Annex II - Technical and Organizational Measures Including Technical and Organizational Measures to Ensure the Security of the Data

1 Technical Measures

1.1 Measures of encryption of personal data

1.1.1 Encryption

The strength of encryption considers the specific time period during which the confidentiality of the encrypted personal data is preserved.

The encryption algorithm is implemented correctly, by properly maintained software that is certified or evaluated for security and is without known vulnerabilities.

The keys are reliably managed (generated, administered, stored, linked to the identity of the intended recipient, and revoked), by the exporter.

Proprietary Encryption Algorithm(s) are reviewed and approved by Ericsson Security.

User credentials are encrypted during authentication when transmitted using a secure communications channel.

Passwords/authentication data are hashed at rest whenever the password is stored. Passwords are not stored or transmitted in clear text (human-readable form).

Encryption Standards (Minimums):

- AES128-bit or AES256-bit Cipher or
- 2048-bit RSA public keys

1.1.2 Cryptographic Key Management

- Keys are reliably managed (generated, administered, stored, linked to the identity of an intended recipient, and revoked)

- Encryption keys are stored separately than the information it is protecting
- Audit logs are kept, maintaining a complete history of each key, including creation, usage, and deletion.
- Keys are changed at least annually.
- Old keys are retired or destroyed.
- For high security keys, dual control or MFA is used for access.
- Key access is restricted on a need-to-know basis.
- Keys are changed when employees with key access change job duties or leave the company.
- Passwords used to protect cryptographic keys are as strong as the keys they protect.

1.2 Intrusion Detection & Prevention

Intrusion Detection & Prevention systems are deployed on networks processing personal data and are configured with rules to enable appropriate detection and prevention of intrusions that are a threat to the personal data.

1.3 Technical Vulnerability Management

Automated port scanning is performed regularly for internal/external web applications, hosts and networks.

Timeframes:

- Datacenter subnets are scanned internally at least monthly.
- Fully authenticated scans at least quarterly
- All external/public IP addresses are scanned from the internet at least monthly.
- Key office locations are scanned at least monthly depending upon the sensitivity of the operations at those locations.
- Other office subnets are scanned at least quarterly.

Identified vulnerabilities are scored, prioritized, and patched according to contextualized risk.

Penetration testing is performed at least once per year on systems processing personal data.

1.4 Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

Ericsson has a Business Recovery Plan to ensure critical systems have adequate backup and restoration capability. The backup and recovery procedures are tested.

1.4.1 Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing

Ericsson performs the following:

- ISO 27001 internal audits yearly
- ISO 27001 external audits yearly
- SOX based attestations for Entity Level Control yearly

- Organizational Information Security Risk Assessment at least yearly
- Business Continuity Management exercises
- Privacy assessments yearly

1.5 Measures for user identification and authorization

ACCESS CONTROL

Information systems have formal user registration and deregistration processes. Access to applications, systems and infrastructure follow the principle of "least privilege.

User access to information systems is granted to individual users. Shared access is not allowed.

Ericsson access utilizes Single Sign On with automated password policy enforcement.

Direct access to information systems containing any sensitive information from outside of the Ericsson corporate network uses user credentials and Multi Factor Authentication (MFA)

Ericsson has implemented a specific process in the employees ´leaving procedure for removing Active Sync profile from systems.

Authorization requests and provisioning are logged, tracked and audited.

Default credentials are either deleted or changed from default values.

VPN and direct Ericsson network access are limited to company managed and approved devices.

1.6 Measures for the protection of data during transmission

Secure transmission protocols protect the transmission of information over public and private networks.

- HTTPS (Transport Layer Security (TLS) protocol 1.2 or higher)
- SFTP
- SSH 2 (Secure Shell)
- IPSec (IP Security)
- S/MIME (Secure Multipurpose Internet Mail Extension)

Application

Application-level or client-side field level encryption is used to protect sensitive personal data elements.

1.7 Measures for the protection of data during storage

Systems without application-level encryption are encrypted at rest.

The encryption algorithm is implemented correctly and by properly maintained software without known vulnerabilities

1.8 Measures for ensuring physical security of locations at which personal data are processed

The Ericsson physical security framework takes local threats, vulnerabilities, and building codes into account and contains requirements based on industry standards.

Ericsson uses zones to segment physical access and provide protection according to, and in proportion with, the level of sensitivity and criticality of the information, assets and operations contained within.

Ericsson facilities are secure and protected by a defined perimeter with appropriate security barriers and entry controls.

Facilities are equipped with intrusion detection to monitor for unauthorized physical access.

Facilities are monitored to detect and respond to unauthorized physical access.

Access is restricted to authorized personnel only.

Access logs are maintained for at least 6 months to provide an auditable trail of access to facilities.

Visitors are registered and wear a visitor badge. Visitors granted access to restricted areas are escorted by Ericsson personnel.

Access rights to facilities are removed upon notification of separation or a change in job responsibilities.

Surveillance cameras or other surveillance devices monitor individual physical access to sensitive areas and exterior entries where appropriate. Footage from surveillance cameras is kept according to a decided retention time based on the purpose and acceptable use on the surveillance as well on local laws and regulations.

1.9 Measures for ensuring event logging

1.9.1 Logging, Analytics, & Event Management

Security event logs are collected across relevant systems with real-time monitoring, correlation, analysis, and alerts.

Relevant logs are collected across services and environments with potential tangible impact to personal data.

Access log files are maintained that relate to disclosure and access of EU/EEA Personal Data by a public authority in a third country, including judicial authorities.

A data access audit trail is maintained that includes:

- Strict logging of all access
- Ability to monitor access logs
- Ability to trigger alerts

Log retention meets the following:

All logs stored for 6 months as minimum

1.10 Measures for ensuring system configuration, including default configuration

System hardening is performed on all systems based on Ericsson guidelines or in accordance with supplier recommendations.

Changes to systems within the development lifecycle are controlled using formal change control procedures.

Change management processes are followed for any changes within Ericsson environment.

1.11 Measures for ensuring data minimization

Data collection is limited to the purposes of processing.

Ericsson privacy assessments include a review of personal data elements and their necessity in relation to the purposes for which they are being processed. Ericsson works with process and system owners to minimize personal data and meet compliance requirements.

Retention periods are defined and implemented for processing activities and supporting systems.

1.12 Measures for ensuring limited data retention

Personal data is retained only as long as necessary to fulfill the stated purposes, or as required by law or regulations, and is thereafter appropriately erased.

In accordance with Ericsson's data retention policies and in compliance with legal, statutory, regulatory, and contractual requirements, personal data is deleted when no longer required by:

- configuring systems to erase the information (e.g., after a defined period subject to the data retention policy or as a result of subject access request)
- removing data from cloud services
- deleting obsolete versions and unnecessary copies wherever they reside
- using Ericsson-approved deletion software to delete files permanently
- using Ericsson-approved providers of secure information disposal services
- degaussing/destroy hard disk drives and other media.

1.13 Measures for allowing data portability

Data portability is enabled through use of API gateway, reverse proxy solutions and as a last resort manual transfer with secure protocols, e.g., SFTP.

2 Organizational Measures

2.1 Measures for Privacy and Security governance and management

Ericsson has established an Information Security Management System (ISMS) in accordance with the ISO 27001 standard and maintains a global certification covering all market areas and business areas.

Ericsson has a security and privacy management board that governs security and an IT board that standardizes security and privacy across the Ericsson IT environment.

Information Security is managed at both the global and local levels with management involvement and supporting information security and IT security resources.

2.1.1 Information Security Policy

A set of policies for information security is defined, approved by management, published, and communicated to employees and relevant external parties.

The policies for information security are reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness.

2.1.2 Organization of Information Security

All information security responsibilities are defined and allocated.

Conflicting duties and areas of responsibility are segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization’s assets.

2.1.3 Audits and Assessments of Controls

Ericsson Corporate Audit conducts ISMS audits at regular intervals, as documented in the Corporate Audit annual Audit Plan.

Ericsson Group Management System (EGMS) Compliance Managers perform and support internal assessments of Ericsson ISMS according to the Internal Assessment Group Instruction.

External Assessments of Ericsson ISMS are performed at regular intervals by External Parties, e.g., as part of ISO 27001 certification.

2.1.4 Human Resource Security

Background verification checks on all candidates for employment are carried out in accordance with local laws and regulations.

Contractual agreements outline responsibilities for information security for both employees and external workforce.

All employees and external workforce are subject to non-disclosure agreements.

All employees and where relevant external workforce receive appropriate information security awareness, education, training and regular updates on organizational policies and procedures, as relevant to their job function.

Specific training is provided to the relevant employees on data privacy requirements.

A formal, communicated disciplinary process is in place to address employees who commit information security breaches.

2.1.5 Information classification and handling

Information is classified and labeled in accordance with the information classification scheme adopted by the organization.

Procedures for handling assets including personal data is developed and implemented in accordance with the information classification scheme.

Customer and personal data is classified and labeled as confidential and handled accordingly.

2.1.6 Risk Management

Information Security Risk Management (ISRM) is part of the Information Security Management System (ISMS). ISRM is a process for identifying, assessing, treating, and monitoring risks to Information Assets. ISRM is defined in accordance with the international standards ISO/IEC 27001:2022 and ISO/IEC 27005:2022 and aligned to Enterprise Risk Management (ERM) Framework and is a continual process of planning and performing risk assessments, reporting on activities, mitigating, and monitoring risks.

As part of Ericsson's third-party security risk management program, appropriate agreements with suppliers are put in place that process personal information, on Ericsson's customer´s behalf. These agreements include requirements for handling and protecting the information which is based on the Ericsson Information Security Requirements for Suppliers and supplementary measures identified as appropriate.

2.1.7 Business Application Management

Business applications are registered, linked to their supported processing activity, and reviewed for privacy compliance.

End-user developed applications are reviewed by IT Security and meet the same requirements as other standard Ericsson enterprise applications.

No direct access to databases storing personal data by end-users.

2.1.8 System Access Management

Roles with access to personal data undergo a formal approval process including approval of a manager.

The location of the computing devices accessing personal data are identified and logged.

Single Sign On (SSO) with multifactor authentication (where feasible) is used when accessing personal data or systems with access to personal data.

Access reviews are performed at least every year for systems containing or processing personal data.

2.2 Measures for ensuring confidentiality, integrity, availability and resilience of processing systems and services

Ericsson ensures confidentiality, integrity, availability and resilience of information, processing systems and services by implementing ISO 27001:2022 globally. Each respective market area, business area, group function, and functional area is then responsible for ensuring risks are managed through the Ericsson information security risk management process.

Ericsson information systems undergo assessment by Ericsson IT Security with sensitive and critical information systems undergoing a complete IT Security and Architecture Council review that includes the design of the system and all integrations.

Ericsson has two organizations that provide security monitoring Cyber Defense Center (CDC) and Product Security Response Team (PSIRT), where CDC focus on corporate solutions and PSIRT for product related investigations.

2.3 Measures for certification/assurance of processes, services and products

Ericsson is ISO 27001:2022 certified globally attesting to its commitment to controls that safeguard the confidentiality, integrity, and availability of information (including personal data) within its processes, information systems, and products.

As part of the ISO 27001:2022 certification process, Ericsson undergoes continual external audits. Additionally, Ericsson conducts internal audits against its information security management system and ISO 27001:2022 controls.

Products are developed in accordance with privacy by design and default and undergo an additional level of scrutiny as part of our Security Reliability Model which includes more stringent controls.

Organizational privacy controls are integrated into our entity level controls which are tested within each Ericsson unit annually.

Ericsson Business Processes are continually assessed for privacy compliance which includes tracking the flow of personal data between processes, information systems, suppliers and legal entities.

Solutions provided by or developed by third parties undergo the same assessments as internally developed tools in addition to an assessment of the supplier if applicable.

2.4 Measures for ensuring data quality

There are processes implemented in order to process only relevant, adequate, accurate, and kept up to date personal data according to the purposes.