TELENOR'S PRODUCT-SPECIFIC DATA PROCESSING TERMS FOR TELENOR ENTERPRISE MOBILITY MANAGEMENT (EMM)

1. Introduction

1.1 These product-specific data processing terms ("**Product-specific Data Processing Terms**") shall apply to the processing of personal data that Telenor A/S (company reg. no. 19433692, Frederikskaj 8, 2450 Copenhagen) ("**Data Processor**") is conducting on behalf of the Customer ("**Data Controller**") when delivering the product ("**Telenor Enterprise Mobility Management (EMM)**") in accordance with the agreement between the Data Controller and the Data Processor ("**Agreement for Telenor Enterprise Mobility Management (EMM)**[1]").

1.2 These Product-specific Data Processing Terms are defined in accordance with Article 28(3) of the General Data Protection Regulation ("**GDPR**") and, together with Telenor's General Data Processing Terms, set forth the rights and obligations of the Data Controller and Data Processor when processing personal data on behalf of the Data Controller in relation to the delivery of Telenor EMM.

1.3 These Product-specific Data Processing Terms form an integral part of Telenor's General Data Processing Terms and apply from the effective date of these general data processing terms.

[1] The agreement may, among other things, be drawn up as a product agreement, a SKI agreement, terms and conditions, or another type of agreement. It depends on the specific type of agreement entered into between Telenor and the Customer.

Appendix A Information about the processing

The Data Processer delivers Telenor EMM and the related services to the Data Controller, as per the Agreement for Telenor Enterprise Mobility Management (EMM).

A.1. The purpose of the data processor's processing of personal data on behalf of the data controller is

The purposes of the Data Processor's processing of personal data on behalf of the Data Controller are to implement and configure the Data Controller's Telenor EMM and support the Data Controller's use of the solution.

A.2. The data processor's processing of personal data on behalf of the data controller shall mainly pertain to (the nature of the processing)

The nature of the processing of personal data carried out by the Data Processor on behalf of the Data Controller primarily consists of configurating Telenor EMM on the Data Controller's mobile devices with the possibility to provide support and service to the Data Controller in using the solution.

Telenor EMM enables the Data Controller's administrator to manage mobile devices, including blocking, locking, and wiping these devices.

Managed Service – OneSupport Admin, OneSupport Admin 24/7, and OneSupport All, Device Management
If the Data Controller opts for Service by Telenor, which constitutes a separate product agreement with the Data Processor, the nature of the processing may also include administration, further configuration, and ongoing service.

A.3. The processing includes the following types of personal data about the data subjects

The solution is developed to include the processing of general personal data covered by Article 6 of the GDPR. The following types of general personal data will be processed in connection with the Data Processor's provision of Telenor EMM.

When creating the Data Controller's users in Telenor EMM, the following personal data is processed:

- Name
- Email address
- User ID

- Telephone number
- Any AD attributes, if the Data Controller uses LDAP mapping

During the Data Controller's use of the solution, the following personal data about the Data Controller's users, which are linked to the user's device, is processed:

- Name
- Email
- MSISDN
- Assigned devices
- Serial number
- UDID
- MAC address
- IP address
- IMSI number
- GPS location, if enabled by the Data Controller
- Apps downloaded by the employee will appear in the log. The Data Processor and sub-processors can see the apps but cannot view the content of the downloaded apps.

An exhaustive overview of the processing and storage of data types is provided in Appendix D.

The solution is not designed for the purpose of processing special categories of personal data under GDPR Article 9 (sensitive personal data).

A.4. Processing includes the following categories of data subject:

The Data Controller's employees (users).

A.5. The data processor's processing of personal data on behalf of the data controller may commence after these data processing terms have entered into force. Processing has the following duration:

The duration of the processing of personal data corresponds to the duration of the provision of the service. The processing is therefore not time-limited but continues until the Agreement for Telenor Enterprise Mobility Management (EMM) is terminated or cancelled by either party.

The Data Controller is responsible for the ongoing deletion and creation of new users.

Appendix B Authorised sub-processors

B.1. Approved sub-processors

On commencement of these Product-Specific Data Processing Terms, the Data Controller authorises the engagement of the following sub-processors:

NAME	ADDRESS	DESCRIPTION OF THE PROCESSING	PERSONAL DATA PROCESSED
SUB-PROCESSOR OF THE DATA PROCESSOR			
Seven Principles Solutions & Consulting GmbH	Ettore-Bugatti-Strasse, 6-14, 51149, Köln, Germany	Development and provision of core elements and software for the solution, as well as 3rd line support	• Full name • Email • User ID • MSISDN • Assigned devices • GPS location, if enabled by the Data Controller
SUB-PROCESSOR'S SUB-PROCESSORS			
7P Austria GmbH	Pottendorfer Str. 25-27, 1120, Wien, Austria	Development and provision of core elements and software for the solution, as well as 3rd line support	• Full name • Email • User ID • MSISDN • Assigned devices • GPS location, if enabled by the Data Controller
7P Nordics AS	Mustamäe tee 46, 10621 Tallinn, Estonia	Provider of 3rd line support	• Full name • Email • User ID • MSISDN • Assigned devices • GPS location, if enabled by the Data Controller
Exoscale	Boulevard de Grancy 19A, 1006 Lausanne, Switzerland	Data center	• Full name • Email • User ID • MSISDN • Assigned devices • GPS location, if enabled by the Data Controller

The Data Processor shall not be entitled – without the Data Controller's written authorisation – to engage a sub-processor for a 'different' processing than the one which has been agreed upon or have another sub-processor perform the described processing.

B.2. Notice for objection to change in sub-processors

The Data Controller shall, within 10 days from the date of the Data Processor's notification of any planned changes regarding the addition or replacement of sub-processors, submit a written objection to the Data Processor regarding the sub-processor(s) in question.

If the Data Controller objects, the objection must include the specific reasons for the objection.

Appendix C Instruction pertaining to the use of personal data

C.1. The subject of/instruction for the processing

The Data Processor's processing of personal data on behalf of the Data Controller is carried out as follows:

The Data Processor distributes Telenor EMM, which is developed, delivered, operated, and hosted by the sub-processor mentioned in section B.1.

The Data Processor implements and sets up Telenor EMM on the Data Controller's mobile devices.

The Data Processor configures Telenor EMM on the Data Controller's mobile devices based on the Data Controller's specification requirements. During the configuration, the Data Processor must access personal data, including name, email address, and potentially department of the relevant employees of the Data Controller.

Once the solution is set up for the Data Controller, the Data Controller decides whether the Data Processor shall have access to the Data Controller's solution for the purpose of managing the solution and providing 2nd line support. The Data Controller may also choose that the Data Processor shall not provide support on regular basis but instead grant access to the Data Processor in specific support cases.

The Data Processor is only a data processor for the processing of personal data falling within the scope of delivering the Data Controller's Telenor EMM. Other processing of the Customer's telecommunications data processed as part of Telenor's transmission of communication in the network is not covered by the general Data Processing Terms or these Product-Specific Data Processing Terms.

C.2. Security of processing

The level of security shall reflect the scope of the data processing and the fact that Telenor EMM is designed for the purpose of processing general (non-sensitive) personal data, as stated in Appendix A.

The Data Processor is entitled and obligated to decide which technical and organizational measures must be implemented to obtain the necessary level of security.

However, the Data Processor must – in all circumstances and as a minimum - implement the following measures, as agreed with the Data Controller:

The Data Processor must maintain access restrictions, meaning that the number of the Data Processor's employees with access to the personal data must be limited to what is necessary.

The Data Processor must ensure adequate physical security at all offices from which it performs its tasks.

Access to the Data Controller's Telenor EMM is role-based and requires two-factor authentication.

C.3. Assistance to the data controller

The Data Processor shall insofar as this is possible – within the scope and the extent of the assistance specified below – assist the Data Controller by implementing the following technical and organisational measures:

The Data Processor shall, as far as possible and to a reasonable extent, assist the Data Controller with available information for the purpose of the Data Controller's compliance with the rights of the data subjects.

Should the Data Processor be met with inquiries or requests from the data subjects, the Data Processor will forward these to the Data Controller.

The Data Processor assists, without undue delay, the Data Controller with information relevant to the Data Controller's reporting of personal data breaches in cases where the breach has occurred in relation to the Data Controller's EMM-solution.

C.4. Storage period/erasure procedures

The personal data is stored during the contract period and deleted 30 days after termination of the Data Controller's EMM platform.

Routine operations: If an employee is no longer working for the Data Controller, personal data related to the former employee is deleted immediately after the employee has left the Data Controller. The Data Controller is responsible for the ongoing deletion of personal data related to employees who have left.

C.5. Processing location

Processing of the personal data under these Product-specific Data Processing Terms cannot be performed at other locations than the following without the Data Controller's prior written authorisation:

NAME	LOCATION FOR PROCESSING	TRANSFER BASIS
THE DATA PROCESSOR		
Telenor A/S (company reg. no. 19433692)	Denmark	N/A
SUB-PROCESSOR OF THE DATA PROCESSOR		
Seven Principles Solutions & Consulting GmbH	Germany	N/A
SUB-PROCESSOR'S SUB-PROCESSORS		
7P Austria GmbH	Austria	N/A
7P Nordics AS	Estonia	N/A
Exoscale	Germany	N/A

C.6. Instruction on the transfer of personal data to third countries

If the Data Processor uses sub-processors in accordance with Appendix B and the use of these sub-processors requires transfer to third countries, the Data Processor must ensure a basis for transfer pursuant to Chapter 5 of the GDPR.

When the transfer of personal data takes place to countries where the European Commission has determined that the country provides an adequate level of protection ("secure third countries"), the legal basis for the transfer is Article 45 of the GDPR.

C.7. Procedures for the Data Controller's audits, including inspections, of the processing of personal data being performed by the Data Processor

The Data Controller may, once a year, conduct a written audit to ensure that the processing of personal data is carried out in accordance with the applicable data processing terms, GDPR and the Danish Data Protection Act.

C.8. Procedures for audits, including inspections, of the processing of personal data being performed by sub-processors

The Data Processor shall conduct audits of the sub-processor's processing of personal data and notify the Data Controller if the outcome of such audits gives rise to such notification. The audits may be written audits.

Appendix D Information regarding data storage on the EMM Server

User Information

- Name
- Email
- User ID
- Phone number
- Any AD attributes, if the Data Controller uses LDAP mapping. The Data Controller determines which fields to import if LDAP sync is used.

Device Information – iOS/iPadOS Devices

- OS platform
- OS version
- Firmware ID
- Apple Product ID for the model
- Model type (e.g., iPhone 11, iPhone 12)
- DEP status
- IMEI number
- Serial number
- MAC addresses
- Whether an iTunes account is activated on the device (i.e., whether an Apple ID is used – Yes/No; the specific Apple ID is not visible)
- Language selection
- Time zone setting
- Device name defined by the user under Settings → General → About
- Memory usage in percentage, available GB, and total GB
- If a SIM card is inserted: ICCID, operator name, MNC and MCC codes
- Phone number of the SIM card (if supported by the operator)
- Mobile network connected via SIM card
- Roaming status (Yes/No)
- Battery status
- Find My iPhone activation status (Yes/No)
- ActiveSync ID (if email is configured via the native Apple Mail app)
- Whether the user has a passcode on the device (Yes/No)
- Supervised status (Yes/No)
- Lost Mode activation status (Yes/No)
- OS validity and encryption status
- Do Not Disturb status (Yes/No)
- SIM card change history
- Compliance with passcode policy (Yes/No)
- Installed apps
    - *Differentiation between "Managed" apps installed by EMM and "Unmanaged" apps installed by the user. Privacy modes can*

be activated by Telenor to hide user-installed apps. EMM can detect this, and data is stored in the cloud, but EMM admins cannot view it.

- Configurations, certificates, or setups deployed from the EMM server
- IP address from which port 443 EMM traffic originates
- If Supervised mode is enabled, Lost Mode can enforce GPS location even if Find My iPhone/iPad is not activated

Following data is not processed

- Messages (except those sent by EMM)
- Emails, SMS, MMS
- Photos
- Call history
- Device usage duration
- App usage (time and frequency)
- Data inside apps
- Private Apple ID information
- Browser history
- Notes

Device Information – Android Devices

- OS platform
- Management mode (device, managed device, work profile, work profile on company-owned device)
- OS version
- Firmware ID
- Product model ID
- AE (Managed Google Play) account status and ID
- IMEI number (up to OS12; afterward, a random Android ID is used)
- Serial number
- Push status
- Managed Google Play auto-update policy/status
- MAC addresses (if OS version allows reading)
- Language selection
- Time zone setting
- Device name defined by the user under Settings → General → About
- Memory usage: RAM, flash memory, and SD card (if inserted)
- If SIM card is inserted: IMSI, ICCID, operator name, MNC and MCC codes
- Phone number of the SIM card (if supported by operator and device)
- Mobile network connected via SIM card
- Roaming status (Yes/No)
- Mobile hotspot activation status (Yes/No)
- Battery status

- Lock screen timeout (if supported)
- ActiveSync ID (if email is configured via native email app, primarily Samsung)
- GPS status and permission
- Kiosk mode activation status (Yes/No)
- Passcode status (Yes/No), and if a profile is linked
- OS validity and encryption status
- SIM card change history
- Compliance with passcode policy (Yes/No)
- Installed apps:
    - *Differentiation between "Managed" apps installed by EMM and "Unmanaged" apps installed by the user. Privacy modes can be activated by Telenor to hide user-installed apps. EMM can detect this, and data is stored in the cloud, but EMM admins cannot view it.*
- Configurations, certificates, or setups deployed from the EMM server
- IP address from which port 443 EMM traffic originates

Following data is not processed

- Messages (except those sent by EMM)
- Emails, SMS, MMS
- Photos
- Call history
- Device usage duration
- App usage (time and frequency)
- Data inside apps
- Private Google account information
- Browser history
- Notes