Group Guideline Data Protection

Guideline for the protection of the personal rights in dealing with personal data in the Telio Group

Inhaltsverzeichnis

I. Preamble 4
II. Scope 4
1. Legal nature of the Group Guideline Data Protection 4
2. Scope 4
3. Relationship to other legislation 5
4. Cessation and termination 5
III. Transparency of data processing 5
1. Duty to inform 5
2. Content and design of the information 6
3. Availability of information 7
IV. Admissibility requirements for the use of personal data 7
1. Principle 7
2. Permissibility of the use of personal data 7
3. Consent of the person concerned 8
4. Automated individual decisions 8
5. Special types of personal data 8
6. Data economy, data avoidance, anonymisation and pseudonymisation 8
7. Prohibition of Tying 9
V. Transfer of personal data 9
1. Types and purposes of the transfer of personal data 9
2. Transmission of data 9
3. Commissioned data processing 10
VI. Data quality and data security 10
1. Data Quality 10
2. Data security - technical and organizational measures 10
VII. Rights of the affected Person 11
1. Right to information 11
2. Right of Appeal and Right to Cancellation, Blocking and Correction 11
3. Right to clarification, opinion and remedy 12

4. Right to ask and to object 12
5. Exercise of the rights of the affected person 12
6. Text version of the Group guideline 12
VIII. Data protection organization 13
1. Responsibility for data processing 13
2. Data Protection Officer 13
3. Information obligation in case of infringements 13
4. Privacy checks 14
5. Employee commitment and training 14
6. Cooperation with supervisory authorities 14
7. Competent bodies for contacts and inquiries 15
IX. Final provisions 15
1. Review and revision of this Group Guideline 15
2. Contact list and company list 15
3. Procedural Law / Severability Clause 15

I. Preamble

The protection of personal data of customers, employees and other persons associated with the Telio Group is a key objective of all Telio Group companies.

The companies of the Telio Group are aware that the success of the Telio Group as a whole depends not only on the global interconnection of information flows, but above all on the trusting and secure handling of personal data.

In many areas, the Telio Group is perceived as a single entity from the point of view of its customers and the public. It is therefore the joint concern of the companies of the Telio Group to make an important contribution to the common entrepreneurial success through the implementation of this Group Guideline and to support the claim of the Telio Group as a supplier of high-quality and trend-setting products and services.

With this Group Guideline, the Telio Group creates a globally consistent and high level of data protection. Both for internal and cross-company data use and for both national and international data transmission. Personal data must be processed in the Telio Group at the recipient of data in accordance with the data protection principles, which apply according to the GDPR and the other legal bases.

II. Scope

1. Legal nature of the Group Guideline Data Protection

The Group Guideline Data Protection is a binding Group Guideline for the handling of personal data. It applies to all companies of the Telio Group, which have made them legally binding. The same applies to companies in which Telio Management GmbH has the right to demand the adoption of this Group Guideline or in which it has been voluntarily taken over by the companies. This applies regardless of the location of the data collection.

2. Scope

The Group Guideline Data Protection applies to all types of use of personal information in the Telio Group, regardless of where it is collected. Personal data is used by the Telio Group for the following purposes:

For the management of employee data in the context of the initiation, execution and completion of employment relationships as well as for addressing the employees to present products and services that the Telio Group or third parties offer to their employees.

Execution and processing of prison inmate telephony and other digital services and the telephony and other digital services for patients of forensic commitment institutions.

Execution and procession of services on MYTELIO in connection with the payment of funds to telephony accounts.

For the proper handling of other third parties, in particular shareholders or visitors, as well as for complying with mandatory statutory provisions.

Use of the data will be within the current and future business objectives of Telio Group companies, including but not limited to telecommunications and digital services for inmates of detention centers or law enforcement personnel, as well as IT services and consulting services.

3. Relationship to other legislation

The provisions of the Group Guideline Data Protection are intended to ensure a uniformly high level of data protection throughout Telio Group. Individual company obligations and rules governing the processing and use of personal data that exceed the principles set forth herein or that contain additional restrictions on the processing and use of personal data remain unaffected by this Group Guideline.

For the data collected in Europe, the requirements for the data protection compliant use of the data are basically and independently of the place of use according to the statutory provisions of the GDPR, and according to the legal regulations of the country in which the data was collected, but at least according to the requirements in this Group Guideline.

The validity of national regulations, which have been issued for reasons of state security, national defense, public security and the prevention, investigation and prosecution of criminal offenses, and which oblige the disclosure of data to third parties, shall remain unaffected by the provisions of this Group Guideline. If a company finds that material parts of this Group Guideline contradict national data protection regulations and this precludes the signing of the Group Guideline, the group data protection officer of the Telio Group must be informed immediately. The responsible supervisory authority of the company is to be mediating involved.

4. Cessation and termination

The binding effect of this Group Guideline ends when a company leaves the Telio Group or overrides the Group Guideline. However, the cessation or termination of the Group Guideline does not exempt the Company from the obligations and / or provisions of this Group Guideline for the use of data already transmitted. Any further transfer of data from or to this company can only take place if other appropriate procedural guarantees comply in accordance with the requirements of European law.

III. Transparency of data processing

1. Duty to inform

The affected persons are informed of the use of their personal data by the controller in accordance with the statutory provisions and the following provisions.

2. Content and design of the information

When personal data are collected from the affected person, the controller shall, at the time of collecting such data:

- The name and contact details of the person responsible and, where appropriate, his representative;
- If applicable, the contact details of the data protection officer;
- The purposes for which the personal data are to be processed and the legal basis for the processing;
- If the processing is based on Article 6 (1) (f), the legitimate interests pursued by the controller or a third party;
- Where appropriate, the recipients or categories of recipients of the personal data and
- where appropriate, the intention of the controller to transfer the personal data to a third country or international organization and the presence or absence of an adequacy decision by the Commission or, in the case of transfers pursuant to Article 46 or Article 47 or Article 49 (1) second subparagraph, a reprimand the appropriate or reasonable warranties and the possibility of obtaining a copy of them or where they are available.

In addition to the information referred to in the further indention one, the controller of the personal data of the affected person shall, at the time of collecting such data, provide the following further information necessary to ensure fair and transparent processing:

- The duration for which the personal data are stored or, if this is not possible, the criteria for determining that duration;
- the existence of a right to information on the part of the person responsible concerning the personal data concerned, as well as rectification or erasure, or limitation of processing or of a right to object to processing and the right to data portability;
- if the processing is based on Article 6 (1) (a) or Article 9 (2) (a), the existence of a right to revoke consent at any time without affecting the lawfulness of the processing on the basis of the consent to revocation;
- the existence of a right of appeal to a supervisory authority;
- whether the provision of personal data is required by law or by contract or is required for a contract to be concluded, whether the data subject is required to provide the personal data and the possible consequences of non-provision, and
- the existence of automated decision-making, including profiling, as referred to in Article 22 (1) and (4) and, at least in such cases, meaningful information on the logic involved and the scope and intended impact of such processing on the data subject.

If the controller intends to process the personal data for a purpose other than that for which the personal data was collected, it shall provide the affected person with information about that other purpose and all other relevant information referred to in the further indention two prior to such further processing.

Indentions 1, 2 and 3 shall not apply if and to the extent that the data effected person already possesses the information.

3. Availability of information

The information must be available to affected persons when collecting the data and thereafter whenever necessary.

IV. Admissibility requirements for the use of personal data

1. Principle

Personal data may only be used in accordance with the following provisions and only for the purposes for which they were originally collected.

The use of data already collected for other purposes is only permitted if the conditions for admissibility in accordance with the following provisions apply.

2. Permissibility of the use of personal data

The use of personal data may take place if one or more of the following conditions are fulfilled:

a. It is expressly permitted by law.
b. The person concerned has consented to the use of his data.
c. The use of the data is necessary for the fulfillment of the company's obligations under a contract with the data subject, including the contractual information and / or ancillary obligations, or for the implementation of pre- and / or post-contractual measures, the initiation or execution of the contractual relationship at the request of the data subject.
d. Use of the data is required to fulfill a contract or legal obligation to which the Company is subject.
e. The use of the data is necessary for the preservation of the vital interests of the affected person.
f. The use of the data is necessary for the performance of a task that is in the public interest or in the exercise of official authority and imposed on the company or the third party to whom the data are transmitted.
g. Processing is necessary for the realization of the legitimate interest exercised by the company or the third party to whom the data are transmitted, unless the legitimate interest of the interested party clearly outweighs it.

3. Consent of the person concerned

The consent of the affected person under this Group Guideline is effective if:

a. Consent has been given expressly and voluntarily and is based on an informed basis, which shows the person concerned in particular the scope of the consent. The declaration of consent must be sufficiently clear and inform the person concerned about his right of withdrawal at any time. For business models in which the revocation leads to the fact that contractual obligations cannot be fulfilled, the person concerned must be informed.
b. The consent is obtained in a form appropriate to the circumstances (text form). It may, in exceptional cases, be made orally, provided that the fact of the consent and the particular circumstances that make the oral consent appear reasonable are adequately documented.

4. Automated individual decisions

a. Decisions that assess individual aspects of a person and may have legal consequences or significant harm to those concerned should not be based solely on the automated use of data. These include, in particular, decisions that govern the data on the creditworthiness, professional capacity or state of health of the person concerned.
b. If, in the individual case, the factual necessity to make automated decisions exists, the person concerned must be informed of the result of the automated decision. He must have the opportunity to comment within a reasonable time. The opinion must be given due consideration before a final decision is taken.

5. Special types of personal data

a. The use of special types of personal data is only permitted if they are subject to legal regulation or the prior consent of the affected person. It may also take place when the processing is necessary in order to take into account the rights and obligations of the company in the field of labor law, provided that adequate safeguard measures are taken and the use is not prohibited by national law.
b. Before commencing such collection, processing or use, the Company (controller) shall inform and document the Company's Data Protection Officer. In particular, the nature, scope, purpose, requirement and legal basis of the use of the data should be taken into account in the assessment of admissibility.

6. Data economy, data avoidance, anonymisation and pseudonymisation

a. Personal data must be appropriate and relevant, taking into account the purpose of their use, and must not exceed the required level (data economy). Data may only be processed under a particular application if necessary (data avoidance).
b. In cases where it is possible and economically reasonable, procedures for the deletion of the identification characteristics of the data subject (anonymisation) or for the replacement of the identification features by other characteristics (pseudonymisation) are used.

7. Prohibition of Tying

The use of services or the receipt of products and / or services shall not be made conditional upon the data subject consenting to the use of his data for purposes other than those for the purposes of the contract and its performance. This shall only apply if the affected person is unable or unreasonable to use comparable services or to use comparable products.

V. Transfer of personal data

1. Types and purposes of the transfer of personal data

Personal data may be disclosed in such a way that the receiving agency is responsible for the data received or that it may use the data only in accordance with the instructions and conditions of the controller.

The transfer of personal data takes place exclusively for the permissible purposes in accordance with this Group Guideline in the context of the business-oriented orientation of the companies, their legal obligations or the consent of the affected persons.

2. Transmission of data

a. When a company submits data to entities located in a third country or carrying out cross-border data transfer, it must be ensured that such data is transferred in a lawful manner. Prior to the transfer, adequate data protection and data security requirements must be agreed with the recipient. In addition, personal data, in particular those collected in the EU or EEA, may only be transmitted to bodies outside the European Union if the adequate level of data protection has been ensured by this Group Guideline or by other appropriate measures. These may be the EU standard contractual clauses or individual contractual agreements that comply with the requirements of European law.
b. Based on the Telio Group's specifications and generally accepted technical and organizational standards, appropriate technical and organizational measures must be taken to ensure the protection of personal data during their transmission to another body.

3. Commissioned data processing

a. If another entity (processor) acts on behalf of a company (controller) in accordance with its instructions and for its purposes, the processors obligations of the contract shall be referred to in addition to the services to be provided in the contract. These obligations shall specify the instructions of the contracting authority regarding the way in which the personal data is processed, the purpose of the processing and the technical and organizational measures necessary to protect the data.
b. Without the prior consent of the controller, the processor may not use the personal data provided to him for the fulfillment of the contract for his own or other purposes. The involvement of subcontractors by the processor to fulfill the contractual obligations requires the prior information of the controller. The controller has a right to object to the assignment of subcontractors. In the case of the permissible involvement of subcontractors, the processor shall oblige the subcontractor accordingly to the agreements made between the processor and the controller.
c. The processors are selected by the companies according to their ability to meet the above requirements.

VI. Data quality and data security

1. Data Quality

a. Personal data must be correct and must be kept as up to date as possible.
b. Taking due account of the intended use of the data, appropriate measures must be taken to ensure that incorrect or incomplete data is deleted, blocked or, if necessary, corrected.

2. Data security - technical and organizational measures

Business processes, IT systems and platforms that collect, process or use personal information require companies to take appropriate technical and organizational measures to protect the data.

These measures include:

a. Deny access to data processing equipment used to process or use personal data,
b. to prevent data processing systems from being used by unauthorized persons,
c. to ensure that the persons entitled to use a data processing system can only access the data subject to their access authorization, and that personal data cannot be read, copied, altered or removed without authorization during processing, use after storage,
d. to ensure that personal data cannot be illegally read, copied, altered or removed during electronic transmission or during transport or storage on data carriers, and that it is possible to verify and determine to which places a transfer of personal data by means of data transmission provided,

e. to ensure that it can be subsequently verified and ascertained whether and by whom personal data has been entered, modified or removed in data processing systems,
f. to ensure that personal data processed on behalf of the controller can only be processed in accordance with the instructions of the controller,
g. to ensure that personal data are protected against accidental destruction or loss,
h. to ensure that data collected for different purposes can be processed separately.

VII. Rights of the affected Person

1. Right to information

Any affected person may request information from any controller using their data at any time about:

a. the data stored about him, including his or her origin and recipient,
b. the purpose of using the data,
c. the persons and entities to whom his data are regularly transmitted, in particular as far as the transfer abroad is concerned,
d. the regulations of this Group Guideline.

The information is to be given to the affected person in a reasonable time in an understandable form. It usually takes place in writing or electronically. The information about the regulations of this Group Guideline can be made by leaving a text version of the Group Guideline.

The companies may demand a fee for providing information if and insofar as this is permissible in accordance with the respective national law.

2. Right of Appeal and Right to Cancellation, Blocking and Correction

The affected person can at any time object to the use of his data vis-à-vis the controller if they are not used for legally binding purposes.

The right of objection also applies in the event that the affected person previously gave his consent to the use of his data.

Authorized requests to delete or block data must be submitted without delay. Such a request is in particular justified if the legal basis for the use of the data has been removed. If there is a right to delete the data, but deletion is not possible or unreasonable, the data must be blocked for inadmissible uses. Legal storage periods must be observed.

The affected person may at any time request the controller to correct the data stored about him, if these are incomplete and / or incorrect.

In the case of business models in which the opposition or deletion leads to contractual obligations not being fulfilled, the person concerned must be informed.

3. Right to clarification, opinion and remedy

If an affected person asserts a violation of his rights by improper use of his data, in particular in the form of a demonstrable infringement of this Group Guideline, the responsible companies must clarify the facts without culpable hesitation. In particular, in the case of a transfer of data to companies outside the European Union, the company established in the European Union has to clarify the facts and provide evidence that the Company which received the data did not infringe this Group Guideline or is responsible for a damage is done. Companies work closely together to establish the facts and give each other access to all the information they need.

The affected person may lodge an objection at Telio Group at any time if it suspects that a Telio Group company is not processing its personal data in accordance with the laws or provisions of this Group Guideline. The Group Data Protection Officer must be informed about the objection and consulted for processing. The substantiated objection will be remedied within a reasonable period of time and the affected person will be informed accordingly.

If several companies are affected by an objection, the Group Data Protection Officer coordinates all relevant correspondence with the affected person. The Group Data Protection Officer has at all times a right of entry and takeover.

Notifications of a data protection incident must be able to be made in a suitable manner (for example, via a functional mailbox of the data protection area or a direct contact person on the Internet).

The Data Protection Coordinator of the affected company must immediately inform the Group Data Protection Officer about a data protection incident on the basis of the designated reporting processes.

4. Right to ask and to object

Anyone affected has the right to contact the Group Data Protection Officer of the Telio Group at any time with questions and complaints about the application of this Group Guideline. The company closest to the subject or the company from which the data was collected ensures that the rights of the affected person are transferred to the other competent companies.

5. Exercise of the rights of the affected person

Affected parties may not be disadvantaged because of the use of the rights described here. The way of communicating with the person concerned - e.g. telephone, electronic or written - should, as appropriate, comply with the request of the affected person.

6. Text version of the Group guideline

Everybody gets on request a text version of this Group Guideline sent.

VIII. Data protection organization

1. Responsibility for data processing

The companies of the Telio Group are required to ensure compliance with the statutory privacy policies and this Group Guideline.

2. Data Protection Officer

It is an independent data protection officer to order. Its task is to ensure that the various organizational companies of the Telio Group are advised of the legal, corporate and internal requirements for data protection and, in particular, this Group Guideline. The Data Protection Officer monitors compliance with data protection rules through appropriate measures, in particular random checks.

The controller ensures that the Data Protection Officer has the necessary competences for the legal, technical and organizational evaluation of data protection relevant measures.

The Group Data Protection Officer is to be provided with the appropriate financial and human resources by the person responsible for the performance of his duties.

The Data Protection Officer is to be granted a direct reporting right to the company management. He is organizationally linked to the management.

The implementation of the specifications of the Group Data Protection Officer and the data protection strategy of the Telio Group is the responsibility of the controller.

All divisions of the company are required to inform the Data Protection Officer about all developments regarding the IT infrastructure, the network infrastructure, business models, products, personal data processing and the associated strategic planning. The Data Protection Officer should be involved in new developments at an early stage to ensure that all data protection concerns are taken into account and evaluated.

The Group Data Protection Officer coordinates cooperation and coordination on all important data protection issues in the Telio Group. If necessary, it informs the Executive Board about current developments or formulates recommendations.

It is the task of the Group Data Protection Officer to advise those responsible in developing the privacy policy of the Telio Group. The privacy team will be appropriately involved. A joint exchange between the Group Data Protection Officer and the data protection team takes place four times a year.

3. Information obligation in case of infringements

The data protection officer must be informed immediately by the company concerned of any breaches or concrete indications of a breach of data protection regulations, in particular this Group Guideline. The

Company Data Protection Coordinator will also inform the Group Data Protection Officer if the applicable laws of a company materially change in the sense of this Group Policy.

4. Privacy checks

Verifications of compliance with this Group Guideline and the resulting level of data protection are made through controls performed by the Group Data Protection Officer on the basis of an annual control plan, as well as through other measures such as Data Protection Coordinator checks or reports.

If weaknesses are identified during an inspection, these must be remedied by appropriate measures by the company. The Group Data Protection Officer advises on the implementation of the measures. If these are not implemented without sufficient justification, the Group Data Protection Officer assesses the effects on data protection and forwards the findings to the responsible person.

The Data Protection Coordinators of the companies or other organizational units equipped with an audit order additionally check compliance with the data protection requirements on the basis of the checklists provided by the controller, which were created with the assistance of the Data Protection Officer.

Unless otherwise required by law, the Group Data Protection Officer is authorized to review the proper use of personal information for all companies. To this end, companies provide comprehensive access and insight to the information that the Group Data Protection Officer deems necessary for the clarification and assessment of a situation. The Group Data Protection Officer can issue instructions in this connection.

5. Employee commitment and training

The companies commit their employees to the data and telecommunications secrecy at the latest when they start their work. As part of the commitment, the employees are sufficiently trained in the interests of data protection. To do this, the company sets up suitable processes and provides materials.

Employees are regularly trained, at least every two years, on the basics of data protection. The companies can develop and carry out the training for their own employees. The implementation of the training courses is to be documented by the person responsible for HR and reported annually to the controller as well as to the Group Data Protection Officer.

Materials and processes can be centrally provided for the commitment and training of Telio Group employees.

6. Cooperation with supervisory authorities

The companies agree to cooperate with the supervisory authority responsible for them or the data submitting company in a trusting manner, in particular to answer inquiries and make recommendations.

7. Competent bodies for contacts and inquiries

Responsible for contacts and inquiries about this Group Guideline are the Data Protection Coordinators of the companies or the Group Data Protection Officer. The Group Data Protection Officer also names the contacts with the Data Protection Coordinators of the companies on request.

The Group Data Protection Officer is over Data.Protection.Officer@tel.io reachable.

IX. Final provisions

1. Review and revision of this Group Guideline

The Group Data Protection Officer regularly reviews this Group Guideline, at least once a year, to determine whether it is compatible with the applicable laws and advises on its adaptation by the controller.

The Group Data Protection Officer informs all companies that have made the Group Guideline Data Protection obligatory about the content changes.

2. Contact list and company list

The Group Data Protection Officer maintains a list of companies that have bindingly introduced this Group Guideline and their contact persons. He keeps them up to date and informs affected persons or the data protection authority on request.

3. Procedural Law / Severability Clause

The Group Guideline is subject to the procedural law of the Federal Republic of Germany in disputes.

If any provision of this Group Guideline is or becomes invalid, it will be deemed to be replaced by terms that are closest to the original intent of this Group Guideline and the deleted provision. In case of doubt, the relevant provisions of the European Union on data protection apply accordingly in these cases or in the case of a lack of regulation.