Appendix 7 Processing of commissioned data

Version	1.0
Issue Date	28.04.2023
Replaces version	-
Modifications	New document
Valid from	01.07.2023

1. Introduction

This Appendix specifies the obligations of the Parties in relation to the requirements of the Swiss Data Protection Law (DSG) ([6] Appendix 4) and the European Data Protection Regulation (EU-DSGVO 2016R0679) ([9] Appendix 4). It supplements the Teldas contracts “Use of the TSP INet-Server for Numbers when changing the TSP (Number Portability)” and “Use of the TSP INet-Server for INA Services”.

Teldas (Order Processor) processes personal data (“Relevant Data”) on behalf of the User (Controller) in accordance with the provisions of this Appendix.

2. Subject matter and duration of the agreement

The subject of the mandate as well as the type and purpose of the processing result from the User contract.

The present agreement shall enter into force upon mutual signature of the User contract. The term of this agreement is based on the term of the contract "Use of the TSP INET server for Numbers when changing the TSP (Number Portability)" and/or "Use of the TSP INet server for INA services".

The obligations under this Agreement are in addition to and do not limit the obligations set out in the contract "Use of the TSP INET Server for Numbers when changing TSP (Number Portability)" and/or "Use of the TSP INet Server for INA Services". Regarding the technical-organisational measures (TOM) defined generically in an annex to this agreement, the provisions of this agreement shall take precedence in the event of contradiction.

3. Duties of Teldas

(1) Teldas shall process personal data exclusively in accordance with the provisions of this Agreement or any further documented instructions of the User, unless Teldas is legally obliged to further processing. Teldas shall notify the User of such obligations prior to the processing unless the relevant law prohibits such notification due to an important public interest.

(2) Teldas shall inform the User immediately if, in its opinion, an instruction given violates legal provisions. Teldas is entitled to suspend the execution of the corresponding instruction until it is confirmed or changed by the user at Teldas after verification.

(3) The instructions are initially laid down in this agreement and may subsequently be amended, supplemented, or replaced by the user in written form or in an electronic format (text form) to Teldas by individual instructions insofar as these can be implemented by Teldas within the framework of the contractually agreed services and are objectively reasonable. If such instructions lead to additional costs for Teldas or a changed scope of services, the contractual contract amendment procedure shall apply.

(4) Teldas shall not use the data provided for processing for any other purposes, in particular not for its own purposes. Copies or duplicates of the personal data shall not be made without the User's consent. Excepted are technically necessary temporary duplications, as far as an impairment of the level of data protection agreed upon here is excluded.

(5) Teldas commits itself to observe the relevant, general data protection regulations within the scope of data processing. Teldas confirms that the persons employed by it for data processing are familiar with the relevant provisions of data protection and this agreement. Corresponding training and awareness-raising measures shall take place at regular intervals.

(6) Teldas declares in a legally binding manner that it has committed all persons entrusted with the data processing to confidentiality prior to the start of the activity or that they are subject to an appropriate legal obligation of confidentiality. In particular, the confidentiality obligation of the persons entrusted with the data processing shall remain in force even after termination of their activity and leaving Teldas (or subcontractors).

(7) Teldas shall support the User to the extent necessary to respect the rights of the data subjects under chapter 4 DSG or chapter 3 EU-DSGVO, so that the User can fulfil its tasks within the legal deadlines at any time and Teldas shall provide the User with all information necessary for this purpose. If a data subject sends a request directly to Teldas, the latter shall forward the request to the user without delay. Teldas may only provide information to third parties or data subjects with the prior consent of the User.

(8) Teldas shall support the User in complying with the obligations set forth in Art. 22-24 DSG or Art. 32 to 36 EU GDPR (data security measures, notifications of personal data breaches to the supervisory authority, notification of the person affected by a personal data breach, data protection impact assessment, prior consultation). Also, Teldas shall inform the User without delay if it becomes aware of breaches of the protection of the relevant data at the User's premises or at the premises of one of its subcontractors.

(9) If the User is subject to inspection by supervisory authorities or other bodies, Teldas undertakes to assist the User to the extent necessary insofar as the processing is concerned in the order.

(10) Teldas shall correct, delete or restrict the processing of personal data from the commissioned relationship if the User requests this and there are no legitimate interests of Teldas or legal requirements against it.

(11) Teldas has not appointed a data protection officer according to Art. 37 EU-DSGVO, as the legal necessity for an appointment does not exist. The contact person for data protection issues at Teldas is listed in Appendix 1.

4. Subcontractors

(1) Teldas shall be entitled to engage subcontractors but shall inform the User in advance if it engages new subcontractors or replaces existing ones after the entry into force of this Agreement. The list of subcontracted processors is published in Annex 2, item 6.

(2) The User may object to the appointment of a new subcontracts for good cause under data protection law in writing within a period of 30 days. If there is an important reason under data protection law and if a mutually agreeable solution cannot be found between the parties, the User shall be granted a right of termination with respect to the service affected thereby.

(3) Teldas shall enter into agreements with its subcontractors to the extent necessary to ensure the obligations under this Agreement.

(4) Upon request, the User shall be granted access to the relevant data protection provisions between Teldas and the subcontractor.

(5) In the event of justified suspicion of a breach of the obligations laid down herein, the User shall be entitled to carry out checks to the extent stipulated herein, also at subcontractors, or to have such checks carried out by third parties. In any case, the principle of proportionality shall be observed within the scope of such controls and the interests of Teldas as well as its sub-contractors worthy of protection (namely confidentiality) shall be adequately taken into account.

(6) Teldas shall be responsible for the lawfulness of the data processing itself, including the lawfulness of the subcontracted processing.

5. Technical and organisational measures (TOM)

(1) Teldas shall take all necessary measures to ensure the security of the processing pursuant to Art. 8 DSG or Art. 32 EU-DSGVO. The measures shall ensure a level of protection appropriate to the risk about confidentiality, integrity, availability, and resilience of the systems. The state of the art, the implementation costs and the nature, scope, and purposes of the processing as well as the varying likelihood and severity of the risk to the rights and freedoms of natural persons shall be taken into account.

(2) The required technical and organisational measures are documented in Annex 1 to this agreement.

(3) Significant changes shall also be documented immediately. Teldas may adapt the agreed TOM at any time as long as the agreed level of protection is not undercut (cf. Clause 9 Changes to the Agreement).

(4) Insofar as the security measures taken do not or no longer meet the requirements of the user, the latter shall notify Teldas in writing.

6. Obligations of Teldas after termination of the contract

(1) After termination of the commissioned processing, Teldas is obliged following an order of the User, to destroy all processing results and transmitted personal data and their copies, unless there is a legal obligation to store the personal data (as per Art. 28 para. 3 sentence 2 let. G EU-DSGVO). The customer data are contained in so-called work order data. The data storage length is specified in the document "Archiving Rules" (See https://extranet.teldas.ch/documents).

(2) If Teldas processes the data in a special technical format, it is obliged to return the data after termination of this agreement either in this format or, at the User's request, in the format in which it received the data from the User or in another common format. The client data is contained in so-called work-orders. The data can be downloaded via a web-based manual interface or via WS in a common format (see specifications under https://extranet.teldas.ch/documents).

7. Verification options, reports and audits

The User is entitled to:

(1) Monitor compliance with the technical and organisational measures taken by Teldas as well as with the obligations laid down in this agreement to a reasonable extent himself or through third parties on site. The persons entrusted with the control shall be granted access and insight by Teldas as far as necessary. Teldas shall provide the necessary information to document the compliance with the agreed obligations. In any case, the principle of proportionality shall be observed within the scope of such controls and the interests of Teldas worthy of protection (namely secrecy) shall be adequately taken into account.

(2) Inspections at Teldas shall be carried out without avoidable disruption of its business operations and, except in case of urgent reasons, after reasonable advance notice and during Teldas' business hours.

(3) Unless otherwise agreed, the User shall bear all costs of such audits (including proven internal costs of Teldas incurred in participating in the audit).

(4) If violations of this Agreement or deficiencies in the implementation of the obligations are identified after the submission of evidence or reports or during an audit, Teldas shall implement appropriate corrective measures without delay and free of charge.

8. Duties of the User

The user is obliged:

(1) to ensure that the lawfulness of the processing is given in accordance with Art. 6 para. 1 DSG or Art. 6 para. 1 EU-DSGVO;

(2) to ensure that the rights of the data subjects pursuant to Chapter 4 DSG or Chapter 3 EU-DSGVO are safeguarded;

(3) to transmit orders and instructions to Teldas as a rule in writing or in a documented electronic format. Verbal instructions shall be confirmed in writing or in a documented electronic format;

(4) to inform Teldas without delay of any errors or irregularities in the verification of the results of the assignment;

(5) to keep confidential all knowledge of business secrets and data security measures of Teldas obtained in the course of the contractual relationship. This obligation shall remain in force even after termination of the contract;

(6) to name the contact person for data protection questions arising within the framework of the contract as well as the data protection officer in cases where this is required according to Art. 37 EU GDPR. See Appendix 1.

9. Amendments of the Agreement

The user can demand changes (including supplements) of this agreement from TELDAS, if and as far as this is necessary for the compliance of mandatory data protection law to be observed by the users.

TELDAS shall inform the users in good time by email about necessary adjustments or amendments of the annexes 1 and 2. The amendments shall be deemed to be approved if the user does not object to them within 30 days from receipt for important reasons.

Annex 1: Technical organisational measures (TOM)

The following chapters describe the measures taken by Teldas about the protection of personal data according to Art. 8 DSG resp. 32 EU-DSGVO). The assessment of whether the technical and organisational measures described below are adequate to protect the data entrusted to Teldas for processing is the sole responsibility of the User.

Within the framework of the contractual relationship, each Party processes personal data about employees and other auxiliary persons of the other Party. For the purposes of implementing the contract and maintaining the contractual relationship, the Parties process this personal data under joint responsibility on their own systems and using appropriate technical and organisational measures to protect the data. This type of data processing is not subject to the regulations on order data processing. Contacts of employees or other auxiliary persons of the Users shall be made accessible to other Users of Teldas for necessary operational, administrative and billing purposes between Providers.

1. Confidentiality

(1) **Entry control:** No authorised access to data processing facilities.

The INet database is stored in a secured data centre of the Teldas sub-processor, See Data Center DSC Wankdorf of Swisscom:

https://www.swisscom.ch/fr/about/entreprise/durabilite/objectifs-cr-et-resultats/centre-de-calcul-wankdorf.html and Tier4 certification by external body: https://uptimeinstitute.com/TierCertification/allCertifications.php?page=1&ipp=All&clientId=251&countryName=&tierLevel.
To gain access to secured zones, a badge or key is required. The issuance of keys to authorised persons is logged, and visitors must register and are escorted by responsible staff in the secured zones

(2) **Access control:** No authorised system use.

Access to Teldas systems is always through personalised identifications of Teldas' appointed persons.
Access to the systems is always protected with at least a password or an equivalent authentication feature and the associated digital identification. The access data are stored in such a way that no direct derivation of the valid authentication feature is possible if this data were to become accessible.

Passwords must meet complex requirements, be 8 characters long and consist of at least three classes of the following elements: upper case letters, lower case letters, numbers, special characters.

(3) **Authorisation control:** No unauthorised reading, copying, modification or removal within the system.

Access to the Teldas INet-Server is based on User authorisations with assignment of different roles. Client files are only available to the providers (Donor and Recipient) and authorised persons (Teldas Helpdesk and Support Teams) affected by the porting order. Access logs are stored for a defined period of time.
Access with increased rights for the administration of the Teldas INet system is mapped with strong two-factor authentication. All logins, logouts and incorrect logins are centrally logged and stored for a defined period of time.
Accesses to the systems are centrally logged and analysed if necessary.

(4) **Separation control:** Separate processing of data collected for different purposes.
Teldas ensures that Users' data cannot be viewed by each other. To this end, up-to-date security procedures are used to ensure the separation of User data at the logical level.

Work-order files are separated from porting files. Only Donor and Recipient can view details of the work-order file.

2 Integrity

(1) **Transport control:** No authorised reading, copying, modification or removal during electronic transmission or transport.

Personal data is delivered by the Recipient with two-factor authentication via the Website or HTTPS secured and encrypted connection (SSL) via a Web Service.

(2) **Input control:** Determining whether and by whom personal data have been entered, modified or removed from data processing systems.

The user is responsible for the correct handling and modification of the data. Generation and changes to WO data are logged (user ID is visible in the WO data).

3 Availability and resilience

(1) **Availability control:** Protection against accidental or deliberate destruction or loss. Data is backed up to hard disk systems in another data centre with sufficient geographical distance between the two locations.

Uninterruptible power supply: The INet-System is housed in a Swisscom Pier 4 data centre. The permanent storage in the data centres is protected against loss with physical protection measures. This includes redundant power supplies and the necessary systems to enable self-sufficient operation for a defined period of time.

Backup strategy (online/offline; on-site/off-site): regular back-ups are carried out to minimise data loss. The INet system is backed up every 4 hours.

Virus protection, firewall are in place.

The standard patch management process ensures that patch announcements are assessed and installed on the relevant systems after a check.

(2) **Fast recoverability:** Database can be temporarily restored to cloud environment within 24 hours. A contingency plan is in place to get the system operational again within 24 hours.

4. Procedures for regular review, assessment and evaluation.

(1) **Data protection management:** periodic meetings between Teldas and Teldas subcontractors take place. The Teldas main subcontractor (Swisscom) is subject to an annual ISAE3402 report based on an audit by PWC.

(2) **Incident response management:** Users can report errors to the Teldas helpdesk and tickets are then opened and tracked.

(3) **Privacy-friendly defaults** for each new project, security and privacy aspects are prioritised.

(4) **Order control:** No commissioned data processing without appropriate instruction from the User.

Teldas carefully selects possible subcontractors with access to the data and assigns the relevant data protection responsibilities to the suppliers. The new Teldas subcontractors will be named to the User for each individual service purchased.

(5) **Security audits** are commissioned periodically. Security risks are assessed, quantified, and prioritised.

Annex 2: Description of the data processing

1. Execution place of the commissioned processing

All data processing activities are carried out exclusively within Switzerland.

The adequate level of data protection in Switzerland is derived from an adequacy decision of 26 July 2000 of the European Commission pursuant to Art. 45 EU-DSGVO.

2. Categories of data and data subjects

The User makes personal data available to Teldas for processing in the context of the number portability service and INA service. It concerns subscriber data of holders of official telephone numbers and who wish to change providers.

The personal data provided by the User (Art. 5a DSG or Art. 4 Nr 1 EU-DSGVO) belong to the following categories of data:

- Personal information such as surname, first name
- Private or business contact information, such as telephone number, address.
- INA reference code assigned by Bakom to the INA number holder.

Teldas and its subcontractors do not process any relevant data which is subject to a special legal obligation of secrecy.

3. Type of processing

The processing of subscriber data concerns porting data (surname, first name, address, telephone number) of the customer, which are stored in so-called WO data and are part of the porting process. In case of problems with porting, it is possible to follow the history. The personal data transferred will not be changed by Teldas. Data is entered by the new provider ("Recipient") and is visible to the current provider ("Donor") but is not changed by him or by the system.

The data retention period and deletion of client data is defined in the document [13] of Appendix 4.

4. Processing purposes

Teldas processes the relevant data exclusively in accordance with the provisions of the contract "Use of the TSP INET server for Numbers when changing the TSP (Number Portability)" and/or "Use of the TSP INet server for INA services". The fulfilment of legal, regulatory or official obligations by Teldas remains reserved.

The personal data transmitted will be processed for the following purposes:

- Number Portability (see [15] Appendix 4): Personal customer data is not published publicly and is only visible to the new ("Recipient") and current ("Donor") provider. They are used to terminate the contract with the current provider.
- INA processes (see [18] Appendix 4).
- So-called WO data are required for billing between providers for SLA disputes, as well as for the billing of transaction-based fees by Teldas to the User.

5. Disclosure of relevant data to subcontractors (e.g. group companies, suppliers)

Hereafter the list of Teldas subcontractors with a description of the type of personal data processed:

Company	Address	Country	Scope of the data processing
MNC Mobile News Channel SA	Avenue de la Gare 10, 1003 Lausanne	CH	Outsourcing Partner for SMS delivery and receipt
Swisscom (Schweiz) AG	Alte Tiefenaustrasse 6, 3050 Bern	CH	Outsourcing Partner for Application Operations
Open Web Technology SA	Avenue de Rhodanie 40C Building C, 4th floor, 1007 Lausanne	CH	Outsourcing Partner for Application Management

6. Data Breach Reporting / Security Incident Reporting

Teldas reports data protection breaches through an ITBd message that Users can subscribe to under the Teldas Extranet (https://extranet.teldas.ch/account).