PostNord Group
Information Security Requirements for Suppliers

Table of contents

Part 1: PostNord Group – Introduction to information security requirements

PostNord Group uses, creates, and stores a significant amount of data in its business and must ensure that the confidentiality, integrity, and availability of data is protected. PostNord Group AB and its subsidiaries (referred to as PostNord Group) expect and requires all Suppliers to PostNord Group to implement and maintain appropriate and effective safeguards and Controls to ensure the security of PostNord Group Systems and information.

Capitalized terms used in this appendix shall have the meaning assigned to those terms in the definitions section at Part 4 of the appendix. Where the appendix forms part of any agreement between the Supplier and a member of PostNord Group, the definitions provided within this appendix shall prevail over any conflicting definitions in the remaining part of such agreement, but only with regards to the interpretation of this appendix.

Part 2 of the appendix sets out mandatory minimum-security requirements with which PostNord Group expects the Supplier to comply.

Part 3 of the appendix sets out enhanced requirements with which all Suppliers should comply with. Further, if the Supplier meets any of the following criteria, then it must comply with the enhanced Controls in Part 3 of the appendix:

a) the Supplier processes PostNord Group data using Supplier systems outside PostNord Group premises; and /or
b) the Supplier has access to PostNord Group Systems, whether via remote access or otherwise.

Where the Supplier Process Processes Personal data on behalf of PostNord Group and/or the Supplier Process Processes Personal data outside of the European Economic Area, additional requirements, and expectations pursuant to Data Protection Legislation will be included in the relevant agreement between the Supplier and the PostNord Group. To the extent that those additional measures overlap or conflict with requirements set out in the appendix, the stricter requirements of the two shall apply to the Supplier.
The Supplier is responsible for its own costs as regards these information security requirements, including Mandatory and Enhanced security requirements.

Part 2: Mandatory minimum-security requirements

In addition to the below mandatory minimum-security requirements, the Supplier should manage information security in accordance with the practices described in ISO 27001 (not necessarily certified) or other equivalent international standards.

Where any part of the Services is not covered by the scope of a current ISO 27001 certification, the Supplier should always and upon request be able to demonstrate it has implemented Controls equivalent to industry standard Controls such as, but not limited to, ISO/IEC 27002, in the current valid version.

PostNord Group may, at its own discretion, conduct information security audits relating to the compliance of requirements set forth here. Details regarding PostNord Group's right to audit are set out below.

The Supplier shall comply with the following mandatory minimum-security requirements:

Table A – Minimum-security requirements

Requirement	Expectation
General	
A.1 Preservation of confidentiality, integrity, and availability	The Supplier shall be responsible for preserving the confidentiality, integrity, and availability of PostNord Group data preventing the corruption or loss of PostNord Group data and shall ensure that it has in place appropriate Controls (including with its agents, contractors, or sub-contractors) to guard against unauthorized and/or unlawful use and modification of PostNord Group data.
A.2 System security	The Supplier shall ensure that any system on which the Supplier holds any PostNord Group data, including back-up data, is a secure system that complies with Part 3 of this information security appendix, and only enables access to PostNord Group data in electronic form to Supplier.
Requirement	**Expectation**
Information and cybersecurity protection	
A. 3 Protecting information	The Supplier shall protect PostNord Group data throughout its lifecycle and shall maintain an inventory of PostNord Group data in their possession. The Supplier shall provide PostNord Group with evidence to demonstrate that Controls are in place to protect and manage PostNord Group data in accordance with its classification.
A.4 Information security testing	Where the Supplier hosts a public web site or Internet-facing application which stores, processes, or transmits PostNord Group data or displays PostNord Group branding, the following requirements shall apply. To the extent that the Supplier has agreed to comply with PostNord Group requirements which overlap or conflict with the requirements set out below, the more stringent requirements of the two shall apply to the Supplier: 1) that security testing, including penetration testing, is performed by a qualified and skilled personnel prior to the web-based application being hosted on the Internet; 2) there is a regular security testing schedule on the web site, occurring at a frequency of at least annually. PostNord Group is to be informed of the times and dates of the security testing; 3) PostNord Group is provided with a summary of the results of the annual penetration testing of the software platform provided to PostNord, together with a list of remedial actions for each finding including its risk rating, where each action has a delivery date; and 4) progress on remedial action is reported upon request to PostNord Group.

Requirement	Expectation
Information security incident management	
A.5 Response Plan	The Supplier shall maintain a written Information Security Incident response plan. The Supplier shall remedy each Information Security Incident in a timely manner following its Information Security Incident response plan in accordance with Good Industry Practice.
A.6 Notification Requirements	The Supplier shall notify PostNord Group of any Information Security Incident affecting any PostNord Group data or PostNord Group Systems managed or interfaced by the Supplier within the established period by existing law or regulation but not longer than 24 hours of becoming aware of the Information Security Incident. The Supplier shall use reasonable endeavors to provide a full report of the Information Security Incident and the related response as well as ensuring they reconstruct any lost or destroyed information without any charge to PostNord Group. In case of an Information Security Incident or a Personal data breach (as defined by data protection legislation) affecting PostNord Group data or systems, the Supplier shall report this to PostNord Internal Service Desk (not to be used for customers), and to its defined PostNord Group business contact.
A.7 Cooperation with PostNord Group's Investigations	The Supplier shall cooperate with PostNord Group in handling an Information Security Incident, including, but not limited to, the following: 1) coordinating with PostNord Group on the Supplier's response plan; 2) assisting with PostNord Group's investigation of the Information Security Incident; 3) facilitating interviews with the Supplier personnel and others involved in the Information Security Incident or response; and making available all relevant information required for PostNord Group to comply with applicable laws, regulations, or industry standards, or as otherwise required by PostNord Group.
A.8 Third party notifications	The Supplier agrees that it shall not notify any third party (including any regulatory authority or customer) of any Information Security Incident on behalf of PostNord Group without first obtaining PostNord Group's prior written consent, unless this violates any existing law or regulation. Furthermore, the Supplier agrees that PostNord Group shall have the sole right to determine: 1) whether notice of the Information Security Incident is to be provided to any individuals, regulators, law enforcement agencies, or others; and 2) the form and contents of such notice.

Requirement	Expectation
Data protection legislation requirements for the Supplier	
A.9 Legal compliance	1) The Supplier shall adhere to applicable data protection legislation, including provisions concerning the security of Personal data, and to relevant regulations, such as GDPR; 2) The Supplier shall comply with all relevant regulatory requirements when Personal data, that of customers, consumers, employees, and shareholders, is collected, recorded, hosted, Process Processed, transmitted, used, and / or erased; and 3) The Supplier shall comply with all contractual requirements on data protection and information security and shall not disclose any information that is not known to the public.

PostNord Group shall have the following audit rights over the Supplier. To the extent that the Supplier has agreed to audit rights for PostNord Group which overlap or conflict with the rights set out below, the more extensive audit rights for PostNord Group of the two shall be exercisable by PostNord Group:

Table B – Right to audit for PostNord Group

Requirement	Expectation
B.1 Audit Access	The Services and IT systems provided by the Supplier shall be subject to audit by PostNord Group (or any external auditors as PostNord Group may appoint) within reasonable written notice (including, but not limited to, data Process Processing agreements concluded by the Supplier being compliant with data protection legislation). Audit activities may include providing Supplier with questionnaires for Supplier-self assessment, reviewing documentation, conducting interviews, evidence collection and analysis of delivered reports and Process documents, physical/ remote audit, or certification, provided that these activities do not require any access to view production/confidential data of the Supplier and/or its customers.
B.2 Audit Findings	The Supplier shall mitigate all findings identified in the audit within an agreed-upon period and provide evidence of successful mitigation to PostNord Group.
B.3 Evidence of Compliance	Upon request by PostNord Group, not more often than once every twelve months, the Supplier shall provide evidence of compliance for the provisioned Services and IT systems in the form of independent review from third party auditors or industry recognized security assurance standards. The evidence provided shall comprise: 1) A copy of its annual certification of compliance with ISO 27001 and/or SSAE SOC2 or any equivalent reports; and 2) A summary of its vulnerability assessment or penetration testing reports relating to systems and Process Processes involved in the provision of the Services. Confidential and / or data whose sensitivity is derived from classification or legal requirements may be removed in the report to protect the confidentiality of the Supplier's systems. However, the total number and severity of the identified issues shall be provided including risk mitigation measures and implementation timeline.
B.4 Requests for Information	Upon request by PostNord Group, the Supplier shall provide answers and evidence to PostNord Group regarding the Supplier's information security and data protection risk and compliance.

Part 3: Enhanced security requirements

These enhanced security requirements set out the technical and organizational information security measures that the Supplier must adopt when:

a) the Supplier is processing PostNord Group data using Supplier systems outside PostNord Group premises; or

b) the Supplier has access to PostNord Group Systems, via remote access or otherwise.

These enhanced security requirements shall apply in addition to any requirements relating to information security practices and data protection standards set out in any agreement between the Supplier and PostNord Group.

Table C – Enhanced security requirements

Requirement	Expectation
C.1 Description of information and methods for access	The Supplier shall provide a description of the information that needs to be shared or accessed by the Supplier and describe methods of securing the information shared or with access by the Supplier.
C.2 Classification of information	The Supplier shall provide a mapping between PostNord's information classification scheme and the Supplier's scheme; ensuring that adequate classification and protection is applied.
C.3 Legal and regulatory compliance	The Supplier must ensure that a Data Processing Agreement (DPA), which is provided by or approved of PostNord, is executed between PostNord and the Supplier if the Supplier is handling personal data. Other compliance areas shall be addressed in the main agreement.
C.4 Access control, performance review, monitoring and reporting	The Supplier shall implement least-privilege access control with monitoring and performance reviews which shall be reported at periodic intervals (at least quarterly) to the PostNord service-/product owner.
C.5 Acceptable use of information	Descriptions and criteria for the acceptable use of information shall be given in the main agreement but also as specific instructions for acceptable Processing of personal data, if applicable, in a data Processing Agreement between PostNord and the Supplier.
C.6 Authorized access	The Supplier shall have a clear Process for on- and off-boarding of authorization to access to PostNord's information as part of the delivery.
C.7 Security Controls	The Supplier shall implement cyber security Controls based on industry best practices (such as ISO 27002 or the NIST Cyber Security Framework) for the adequate protection of the ICT infrastructure.
C.8 Incident management	The Supplier shall establish procedures for incident management and have Processes in place, with special focus to notification and collaboration during incident remediation. High-priority incidents shall be reported to PostNord immediately and also periodically (e.g. quarterly) to the service owner.
C.9 Security awareness	Continuous and verified training and awareness activities and/or programs for information security and data protection shall be in place.
C.10 Sub-contracting	Special Controls for sub-contracting shall be implemented to meet the protection level stated in this document, if applicable, and a list of sub-contractors shall be supplied to PostNord and notification before any relevant changes.
C.11 Point of contact for security issues	The Supplier shall provide PostNord with the information of the point of contact for security issues.

C.12 Personnel screening	Background checks shall be conducted for the Supplier's personnel as allowed by the law.
C.13 Third-party attestations	The Supplier shall provide evidence of third-party attestations (i.e. ISO certifications, penetration test reports) related to the Supplier Processes whose effectiveness of Controls shall be verified though independent reporting. These reports shall periodically be presented by the Supplier to PostNord with specific attention to resolving the issues raised in the reports to improve the information security of the service delivery.
C.14 Defect resolution and conflict resolution	The Supplier should put in place special Processes and routines for managing problems in correcting security issues (addressed above in C.13) together with a clear way to handle and resolve conflicts relating to these activities.
C.15 Backup storage and frequency	The frequency of backups and the storage location shall be selected as to suit the business delivery. The backup configuration shall match the recovery time objective as part of the information classification (see point a & b).
C.16 Disaster recovery	An alternate and periodically tested facility shall be available (i.e. disaster recovery site) to provide uninterrupted service when dealing with outages and disturbances. PostNord shall be given evidence of such tests.
C.17 Change management and notification	The Supplier shall have a change management Process in place that enables advance notification to PostNord of significant changes that might negatively impact the service delivery, so that PostNord will have the possibility to not accept the changes, in regards to probable risks of service impact.
C.18 Physical security	There shall be corresponding and adequate physical security Controls in place as part of the Supplier's service delivery to PostNord and in line with the information classification. These physical Controls shall be presented to PostNord.
C.19 Information transfer Controls	The Supplier shall specify and execute information transfer Controls to protect the information during logical transmissions or physical transfers.
C.20 Termination clauses	The main agreement shall regulate the conditions for termination upon conclusion of the agreement. This shall include records management, return of assets, secure disposal of information as well as any ongoing confidentiality obligations.
C.21 Secure destruction of information	Information stored by the Supplier shall, following an established protocol, securely destroy PostNord's information as soon as it is no longer required. This must be communicated with PostNord in each instance or agreed upon as a general scheme for the service delivery. When the destruction concerns personal data, this must be included in the instructions of the DPA as a specific kind of data Processing.
C.22 Handover support	The Supplier shall establish and be able to present to PostNord, upon request, the routines and Processes for handover support to another Supplier or to PostNord at the end of the contract.
C.23 Indemnities and remediation	Indemnities and remediation for failure of contractor to meet these requirements shall be regulated in the main Services agreement.

For PostNord Group's critical deliveries or where the Supplier requires access to PostNord Group internal information and systems the following apply:

Table D – Conditions of Supplier access to PostNord internal systems

Requirement	Expectation
D.1 Access on a need-to-know basis	The Supplier's access to any PostNord Group data shall only be granted to the Supplier when a need to know exists and when such a disclosure has been authorized by the data/information owners at PostNord Group.
D.2 Legitimate and documented business need	Inbound access to PostNord Group Systems shall only be granted to the Supplier where the relevant PostNord Group System manager determines that the Supplier has a legitimate and documented business need for such access, and the systems of the Supplier provide no significant threat to any part of PostNord Group infrastructure. Supplier access shall only be enabled for specific individuals and only for the time required to accomplish approved tasks.
D.3 Follow PostNord Group network access onboarding procedures	The Supplier shall follow PostNord Group System access onboarding procedures to obtain inbound access to PostNord Group Systems. Such procedures include required information provision as part of network configurations including, but not limited to, IP addresses, network protocol, and network access implementation method (e.g., VPN setup).
D.4 Documentary evidence of an Information Security Management System	Before access can be issued to the Supplier for the period of engagement, documentary evidence of an information security management system or Process compliant with ISO 27001 or other equivalent international standards shall be provided and the Supplier shall agree in writing to prevent unauthorized and improper use of PostNord Group Systems made available to the Supplier.
D.5 Immediate termination	PostNord Group also reserves the right to immediately terminate network connections with all Supplier systems if PostNord Group believes either that the Supplier is not meeting these requirements, or if the Supplier is providing an opportunity for attack against PostNord Group Systems.
D.6 Documented security architecture	The Supplier shall maintain documented security architecture of the networks managed by the Supplier in its operation of the Services provided to PostNord Group. The Supplier shall review the network architecture, including measures designed to prevent unauthorized network connections to all systems, applications, and network devices on a regular basis (i.e., at least once a year).
D.7 Separation of PostNord Group Systems and Supplier systems and infrastructure	When Supplier hosts PostNord Group systems or PostNord Group information is stored or processed on Supplier's systems, these Supplier systems shall be strictly separated from the Supplier's internal systems and infrastructure.
D.8 Data logging	The Supplier shall collect all logging data relating to PostNord Group (proof, evidence of actions) and shall provide this data to PostNord Group upon request.

Part 4: Definitions

1) The definitions in this Part 4 apply to this Information Security Appendix.

"Affiliate"	Affiliate means any legal entity which PostNord AB (publ) directly or indirectly owns or Controls
"Control" or "Controlled"	the controlling entity possessing, directly or indirectly, or jointly with a third party or parties, the power to direct management and policies of the controlled entity;
"Data Protection Legislation"	GDPR (General Data Protection Regulation); the Privacy and Electronic Communications Directive 2002/58/EC (as updated by Directive 2009/136/EC) and the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426) as amended; and, to the extent applicable, all other applicable laws and regulations of any other country relating to the Process Processing of Personal data and privacy.
"PostNord data"	all data or records of whatever nature and in whatever form relating to the business, employees, customers, Suppliers or otherwise relating to the business of PostNord;
"PostNord", "PostNord Group"	PostNord Group AB (publ.) and its affiliates.
"PostNord Systems"	the information technology and communication systems, including networks, hardware, software, middleware, virtual platforms, Embedded Technology (see definition below) and interfaces owned by or licensed to PostNord or any of its or their agents, customers, or contractors;
"Embedded Technology"	Embedded Technology Devices are physical objects used for monitoring and / or affecting the physical environment with sensors, data storage and / or Process Processing ability, internal software, and / or the ability to exchange data with other devices and systems over an IT network.
"GDPR"	Regulation (EU) 2016/679 (the General Data Protection Regulation), including any amendments and updates in force from time to time;
"Good Industry Practice"	in respect of any activity, performing that activity effectively, reliably, and professionally using the degree of skill, care, diligence, prudence, foresight, and judgement which would be expected from a skilled and experienced operator of similar standing engaged in the provision of similar Services;
"Information Security Incident"	any actual compromise of the confidentiality, integrity, or availability of PostNord Group data; any actual compromise of, or unauthorized access to, any system that Process Processes PostNord Group data that presents a risk to the confidentiality, integrity, or availability of PostNord Group data; or receipt of a complaint, report, or other information regarding the potential compromise or exposure of PostNord Group data Process Processed by Supplier;

“Process” or “Processing” or “Processes”	any operation or set of operations which is performed on data or on sets of data, whether by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction;
“Personal data”	any Personal data (as such term is defined in data protection legislation) which is subject to the applicable data protection legislation;
“Services”	the Services provided by the Supplier;
“Supplier”	the counterparty to any agreement with PostNord Group to which the Information Security Requirements for suppliers (INFORMATION SECURITY APPENDIX) forms part of such agreement;
“Supplier personnel”	the employees, contractors and other individuals who are engaged by the Supplier, its Affiliates, or their subcontractors from time to time to meet the Supplier’s obligations