date of this DPA are set out in Annex 3. The Sub-processors engaged at any time, including their names, the processing they carry out, the location of processing and any transfer mechanism, are set out in Nord Node's Sub-processor List, which Nord Node keeps up to date and provides to the Customer on request.

7.2 Nord Node will notify the Customer at least 30 days before engaging a new Sub-processor or replacing one, by e-mail to the Customer's Authorised Contact or through another agreed channel. The notice will state the Sub-processor's name, location, the processing it will carry out, and the transfer mechanism, if any.

7.3 The Customer may object to the change on reasonable data protection grounds by written notice within the notice period. The Parties will then discuss the objection in good faith. If Nord Node cannot offer a reasonable alternative, the Customer may terminate the affected Services with effect from the date on which the new Sub-processor would start processing the Customer's personal data, without paying any termination charges for the Managed Services concerned. Fees for Subscriptions remain payable in accordance with the Vendor's commitment terms.

7.4 In an emergency, such as the sudden failure of an existing Sub-processor, Nord Node may engage a replacement Sub-processor at shorter notice, and will notify the Customer as soon as possible. The Customer's right to object under section 7.3 still applies.

7.5 Nord Node will impose on each Sub-processor, by written contract, data protection obligations that provide at least the same level of protection as this DPA, in particular with regard to security. Nord Node remains fully liable to the Customer for the performance of its Sub-processors' obligations.

7.6 On request, Nord Node will provide the Customer with a copy of the relevant data protection terms of a Sub-processor, from which commercial information may be removed.

8. Transfers outside the EU/EEA

8.1 Nord Node will process and store the personal data within the EU/EEA, unless otherwise stated in Annex 3 or the Sub-processor List, or instructed by the Customer.

8.2 Nord Node will transfer personal data to a country outside the EU/EEA, or allow a Sub-processor to do so, only in compliance with Chapter V of the GDPR, for example:

(a) to a country, or a certified organisation, covered by an adequacy decision of the European Commission, such as the EU–US Data Privacy Framework; or

(b) on the basis of the European Commission's Standard Contractual Clauses (Implementing Decision (EU) 2021/914), together with an assessment of the laws of the recipient country and supplementary measures where necessary.

8.3 Where support or access from outside the EU/EEA is technically possible (for example, a Sub-processor's global support function), this is stated in Annex 3 and, for the individual Sub-processor concerned, in the Sub-processor List.

8.4 If an adequacy decision relied on under this section is invalidated, Nord Node will inform the Customer and will without undue delay implement another transfer mechanism or stop the transfer.

9. Assistance with data subjects' rights

9.1 Taking into account the nature of the processing, Nord Node will assist the Customer by appropriate technical and organisational measures in responding to requests from data subjects to exercise their rights under Chapter III of the GDPR.

9.2 If Nord Node receives a request directly from a data subject concerning the Customer's personal data, Nord Node will forward it to the Customer without undue delay and will not respond to it, other than to refer the data subject to the Customer, unless the Customer instructs otherwise.

10. Personal data breaches

10.1 Nord Node will notify the Customer without undue delay, and in any event within 48 hours, after becoming aware of a personal data breach affecting the Customer's personal data.

10.2 The notification will, to the extent the information is available, describe:

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

(b) the name and contact details of Nord Node's contact person;

(c) the likely consequences of the breach; and

(d) the measures taken or proposed to address the breach and mitigate its effects.

Where information is not available at the time of the first notification, Nord Node will provide it in phases without further undue delay.

10.3 Nord Node will take the measures reasonably necessary to contain the breach and limit its effects, and will assist the Customer with its obligations to notify the supervisory authority and data subjects under Articles 33 and 34 of the GDPR. The Customer is responsible for deciding whether to notify, and for making any notification.

10.4 Nord Node's notification or assistance is not an admission of fault or liability.

11. Impact assessments and prior consultation

11.1 Taking into account the nature of the processing and the information available to Nord Node, Nord Node will assist the Customer with data protection impact assessments and prior consultations with the supervisory authority under Articles 35 and 36 of the GDPR, as far as they relate to the Services.

12. Audits and information

12.1 Nord Node will make available to the Customer the information necessary to demonstrate compliance with Article 28 of the GDPR and this DPA, including a description of its security measures, relevant policies and any certifications or audit reports it holds.

12.2 If the Customer reasonably considers that the information provided is insufficient, or if a supervisory authority requires it, the Customer may carry out an audit, including an inspection, itself or through an independent auditor bound by confidentiality who is not a competitor of Nord Node. The Customer must give at least 30 days' notice, unless a shorter period is required by a supervisory authority or following a personal data breach. Audits may take place no more than once every 12 months, unless there has been a personal data breach or the supervisory authority requires it.

12.3 Audits must be carried out during normal working hours, without unreasonably disrupting Nord Node's operations, and without access to other customers' data or to Nord Node's confidential information that is not relevant to the Customer. Each Party bears its own costs. Nord Node may charge for time spent assisting with audits beyond one Business Day per year at its hourly rates, except where the audit reveals a material breach by Nord Node of this DPA.

12.4 Where an audit concerns a Sub-processor, Nord Node may satisfy the request by providing the Sub-processor's audit reports or certifications.

13. Requests from public authorities

13.1 If a public authority requests access to the Customer's personal data, Nord Node will refer the authority to the Customer and notify the Customer without undue delay, unless prohibited by law. Nord Node will disclose the data only if required by law and will limit the disclosure to what is required.

14. Return and deletion

14.1 When the Services end, Nord Node will, at the Customer's choice, return the personal data to the Customer or make it available for export in accordance with section 15 of the General Terms, and then delete it.

14.2 Nord Node will delete the personal data, including copies, within 60 days after the end of the export period in section 15.3 of the General Terms. Data in backups will be deleted as the backups expire in accordance with the normal backup cycle, and at the latest within 90 days after that deletion date. Until deletion, the data remains protected under this DPA.

14.3 Nord Node may retain personal data to the extent required by Union or Member State law. In that case, Nord Node will keep the data confidential and process it only for the purpose required by law.

14.4 On request, Nord Node will confirm the deletion in writing.

15. Liability

15.1 Liability between the Parties for breach of this DPA is governed by section 19 of the General Terms, including the increased limit in section 19.6.

15.2 Each Party is responsible for administrative fines imposed on it by a supervisory authority. Neither Party may seek to recover such fines from the other, except where a fine imposed on a Party has been caused by the other Party's breach of this DPA or Data Protection Law, in which case the amount recoverable is subject to section 15.1.

15.3 This section does not limit either Party's liability to data subjects under Article 82 of the GDPR. Where a Party has paid full compensation to a data subject, it may recover from the other Party the part of the compensation corresponding to that Party's share of responsibility, in accordance with Article 82(5) of the GDPR.

16. Records and cooperation

16.1 Nord Node maintains a record of the categories of processing activities carried out on behalf of the Customer in accordance with Article 30(2) of the GDPR.

16.2 Each Party will cooperate with the supervisory authority on request.

17. Costs of assistance

17.1 Assistance under sections 9, 11 and 12 that goes beyond what is normally included in the Services, and that is not caused by Nord Node's breach, may be charged at the hourly rates in the Order Form. Nord Node will inform the Customer of the expected cost in advance where possible. Assistance under section 10 in connection with a personal data breach caused by Nord Node is not charged.

18. Term and precedence

18.1 This DPA applies for as long as Nord Node processes personal data on the Customer's behalf, including after the Agreement ends until the data has been returned or deleted.

18.2 In matters concerning the processing of personal data, this DPA takes precedence over the other documents forming part of the Agreement.

18.3 This DPA is governed by Swedish law, and disputes are resolved in accordance with section 24 of the General Terms.

Annex 1 — Description of the processing

Item	Description
Subject matter and duration	Provision of the Services under the Agreement, for the term of the Agreement and until the personal data has been returned or deleted under section 14.
Nature and purposes	Administration, support, monitoring, maintenance and security management of the Customer Environment; service desk and ticket handling through the customer portal; endpoint management, patching and software deployment; identity and access administration; management of credentials used to administer the Customer Environment; endpoint and e-mail security; backup and restore where ordered; incident handling; migration and project work; procurement and provisioning of Third-Party Services and Hardware, as ordered in the Order Form.
Categories of data subjects	The Customer's employees, contractors and other Users; persons whose data is contained in the Customer's e-mail, files, systems and, where backup is ordered, backups (for example the Customer's own customers, suppliers and contacts); for schools and preschools, pupils and guardians where they are Users or appear in the Customer's data.
Categories of personal data	Identity and contact data (name, e-mail, phone, title, username); portal account data and ticket content, including descriptions, attachments and correspondence; account, authentication and access data (group membership, roles, MFA registration, sign-in logs); device and endpoint data (device name, serial number, IP address, logged-on user, installed software, configuration state, patch status, process and network telemetry where Tanium Threat Response or an equivalent module is ordered, location where enabled for lost devices); security alerts and investigation data; credentials used to administer the Customer Environment, held in an encrypted vault; content of e-mail, files and other data stored in the Customer Environment, to the extent Nord Node accesses it to perform a task or holds it in backups taken under an ordered backup module.
Special categories of data	Nord Node does not intend to process special categories of personal data (Article 9 GDPR) or data about criminal convictions (Article 10 GDPR) as such. Such data may, however, be contained in the Customer's e-mail, files, tickets and backups, which Nord Node may access only as described in section 10.2 of the General Terms. The Customer must inform Nord Node in the Order Form if its environment contains significant amounts of such data (for example health data, or data about children), so that appropriate additional measures can be agreed.
Processing operations	Storage, access, retrieval, copying (including backup where ordered), configuration, alteration, restoration, transfer between systems (migrations), restriction and erasure.
Location	EU/EEA, subject to Annex 3.
Retention	For the term of the Services and as set out in section 14; ticket records are retained for 24 months after closure unless the Customer instructs otherwise; backup retention as stated in the Order Form; Nord Node's logs of administrative activity in the Customer Environment are kept for 12 months.

Annex 2 — Technical and organisational security measures

Area	Measures
Governance	Documented information security policy approved by management and reviewed at least annually; designated person responsible for information security and data protection; risk assessment of new services and Sub-processors.
Personnel	Confidentiality undertakings for all personnel and subcontractors; background checks proportionate to the role, where permitted by law; security and data protection training on engagement and at least annually; access removed promptly when an engagement ends.

Area	Measures
Identity and access	Individual named accounts, no shared administrator accounts; phishing-resistant or app-based multi-factor authentication for all access to Nord Node systems, delivery platforms and Customer Environments; least-privilege and role-based access; privileged access granted just-in-time or time-limited where the platform supports it, and brokered through privileged access management where that module is in use; access reviews at least quarterly; break-glass accounts under the Customer's control.
Credential handling	Credentials used to administer the Customer Environment are held in an encrypted password vault with separate storage per Customer, protected by multi-factor authentication. The vault uses an architecture in which vault contents are encrypted on the device, so that the vault provider cannot read them. Credentials are never stored in tickets, e-mail, chat or documentation in plain text, and are rotated on personnel changes and on suspected compromise.
Endpoint management platform	Management agents are deployed only to devices covered by the Services. Administrative actions through the platform are logged and attributable to a named technician. Scripts and packages are reviewed before deployment to multiple devices. Platform administrator access is restricted to authorised personnel and protected by multi-factor authentication.
Remote access and remote support	Remote access only through tools approved by Nord Node. Remote control of a User's device requires the User to accept the session and can be ended by the User at any time; Nord Node does not use unattended remote control. Device configuration, security policies, software deployment and remote wipe are carried out through the management platforms, which record the actions taken. Every remote support session is recorded in the service ticket, stating the technician, the device, the time and the purpose.
Service desk platform	Tickets are stored in Nord Node's service management platform with separation between Customers, role-based access for Nord Node personnel, and portal accounts limited to the Users the Customer has authorised.
Endpoint and infrastructure security	Nord Node's own devices are managed, encrypted, patched and protected by endpoint detection and response; secure configuration baselines; security updates applied within the time frames in the Service Description.
Encryption	Encryption in transit (TLS 1.2 or higher) for all remote management, platform access and data transfer; encryption at rest for Nord Node devices, documentation repositories and, where a backup module is ordered, backup data.
Logging and monitoring	Logging of administrative activities in Nord Node's systems and delivery platforms and, where the platform supports it, in the Customer Environment; logs protected against alteration and kept for at least 12 months; alerting on suspicious activity, reviewed during support hours unless a managed detection and response module is ordered.
Backup and continuity (where a backup module is ordered)	Backup jobs monitored on each Business Day and failures remedied; restore testing at the frequency stated in the Order Form and at least quarterly; backup data stored within the EU/EEA unless the Order Form states otherwise; encryption of backup data at rest.
Nord Node's own continuity	Nord Node's business data is held in Microsoft 365 and in its delivery platforms and relies on those platforms' resilience together with retention policies. Nord Node maintains a documented procedure for restoring its service delivery capability, including access to customer documentation and credentials.
Incident management	Documented procedure for security incidents and personal data breaches, including assessment, containment, notification to Customers within the time frames in this DPA, and post-incident review.
Data minimisation and segregation	Customer data kept logically separated per Customer in every platform; Customer data not copied to Nord Node systems unless needed for the Services; test and demo environments do

Area	Measures
	not use Customer personal data.
Physical security	Customer data is not stored in premises controlled by Nord Node, except on encrypted devices; Sub-processor data centres hold recognised security certifications such as ISO/IEC 27001.
Deletion and disposal	Secure deletion of data at the end of the Services; certified wiping or physical destruction of storage media, with a record of the process.
Sub-processor management	Security and data protection assessment before engagement; written contracts meeting Article 28(4) GDPR; review of each Sub-processor's certifications and sub-processor lists; periodic review.

Annex 3 — Approved Sub-processors

Nord Node engages the following Sub-processors. The Sub-processor List, which Nord Node keeps up to date and provides to the Customer on request, states the Sub-processors in force at any time and forms part of this Annex 3.

Applies to all Customers:

Sub-processor	Service / purpose	Location of processing	Transfer mechanism
Microsoft Ireland Operations Ltd (and Microsoft affiliates)	Nord Node's own Microsoft 365 environment (e-mail, documents, Teams and service records); the Microsoft Intune, Entra ID and Microsoft Defender portals used to administer the Customer Environment; Microsoft Quick Assist for remote support sessions accepted by the User	EU/EEA (Microsoft EU Data Boundary); limited remote access by Microsoft personnel from outside the EU/EEA for support and security	EU–US Data Privacy Framework and Standard Contractual Clauses in Microsoft's Data Protection Addendum
ServiceNow (ServiceNow Nederland B.V. / ServiceNow, Inc.)	Customer portal, ticketing, service requests, service level tracking, knowledge base and configuration management database	EU/EEA data centre region; support access from outside the EU/EEA may occur	EU–US Data Privacy Framework; Standard Contractual Clauses in ServiceNow's Data Processing Addendum
Tanium (Tanium Inc. and its EMEA affiliate)	Endpoint management platform: inventory, patching, software deployment, configuration management, endpoint visibility and remediation; and, where ordered, Tanium Threat Response	EU/EEA data centre region; support access from outside the EU/EEA may occur	Standard Contractual Clauses in Tanium's Data Processing Addendum
Keeper Security (Keeper Security, Inc. / Keeper Security EMEA)	Encrypted storage of credentials used to administer the Customer Environment (Keeper MSP) and, where ordered, privileged access management (KeeperPAM). Vault contents are encrypted on the device and are not readable by the provider	EU region (Ireland or Frankfurt)	EU–US Data Privacy Framework; Standard Contractual Clauses in Keeper's Data Processing Agreement

Applies only where the Customer has ordered the relevant module:

Sub-processor	Service / purpose	Applies to	Location of processing	Transfer mechanism
Veeam Software (including Veeam Backup for Microsoft 365)	Backup and restore of Microsoft 365 data, servers, virtual machines and endpoints	Customers who have ordered backup on a Veeam platform	EU/EEA	Standard Contractual Clauses in Veeam's data processing terms, where applicable
Rubrik (including Rubrik Microsoft 365 Protection)	Enterprise backup, immutable storage and cyber recovery	Customers who have ordered backup on Rubrik	EU/EEA	Standard Contractual Clauses in Rubrik's data processing terms, where applicable
Microsoft 365 Backup	Native backup of Exchange Online, SharePoint Online and OneDrive	Customers who have ordered Microsoft 365 Backup	EU/EEA (Microsoft EU Data Boundary)	As for Microsoft above
Managed detection and response provider	Security monitoring and response outside Nord Node's support hours	Customers who have ordered MDR; the provider is named in the Order Form and added to the Sub-processor List before the service starts	To be stated when the provider is engaged	To be stated when the provider is engaged

Where a Sub-processor's own data processing terms, certifications or sub-processor list are relevant to the Customer's assessment, Nord Node will provide them on request (section 7.6).

The Customer's own Microsoft 365, Azure or other cloud tenants are provided to the Customer directly by the Vendor under the Customer's own agreement with the Vendor (see section 3.3). The Vendor is therefore not Nord Node's Sub-processor for the data stored in those tenants. This includes Microsoft Defender, Microsoft Entra ID, Microsoft Intune, Microsoft Sentinel and Microsoft Purview where the Customer holds the licences, even though Nord Node administers them.

Related documents

Document	Web address
Sub-processor List	https://www.nordnode.se/en/dam/nordnode/legal/final/document/nordnode-subprocessors-en.pdf