Document name	Group Privacy Policy
Document owner	Torkel Sigurd, EVP Corporate Affairs
Other stakeholders	The Group Leadership Team, Helena Wanhainen (Head of Legal)
Document last revised (date)	May 2025
Version	1.3
Document approved by (name / date)	Tele2 Board of Directors, May 2025
Document first valid as of	May, 2018
Document valid until	Next revision, latest May 2028

Group Privacy Policy

Version Table

Revision	Date	Prepared and approved by	Information
1.0	2018-05-17	Stefan Backman, EVP General Counsel	First version.
1.1	2020-08-14	Stefan Backman, EVP General Counsel	Moved text to new template. General review, only minor updates.
1.2	2024-11-26	Data Protection Officer Tele2 Sverige AB	Revised version after review. Significant updates of text to simplify and correctly reflect the way of working. New section 4 added regarding DPO's role.
1.3	2025-05-14	Helena Wanhainen, Head of Legal	Clarification of the international frameworks that Tele2 aim to adhere to with respect to data protection.

1 Objective and Scope

A lot of information is being processed in Tele2 on a daily basis, e.g. corporate information as well as personal data, both within customer operations and internally. For Tele2 it is important to win and preserve the trust and confidence of our customers, employees, partners, suppliers and shareholders, by ensuring the right to privacy and data protection in our business and services while staying compliant with applicable laws and regulations. Providers of electronic communications services have a certain obligation to ensure the users' right to privacy and confidentiality of their communications and earn the trust of end-users for using electronic communications services in a modern digital world, both in the work life as well as in the private life.

The objective of this Group Privacy Policy is to set the boundaries of the Tele2 Privacy Management System by defining the general principles that apply within Tele2 with the aim to guide the organisation on how to make privacy related decisions and to ensure that privacy considerations are taken in all parts of our business. Tele2 strives to always process personal data in a responsible manner and to ensure an appropriate level of protection for personal data, both technically and organizationally.

This Group Privacy Policy, which is the basis on which all other steering documents within the Tele2 Privacy Management System is based upon, applies to everyone employed by Tele2, directly or indirectly. This includes members of the Board and the Leadership Team. For this policy, Tele2 means Tele2 AB and all its majority owned or controlled subsidiaries within the Tele2 Group.

2 Alignment with international and national frameworks

This policy sets out the data protection principles that Tele2 aims to adhere to, and reflects Tele2's commitment to international and national guidelines and directives, including but not limited to:

- The European Data Protection Regulation, GDPR
- National electronic communications legislation concerning data protection.
- The UN Global Compact
- The Universal Declaration of Human Rights (Article 12)
- The International Covenant on Civil and Political Right (Articles 17 and 19)

3 Compliance, roles and responsibilities

Legal entities within the Tele2 Group shall comply with all applicable privacy related laws, rules and regulations in the countries where we operate and shall also strive to comply with relevant applicable industry standards and best practices. As a telecom operator, when processing personal data in the daily operations, there is a need not only to comply with the General Data Protection Regulation (the GDPR) but also with electronic communications legislation, which constitutes *lex specialis* within the telecom sector, and other applicable legal acts and regulations concerning data protection.

This Group Privacy Policy highlights the fundamental data protection principles for a responsible and lawful processing of personal data. The principles set out below and other mandatory legal requirements shall be fully implemented across Tele2 Group. In cases of conflict between this policy and a mandatory local regulation, the local regulation shall prevail.

The legal responsibility for compliance of applicable data protection legislation is a responsibility for the highest management level of a legal entity in its role as a controller. The operational responsibility for compliance is decentralised and follows the ownership for information which is delegated internally. It is the responsibility of Tele2's managers to ensure adherence to this policy and to promote data protection awareness within their organisations.

Data protection awareness is an important part of the security practices within Tele2. All employees shall be provided with a yearly and mandatory training as well as, when necessary, additional specific training sessions, guidance and other awareness raising activities to ensure an appropriate level of protection of personal data. All employees have a responsibility to contribute a careful processing of personal data in their daily operations and they are also expected to be observant of any deviations from this policy which could imply non-compliance.

4 Data Protection Principles

Processing of personal data as a natural part of daily operations within Tele2 shall always follow the key principles of the GDPR. Compliance to these principles is fundamental for good data protection practices and an important part of the security culture.

4.1 Lawfulness, fairness and transparency

Personal data shall only be processed for ethical and legitimate purposes in accordance with at all times relevant legislation and in a manner that is fair and transparent in relation to those whose personal data is being processed (the data subjects). It shall always be clear to the individual which personal data that is processed, for what purpose, on which legal base and this information shall be given in an easily accessible and understandable manner. Transparency is very important for the data subjects to be aware of and to be in control of the processing of their personal data and to be able to exercise the data subject's rights.

4.2 Purpose limitation

Personal data shall only be processed for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Being clear about the purposes will ensure that the processing is fair and transparent, which is necessary to gain trust.

4.3 Data minimization

Tele2 shall only process personal data that is adequate, relevant and limited to what is necessary in order to fulfil the purpose(s) for which the data is being processed. Not more personal data than necessary shall be collected, stored or processed in any other way.

4.4 Accuracy

All processed personal data shall at all times be accurate and, where necessary, kept up to date and all inaccurate data shall be erased or rectified without undue delay. Such actions should be taken on a regular basis or upon request to ensure that personal data is not incorrect or misleading.

4.5 Storage limitation

Personal data shall only be stored in a format that permits identification of the data subject for as long as necessary for the purpose for which the data are being processed. Tele2 must not keep personal data for longer than necessary according to each applicable purpose for holding the relevant personal data and shall have processes to ensure to erase or anonymise such data when the retention period has ended. Such actions should also be taken on a regular basis or upon request to ensure a lawful processing.

Tele2 shall also ensure storage limitation to avoid any unnecessary costs and security concerns and, from a sustainability perspective, be mindful of our digital footprint and strive to ensure storage limitation in an as environmentally friendly way as possible.

4.6 Integrity and confidentiality

Personal data shall only be processed in a manner that ensures an appropriate level of security and confidentiality of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage. Appropriate technical and organizational measures to achieve this goal shall be implemented and regularly reviewed for the processing of all types of personal data according to assessments of the risk(s). As part of an ongoing and systematic information security management a process for incident management must be in place, including procedures for both internal and external reporting of privacy related security incidents.

Also, Tele2 shall comply with the obligation under electronic communications legislations to take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of networks and services and to ensure a high level of protection for end-users of electronic communications services.

4.7 Accountability

The principle of accountability requires Tele2 to take responsibility for the processing of personal data and how to comply with applicable data protection legislation in practice and on a daily basis. Tele2 shall at all times be able to demonstrate compliance with the above-mentioned principles as well as with current relevant data protection legislation and shall therefore implement necessary processes in order to achieve this goal.

5 Designation of a data protection officer

Tele2 companies shall designate a data protection officer when processing of personal data is carried out on a large scale, in accordance with article 37.1.b) of the GDPR. The data protection officers within Tele2 shall perform the legal tasks set out article 38 and 39 of the GDPR, e.g. to monitor internal compliance, inform and advise on data protection obligations, act as a contact point for data subjects as well as the supervisory authorities and directly report to highest management level.

The legal responsibility for compliance and the fulfilment of the principle of accountability is always the responsibility of the controller.