Security Appendix

29.11.2021

Posti security requirements for suppliers

Security Appendix

29.11.2021

Contents

Security Appendix

29.11.2021

1. Introduction

Posti Group Oyj (“Posti”) relies heavily on its data and especially personal data of Posti’s customers that Posti processes (hereby referred to as “Posti Information”), to successfully deliver its services, and to enable subsidiaries to fulfil their commercial objectives. Therefore, it is essential that the confidentiality, integrity, and availability of Posti Information and related Services (i.e. IT systems, platforms, people, networks, suppliers, cloud, external services, etc. utilized to provide services) is ensured. Any third party (referred from now on as “Supplier”) that has access to, processes, or stores Posti Information must adhere by this document to ensure that Posti maintains the trust of all its stakeholders and remains compliant with relevant legal and regulatory requirements.

Suppliers may have access to a wide range of Posti systems or Information. This access could be either through storing Information or infrastructure belonging to Posti at an offsite facility (e.g. as part of a Cloud service provider arrangement), or through having remote or physical access to Posti’s systems. As a result, all applicable security controls must be implemented according to recognized standards and risks related to information security must be mitigated to fulfill Posti’s approved risk management policy. In that context, the purpose of this document is to ensure that Posti’s Information and systems that are accessed by external Suppliers and service providers are subject to appropriate protection.

2. Basic principles & scope

- For general information security related to Suppliers own security processes and practices (non-Posti specific practices), it is sufficient if the Supplier can demonstrate an acceptable level of adherence to industry best practice information security frameworks such as ISO27k, NIST CSF, ISF Standard of Good Practices or similar.
- For Posti's general information security requirements for Suppliers, requirements defined in this document apply. More definitive, supplier-specific requirements may be set in the contract.
- Supplier's information security practices and compliancy with requirements can be evaluated by Posti with periodic information security self-assessments filled by the Supplier, or Audits conducted by Posti or a third party on behalf of Posti. (see section 3. Right to Audit)
- Supplier's answers to information security self-assessments will be included as part of contract attachments.
- Applicable legal and regulatory requirements (e.g. GDPR – General Data Protection Regulation) must always be adhered to when they apply.
- Supplier must designate named individual(s) who will have a responsibility and accountability for information security and privacy implementation, and processes/procedures. The nominated individual(s) must act as the primary point(s) of contact for Posti in situations where information security and privacy are concerned.
- In all cases where Subcontractors are used by the Supplier, the Supplier is fully liable for their performance. Supplier is responsible in ensuring the compliance of respective security measures also for possible Subcontractors used to deliver services to Posti. Subcontractors handling Posti's Information are expected to be assessed for risk in accordance with Posti's Risk Management process. Before transferring production of services to a Subcontractor, use of the Subcontractor and its security arrangements and measures must be approved by Posti to the extent they differ from similar used by the Supplier. For example, any data transfers outside EU/ETA must be approved by Posti
- As an assumption, no payment card cardholder data is stored, transmitted or handled as part of the Services, unless otherwise agreed in the main contract, in which case a separate PCI-DSS requirements must be agreed between Posti and the Supplier.
- In case there are requirements in this document that the Supplier cannot adhere to, Posti shall be notified without delay. Posti and Supplier shall then agree, if deemed necessary, complementary controls to address potential risks posed by non-compliance. It should be noted that notification of non-compliance does not lessen the Supplier's responsibilities towards potential breaches of contract.

3. Right to audit

- To ensure compliance with Posti security requirements, Posti (or a third party on behalf of Posti) may carry out an information security and privacy assessment or an audit to the Supplier. Supplier must assist Posti with the provision of any relevant documentation requested and provide access to all relevant sites, as is necessary and when reasonably requested by Posti.
- Supplier shall regularly conduct independent reviews and assessments of security level and the implementation of security measures in its organization and processes related to services delivered to Posti. The result and findings and the required corrective measures are to be discussed with Posti as part of the service governance model.

4. Security & risk management

- Monitoring and evaluation of information security and privacy related topics regarding Supplier provided services must be covered by a separately agreed approach between the Supplier and Posti.
- Supplier must maintain a register of any identified security risks related to the provision of its services to Posti and Posti's Information. The risk register should be produced in consultation with Posti service manager and Posti Information Security Team, and maintained to show the nature, extent of, and progress in mitigating the identified risks.

5. Personnel security

- If Posti requests, Supplier is responsible that security clearances and/or background checks, as allowed by the local law, are conducted on Supplier Personnel (or supplier's subcontractors) who are involved in delivery of services to Posti.
- Non-disclosure agreement shall be put in place with all Supplier employees who have access to Posti's internal Information and the delivered service.
- Supplier must make sure that key persons and roles associated with delivery of Services to Posti are identified and deputy arrangements established in case of absences. Supplier must inform Posti if changes take place in key personnel involved in the delivery of Services to Posti.
- Supplier must provide Information security and privacy awareness training to all Supplier employees (including subcontractors) as relevant to their role in providing the service to Posti. For Suppliers providing external software developers for Posti, secure development training should be provided similarly as to Posti's internal software developers.

6. Asset management

- The Supplier must record in an asset inventory of all assets (i.e. IT systems, servers, platforms etc.) that are used to process or store Posti Information as part of the provided services. The inventory must be maintained and kept up to date and all assets must have a designated owner.
- If not separately specified, all assets received from Posti must be treated as confidential
- Posti data, material or systems that are owned (or leased) by Posti, must not be used without a written specific permission from Posti to any other purposes other than those specified in the Service Agreement between Posti and the Supplier (e.g. used for system development and testing). A thorough assessment on impact regarding privacy, security and changes in risks are required before Posti can provide such a permission.
- Supplier must securely and permanently destroy/wipe Posti related Information from all media and/or devices when it is no longer required for the Services. Supplier must ensure that also automatic backup arrangements are considered prior to disposal of Information. At Posti's request or upon termination of Service agreement, Supplier must return to Posti, without delay, Information, data and materials owned or managed by Posti which were acquired during the Service lifecycle.

7. Access control

- Supplier must ensure that, at all times, only relevant personnel have access to Posti systems and Information, or Supplier systems used in delivering the service and potentially used in processing or storing sensitive Posti data (incl. data of Posti's customers). Supplier must maintain and review an up-to-date list of all personnel who are authorized to access Posti Informational assets and resources (e.g., IT systems, platforms, networks, cloud, external services, etc.).
- Supplier must ensure multi-factor authentication (MFA) is used where needed, to protect privileged access accounts and access to sensitive Posti Information.

8. Cryptography

- Data transfer methods between Supplier and Posti must be mutually agreed and may only be one of the following methods: encrypted data transfer through a secure application platform (direct entry into a system), encrypted and protected file share platforms (e.g. ShareFile file transfer), password protected email attachments or password protected physical file transfers (USB Storage).

9. Physical security & working at Posti premises

- Supplier must ensure that all personnel present in premises where Posti Service is delivered, are authorized.
- If work related to services delivered to Posti is conducted remotely outside Supplier or Posti premises, secure remote working practices must be in place and followed by Supplier personnel.
- When Supplier is working in Posti's facilities, all Supplier's Personnel must adhere to the local rules of the Posti facility or area in question.
- Posti assets, material and equipment shall not be removed from the premises without separate permission from Posti

10. Operations security

- Procedures for operational activities to provide the Services to Posti must be documented, maintained and made available to anyone responsible for managing, administering or developing applications or systems used to process or store Posti's Information.
- Any changes to the organization, business processes, or systems processing Posti's Information that affect information security and privacy must be controlled, documented and authorized through a formal process. Any such changes must be reviewed and tested to ensure that there is no adverse impact on services provided to Posti or to the security of Posti's or Posti's customers' Information.
- Supplier used development/test and production facilities processing Posti's Information must be separated from each other to reduce the risk of unauthorized access or changes to the operational environment or Posti
- Development and test environments should use pseudonymization to protect sensitive data and if this is not possible, a risk needs to be documented, evaluated and addressed in cooperation with Posti and the Supplier.
- Back-up processes should be in place for timely recovery of systems used in providing the service to Posti.

11. Network security

- As a principle, no Posti data should be copied outside Posti controls. If this is required, a risk needs to be documented, evaluated and addressed in cooperation with Posti and the Supplier.

- Potential testing and scanning of Posti networks or devices, or penetration tests of systems may not be done without permission from Posti in cases where such activities could disturb critical operational activities.

12. Integrating into Posti processes and systems

- Supplier must validate product's or systems' integrity by performing appropriate scanning and testing before possible integration into Posti's infrastructure.
- For the purpose of authorization and access management, Suppliers shall integrate to Posti AD (Active Directory) as well as Posti access management procedures, where possible. If this is not possible, a risk needs to be documented, evaluated and addressed in cooperation with Posti and the Supplier.
- Supplier systems integrated to Posti systems, shall also integrate, where possible, to Posti SOC (Security Operations Center) for the purposes of security monitoring. In cases where this is not possible, a risk needs to be documented, evaluated and addressed in cooperation with Posti and the Supplier.
- Application programming interfaces (APIs) must be designed, developed, deployed, and tested in accordance with leading industry standards (e.g. OWASP Top 10 for Web Applications and OWASP Application Security Verification Standard) and adhere to applicable legal, statutory, or regulatory compliance obligations.

13. Security & privacy by design in system development

- Supplier must design and implement all Products and Services delivered to Posti by considering privacy and security related requirements (e.g. privacy and security by design). For any new or changed functionality, the supplier must conduct:
    - threat analysis for architecture and design, and define controls to be implemented for identified risks
    - security and privacy assessment (e.g. internal/external audits or testing) for features that have been identified to have risks associated with them in threat analysis
- If requested by Posti, Supplier must provide visibility of the identified risks, threats, and assessment results.

14. Incident management

- Any breach or suspected breach of security or privacy, such as compromise of Posti's material or Information, must be reported to Posti without delay. Subject to possible

restrictions by law, Posti has the right to take part in investigations or incident handling when Posti's interests are endangered. Supplier must deliver the report of the security incident investigation as well as the root cause analysis with suggestions for corrective actions to be taken to remediate the situation for Posti. The results and needed measures to be taken including prioritization are discussed as part of the service governance model.

15. Business continuity

- Posti is by law to assure its services during all national or local disturbances or emergencies. Supplier must take actions (regarding people, locations, assets, communication and information systems etc.) so that the services provided, and which are critical for Posti's provision of its services, can timely recover from possible incidents in all circumstances.
- Supplier must have business continuity and disaster recovery plans in place to minimize the impact of realized risk events on the Supplier organization and potential Subcontractors involved in the production of services to Posti.
- The plans must at minimum address:
    - how business operations will be restored following an interruption to or failure of business processes within an agreed time period, accepted by Posti, and how information security will be maintained;
    - define arrangements to inform and engage relevant Posti personnel in their execution;
    - regular testing, review and updating of the plans;
- The availability requirements (e.g. max downtime) for the Service provided to Posti are to be agreed together between Posti and the Supplier.

16. Data privacy

- When personal data is processed, the Supplier (and possible subcontractors) shall have a formal, documented, comprehensive and accurate record of processing activities (ROPA) based on a data mapping exercise that is regularly reviewed, according to the Article 30 of the GDPR.
- If the Supplier processes personal data on behalf of Posti, a separate Data Processing Agreement (DPA) shall be signed between Posti and the Supplier.
- No personal data of Posti employees or Posti's customers that the Supplier is a processor or the controller of, shall be transferred outside of the European Union (EU) and to countries that the European authorities have not deemed to have adequate safeguards in place to protect the data without consent from Posti.

Security Appendix

29.11.2021

Glossary

Term	Description
Active Directory (AD)	A directory service developed by Microsoft for Windows domain networks
Application programming interface (API)	An application programming interface connects computers or pieces of software to each other
Chief Information Security Officer (CISO)	Posti executive responsible for the organization's information and data security.
CISO office / Information security team	A team lead by Posti CISO responsible for providing support in information and cyber security matters.
Data Processing Agreement (DPA)	A legally binding contract that states the rights and obligations of each party concerning the protection of personal data
General Data Protection Regulation (GDPR)	Regulation in EU law considering data protection and privacy.
Group Cyber Steering Group (GCSG)	Posti's executive body with highest security decision making power in the organization.
Information Security Forum (ISF)	An international information security best practices organization
ISO27k	The ISO/IEC 27000-series information security standards published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).
Multi-Factor Authentication (MFA)	An electronic authentication method in which a user is granted access to a website or application only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism
NIST CSF	NIST Cybersecurity Framework is a guidance on how both internal and external stakeholders of organizations can manage and reduce cybersecurity risk. NIST CSF is published by US National Institute of Standards and Technology.
OWASP	The Open Web Application Security Project, is a non-profit online community that produces freely-available articles, methodologies, documentation, tools, and technologies in the field of web application security
PCI DSS	The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organizations that handle branded credit cards from the major card schemes.
Posti information	All data controlled by or processed at Posti
Record of processing activities (ROPA)	Record of processing activities is a written description of organization's personal data processing.
Security Operations Center (SOC)	Posti's centralized unit that deals with security issues on an organizational and technical level.
Supplier / Third-party	Refers to Posti clients and external suppliers, including organizations or individuals contracted by Posti to use, handle or process Posti information.