postnord

Information Security Appendix for Supplier Agreements

Organization	PostNord
Date	October 1, 2025
Document owner	CISO
Version	2.1
Information category	Public

postnord

Table of contents

Section A: Introduction to PostNord's information security requirements

PostNord 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 AB (publ) and its subsidiaries (referred to as PostNord) expect and require that all Suppliers to PostNord implement and maintain appropriate and effective safeguards and controls to ensure the security of PostNord systems and information. Capitalized terms used in this Appendix shall have the meaning assigned to those terms in Section D of this Appendix.

Section B of the Appendix sets out mandatory minimum security requirements which the Supplier shall comply with at all times.

Section C of the Appendix sets out enhanced requirements which the Supplier shall comply with. Further, if the Supplier meets any of the following criteria, then it must also in addition with the mandatory minimum requirements, comply with the enhanced controls in Section C of the appendix:

- the Supplier Processes PostNord data using Supplier systems outside PostNord premises; and /or
- the Supplier has access to PostNord systems, either via remote access or otherwise.

Where the Supplier Processes Personal data on behalf of PostNord and/or the Supplier Processes Personal data outside of the European Economic Area, additional requirements pursuant to Data Protection Legislation will be included in the relevant agreement between the Supplier and PostNord. To the extent that those additional measures overlap or conflict with requirements set out in this Information Security Appendix for Supplier Agreements, the stricter requirements of the two shall apply to the Supplier.

The Supplier shall be responsible for its own costs with regards to these information security requirements, including mandatory and enhanced security requirements.

Section B: Mandatory minimum security requirements

In addition to the below mandatory minimum security requirements, the Supplier shall manage information security in accordance with the practices described in ISO 27001 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 shall always be able to, and upon request, demonstrate it has implemented controls equivalent to industry standard controls such as, but not limited to, ISO/IEC 27002, in the current valid version. The Supplier shall regularly assess and improve its Business Continuity/Disaster Recovery capabilities in line with:

- ISO 22301 (Business Continuity Management Systems) or equivalent standards
- Updates to the EU Cyber Resilience Act or related regulatory guidance
- Lessons learned from passed incidents and recovery test results.

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

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

Table A – Minimum-security requirements

Requirement	Description
General	
A.1 Preservation of confidentiality, integrity, and availability	The Supplier shall be responsible for preserving the confidentiality, integrity, and availability of PostNord data preventing the corruption or loss of PostNord data and shall ensure that it has in place appropriate controls covering its own operations and including its agents, contractors, or sub-contractors, to guard against unauthorized and/or unlawful use and modification of PostNord data.
A.2 System security	The Supplier shall ensure that any system on which the Supplier holds any PostNord data, including back-up data, is a secure system that complies with Section C of this Information Security Appendix for Supplier Agreements, and only enables access to PostNord data in electronic form to Supplier.
Information and cybersecurity protection	
A. 3 Protecting information	The Supplier shall protect PostNord data throughout its lifecycle and shall maintain an inventory of PostNord data in their possession. The Supplier shall provide PostNord with evidence to demonstrate that controls are in place to protect and manage PostNord data in accordance with its classification.

Requirement	Description
A.4 Information security testing	Where the Supplier hosts a public web site or Internet-facing application which Processes PostNord data or displays PostNord branding, the following requirements shall apply. To the extent that the Supplier has agreed to comply with PostNord requirements which overlap or conflict with the requirements set out below, the stricter requirements of the two shall apply to the Supplier: 1. that security testing, including penetration testing, is performed by 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 is to be informed of the times and dates of the security testing; 3. PostNord 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.
Information security incident management	
A.5 Information Security Incident 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. The Supplier shall ensure that digital systems, including all software, hardware, and appurtenant services, are designed and maintained to: 1. Resist, detect, and recover from Information Security Incidents. 2. Maintain essential functions during and after an Information Security Incident. 3. Restore normal operations within the agreed PostNord Recovery Time Objective (RTO) and Recovery Point Objective (RPO).

Requirement	Description
A.6 Notification Requirements	The Supplier shall notify PostNord of any Information Security Incident affecting PostNord data or PostNord systems that are managed or interfaced by the Supplier, in accordance with applicable laws and regulations. Such notification shall be made without undue delay and no later than 24 hours after the Supplier becomes aware of the incident. The Supplier shall provide a detailed incident report within 48 hours, including root cause analysis, potential effects on PostNord operations and mitigation steps. 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 in Data Protection Legislation) affecting PostNord data or systems, the Supplier shall report this to PostNord Service Desk, and to its defined PostNord business contact.
A.7 Cooperation with PostNord Group's Investigations	The Supplier shall cooperate with PostNord in handling an Information Security Incident, including, but not limited to, the following: 1. coordinating with PostNord 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 4. making available all relevant information required for PostNord to comply with applicable laws, regulations, or industry standards, or as otherwise required by PostNord.
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 without first obtaining PostNord prior written consent, unless this violates any existing law or regulation. Furthermore, the Supplier agrees that PostNord 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.

Data Protection Legislation requirements for the Supplier	
A.9 Legal compliance	1. When Processing PostNord Personal data, the Supplier shall comply with applicable Data Protection Legislation, including but not limited to the provisions concerning the security of Personal data; 2. When Processing PostNord Personal data, the Supplier shall comply with all contractual requirements on data protection and information security. 3. For cases where PostNord is a GDPR Controller and Supplier is a Processor, 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.
A.10 NIS2 governance and third-party risk	The Supplier shall comply with the NIS2 regulations including but not limited to: 1. Assigning a named individual responsible for information security governance. 2. Ensuring executive-level awareness and training in information security obligations. 3. Conducting regular third-party risk assessments and ensuring subcontractors meet equivalent security standards. 4. Maintaining a documented information security risk management policy and providing it to PostNord upon request.
A.11 AI compliance	Any use of AI used to Process or analyze PostNord data is strictly prohibited unless expressly agreed in the Agreement. The Supplier shall, where any AI-based systems or components are agreed to be used to Process or analyze PostNord data, comply with the AI Act including but not limited to: 1. Identifying and documenting any "high-risk AI" in accordance with the AI Act scope and requirements. 2. Maintaining robust data governance and transparency for all training data and AI models used, ensuring technical documentation is available upon request. 3. Appointing an AI compliance contact or officer responsible for AI-related obligations and oversight. 4. Implementing technical and organizational measures that address potential AI risks, including regular third-party audits or internal evaluations. 5. Reporting any updates or major changes to AI systems that might alter risk classification promptly to PostNord

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

Table B – Right to audit for PostNord Group

Requirement	Description
B.1 Audit Access	The Services and IT systems provided by the Supplier shall be subject to audit by PostNord, or any external auditors as PostNord may appoint, within reasonable written notice, including, but not limited to, data 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 with 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 Processes involved in the provision of the Services. Confidential 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 regarding the Supplier's information security and data protection risk and compliance.

Section C: Enhanced security requirements

Table C – Enhanced security requirements

Requirement	Description
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 ensure that adequate classification and protection is applied of PostNord data.
C.3 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 systems made available to the Supplier.
C.4 Access on a need-to-know basis	The Supplier's access to any PostNord 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.
C.5 Legitimate and documented business need	Inbound access to PostNord systems shall only be granted to the Supplier where the relevant PostNord 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 infrastructure. Supplier access shall only be enabled for specific individuals and only for the time required to accomplish approved tasks.
C.6 Follow PostNord network access onboarding procedures	The Supplier shall follow PostNord System access onboarding procedures to obtain inbound access to PostNord 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.
C.7 Data logging	The Supplier shall collect all logging data relating to PostNord, such as e.g., proof, evidence of actions, and shall provide this data to PostNord upon request.

Requirement	Description
C.8 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. Access review shall cover standard and privileged user accounts, service accounts including but not limiting to Application Programming Interfaces (APIs), Interactive web elements (e.g. widgets), Secure File Transfers (e.g., SFTP/FTP), Electronic Data Interchange (EDI), message queues and event streaming, cloud storage integrations, notifications to external endpoints (e.g. webhook-based communication), and other digital mechanisms for integration and communication through various PostNord systems and interfaces.
C.9 Immediate termination	PostNord has the right to immediately terminate network connections with all Supplier systems if PostNord believes either that the Supplier is not meeting these requirements, or if the Supplier is providing an opportunity for attack against PostNord systems.
C.10 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.11 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.12 Security Controls	The Supplier shall implement information 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.13 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, at least once a year.
C.14 Separation of PostNord systems and Supplier systems and infrastructure	When Supplier hosts PostNord systems or PostNord information is Processed on Supplier's systems, these Supplier systems shall be strictly separated from the Supplier's internal systems and infrastructure.
C.15 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.

Requirement	Description
C.16 Security awareness	Continuous and verified training and awareness activities and/or programs for information security and data protection shall be in place.
C.17 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. New sub-contractors must be approved by PostNord, before being used by the Supplier. Furthermore, the list should be updated by the Supplier on an annual basis.
C.18 Point of contact for security issues	The Supplier shall provide PostNord with the information of the point of contact for security issues.
C.19 Personnel screening	Background checks shall be conducted for the Supplier's personnel as allowed by the law.
C.20 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.21 Defect resolution and conflict resolution	The Supplier shall put in place special Processes and routines for managing problems in correcting security issues, addressed above in C.20, together with a clear way to handle and resolve conflicts relating to these activities.

Requirement	Description
C.22 Backup storage, confirmations, and frequency	The frequency of backups and the storage location shall be selected to suit the business delivery. The backup configuration shall match the PostNord Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs). The Supplier shall ensure sufficient processes are in place for confirmation of successful and complete backups as well as robust processes for immediate notification of PostNord when backups fail. The Supplier shall implement a Disaster Recovery Plan (DRP) including but not limited to: 1. Redundant infrastructure and failover mechanisms. 2. Secure and geographically diverse backup facilities. 3. Regular, at least annual, testing of disaster recovery procedures, including tests against power outages, human mistakes, software and hardware failures, supply chain disruptions, cyber-attacks e.g., malware, ransomware, denial of service. 4. Evidence of successful disaster recovery testing, including successful backups recovery shall be provided to PostNord upon request.
C.23 Business Continuity Plan	An alternate and periodically tested facility, i.e. disaster recovery site, shall be available to provide uninterrupted service when dealing with outages and disturbances. PostNord shall be given evidence of such tests. The Supplier shall develop, maintain, and annually review a Business Continuity Plan (BCP) that ensures the continued availability of critical services and systems in the event of a disruption including but not limited to: 1. Identification of critical business functions and supporting IT systems. 2. Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) aligned with PostNord's service expectations. 3. Roles and responsibilities during a continuity event. 4. Communication protocols with PostNord during incidents.
C.24 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, regarding probable risks of service impact.
C.25 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.

Requirement	Description
C.26 Information transfer Controls	The Supplier shall specify and execute information transfer controls to protect the information during logical transmissions or physical transfers.
C.27 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.28 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.29 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.30 Indemnities and remediation	Indemnities and remediation for failure of contractor to meet these requirements shall be regulated in the main Services agreement.

C.31 Vulnerability management	The Supplier shall perform regular vulnerability scans on all parts of the services provided to PostNord, including but not limited to: 1. Workstations (e.g., laptops, PCs) 2. Mobile devices 3. Servers 4. Network devices 5. Internet of Things (IoT) and Operational Technology (OT) 6. Software applications Scans must be conducted both internally and externally to ensure comprehensive coverage. The Supplier is responsible for identifying, assessing, and remediating vulnerabilities across all environments where PostNord services may be impacted. All vulnerabilities classified as critical or high severity must be remediated and patched within 72 hours of detection. The Supplier shall maintain documented evidence of scan results, remediation actions, and patch deployments, and make these available to PostNord upon request.
C.32 Security Monitoring	The Supplier shall implement continuous security monitoring and protection mechanisms across all endpoints involved in delivering services to PostNord. This includes, but is not limited to: • Workstations (e.g., laptops, PCs) • Mobile devices • Servers • Network devices • Internet of Things (IoT) and Operational Technology (OT) • Software applications All endpoints must be equipped with appropriate security controls such as Antivirus (AV) or Endpoint Detection and Response (EDR) solutions to detect, prevent, and respond to threats in real time. The Supplier shall ensure that all security logs generated by systems, devices, and applications covering events such as user activity, network events, system changes, and threat detection are actively monitored and integrated into a Security Information and Event Management (SIEM) platform or a comparable solution. These logs must be retained for at least 90 days and analyzed to support timely detection, investigation, and response to potential security incidents. The Supplier shall provide PostNord with access to relevant log data and incident reports upon request.

Section D: Definitions

The definitions in this Section D apply to this Information Security Appendix for Supplier Agreements.

"AI" "	short for artificial intelligence meaning any technology or system that mimics human intelligence to perform tasks such as machine learning, deep learning, language technology, or other advanced data analysis.
“AI Act”	Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonized rules on artificial intelligence and amending (Artificial Intelligence Act) including any amendments and updates in force from time to time.
“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 Processing of Personal data.
“PostNord data”	all data, including Personal 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 AB (publ.) and its affiliates.
“PostNord systems”	the information technology and communication systems, including networks, hardware, software, middleware, virtual platforms, Embedded Technology as defined 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 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 data; any actual compromise of, or unauthorized access to, any system that Processes PostNord data that presents a risk to the confidentiality, integrity, or availability of PostNord data; or receipt of a complaint, report, or other information regarding the potential compromise or exposure of PostNord data Processed by Supplier.

“NIS2 regulations”	NIS2 Directive (Directive (EU) 2022/2555) and all applicable local legislation implementing or supplementing the requirements of the Directive within the relevant jurisdictions’ amendments and updates in force from time to time.
“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 or dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction;
“Personal data”	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, location 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
“Services”	the Services provided by the Supplier;
“Supplier”	the counterpart to any agreement with PostNord to which the Information Security Appendix for Supplier Agreements 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