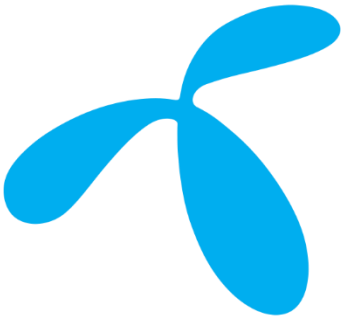
Privacy

GROUP POLICY



telenor group

Contents

GROUP POLICY

Privacy

Policy owner: *EVP People, Sustainability and External Relations*

Approver: *President & Group CEO*

Date of approval: *2023-07-13*

1. Purpose & Scope

The purpose of this policy is to ensure that processing of personal data in Telenor Companies adheres to fundamental data protection principles.

This policy shall apply to all processing of personal data in the Telenor Company, including processing that is carried out by third parties on the Telenor Company's behalf. The policy also applies to the processing of telecommunications data where this data falls under the definition of "personal data".

2. Fundamental Data Protection Principles

Lawfulness: ensure that processing of personal data is *lawful*.

Purpose limitation: ensure personal data is only processed to *fulfil defined purposes*.

Transparency: ensure *transparency* about processing of personal data.

Data minimisation: only process the least amount of personal data that is needed for a specific purpose.

Accuracy and security: ensure personal data is *accurate* and processed *securely*.

Data subject rights: ensure that data subjects can *exercise their legal rights*, and that they are not disadvantaged for doing so.

Accountability: demonstrate *accountability* with the above principles.

3. Requirements

3.1. Governance and Organisation

The Telenor Company shall implement the necessary roles and responsibilities for managing privacy in its organisation. The roles and responsibilities shall include both the line organisation and relevant governance and oversight functions.

The Telenor Company shall assess and document whether it is required to appoint a **Data Protection Officer (DPO)** and register this with local authorities. Where appointed, the Telenor Company shall ensure that the DPO is operationally independent and competent, and that it is assigned sufficient resources.

The Telenor Company shall ensure roles working with privacy have sufficient competence in privacy law, cyber security, governance, risk and compliance.

The adequacy of the privacy governance set-up, including the organisational structure, roles and responsibilities for managing privacy, in the Telenor Company shall be reviewed regularly.

3.2. Risk Management for Privacy

The Telenor Company shall identify, manage, and report on privacy compliance status and related risks.

The Telenor Company shall classify privacy compliance risks and issues according to the applicable risk taxonomy, as adopted by Telenor HQ.

3.3. Internal Controls for Privacy

The Telenor Company shall develop, implement and maintain internal controls for Privacy (control framework) that ensure compliance with this Privacy Policy, legal requirements and other internal and external requirements as applicable.

The Telenor Company shall ensure independent monitoring and reporting on the status and effectiveness of internal controls for Privacy.

3.4. Regulatory Management for Privacy

The Telenor Company shall identify and manage changes to external requirements, such as regulatory developments, impacting the management of privacy in the organisation.

3.5. Personal Data Inventory

The Telenor Company shall maintain an up-to-date inventory of its processing activities.

The inventory shall support legal and contractual transparency and accountability requirements, and applicable data subject rights.

The Telenor Company shall have procedures for maintaining and updating the inventory records to ensure adequate quality and audit trails.

3.6. Privacy Processes

The Telenor Company shall:

- define and implement a “Privacy by Design” framework to ensure implementation of fundamental data protection principles in the design and development of its products, processes, systems, and technologies.
- establish processes that secure the confidentiality, integrity, and availability of personal data.
- define data retention limits for personal data based on what is required for the purpose of processing, as well as to satisfy any local legal obligations, and shall implement them in all relevant processes and systems. ensure that all processes and IT assets/systems processing personal data are designed to support relevant data subject rights.
- maintain and make available a Privacy Notice that describes the purposes, processing activities and related use of personal data of the Telenor Company, and how external parties can inquire about the data processing. In case of digital services, the most important information should be made available in-context.
- ensure that the level of privacy risk to the data subjects associated with its processing activities is acceptable. In assessing the level of privacy risk, the following areas shall, as a minimum, be given adequate consideration:
  - Use of personal data perceived as particularly sensitive to the data subject
  - Use of data related to vulnerable groups of individuals, such as children
  - Use of large data sets, or combination of data sets from multiple sources
  - Security of processing
  - Use of new and unproven technologies, such as AI or algorithms for automated decision making
  - Profiling of individuals
  - Processing of communications content or metadata thereof
  - The ability of data subjects to exercise their rights

Where the risk to the data subjects is considered “high”, or otherwise as legally required, the Telenor Company shall secure that Data Protection Impact Assessments (DPIAs) are performed and necessary mitigations implemented prior to processing.

3.7. Privacy Incident Management

The Telenor Company shall ensure Privacy Incidents (as defined in this Policy) are handled adequately, involving all relevant internal functions, and according to applicable local legal requirements.

The Telenor Company shall ensure that it notifies the competent supervisory authority/authorities as required.

3.8. Communication and Training

The Telenor Company shall ensure the adequate knowledge and awareness of all employees on the fundamental data protection principles as described in this Policy and in applicable local law.

The Telenor Company shall provide additional, role-based training to employees in specific functions, where relevant.

3.9. Ethical use of Algorithms and AI on Personal Data

The Telenor Company shall identify and implement safeguards to manage privacy threats caused by Algorithms and AI and shall ensure that processing of personal data is lawful and ethical.

3.10. Business Partner Privacy Management

The Telenor Company shall regularly monitor, assess and manage privacy compliance risks related to the personal data processing performed by its Business Partners.

The Telenor Company shall adopt contractual clauses that govern the processing of personal data by its Business Partners.

3.11. Cross-Border Transfers

The Telenor Company shall assess and manage the risk of all cross-border transfers of personal data, considering local restrictions or conditions.

4. Internal Notification

The Telenor Company shall immediately notify the Chair of the Board in case of Privacy-matters that may have appreciable impact on the Telenor Company or Telenor.

5. Definitions and Abbreviations

Cross-border transfer (of personal data): the communication, disclosure or otherwise making available personal data by one legal entity ("data exporter") to another legal entity ("data importer").

Business Partner: see definition in Group Policy Business Partner Management.

Personal data: any information relating to an identified or identifiable natural person ("data subject").

Processing activity: Any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Privacy Incident: Any adverse event impacting the privacy of individuals, due to a breach of security, violation of privacy law or other sectoral law, or internal privacy policy and procedures.