TELENOR'S PRODUCT-SPECIFIC DATA PROCESSING TERMS FOR TELENOR UNIFIED ENDPOINT MANAGEMENT (UEM)

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 Unified Endpoint Management (UEM)**") in accordance with the agreement between the Data Controller and the Data Processor ("**Agreement for Telenor Unified Endpoint Management (UEM)**[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 UEM.

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 UEM and the related services to the Data Controller, as per the Agreement for Telenor Unified Endpoint Management (UEM).

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 UEM 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 configuration of Telenor UEM for the Data Controller, as well as the possibility to provide service and support to the Data Controller in connection with the use of the solution.

Telenor UEM provides access to a platform where the Data Controller can manage and protect 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 service 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 UEM.

When creating the Data Controller's users in Telenor UEM, 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 ongoing use of the solution, the following personal data are processed:

- Name
- Email
- MSISDN
- Serial number
- IMEI number
- MAC address
- IP address
- IMSI number
- Authentication details (the type of authentication used)
- Geolocation, if enabled by the Data Controller
- Calendar information, if enabled by the Data Controller
- Apps downloaded by the employee will appear in the log. The Data Processor and sub-processors can see which apps have been downloaded but cannot view the content of the apps.

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

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

The Data Controller is responsible for ensuring that the solution is not used for processing special categories of personal data, other types of personal data subject to special protection, or any other kinds of personal data for which the solution is not intended.

A.4. Processing includes the following categories of data subjects

The data subjects are the Data Controller's users of the solution. These will often be employees of the Data Controller, but the Data Controller independently decides who is created as users and may also include the Data Controller's external partners.

The Data Controller is responsible for assigning the correct role to the data subjects within the solution, as the assigned role may affect the individual's use of the solution.

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 Unified Endpoint Management (UEM) is terminated or cancelled by either party. Following the termination or expiration of the Agreement for Telenor Unified Endpoint Management (UEM), the personal data will be retained in the solution's backup until the backup expires, which is 30 days after termination or expiration of the agreement.

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			
IBM Danmark ApS (company reg. no. 65305216)	Kongevejen 495B, 2840 Holte, Denmark	Delivering the solution.	The information listed in section A.3 above.
SUB-PROCESSOR'S SUB-PROCESSORS (IBM AFFILIATES)			
IBM Deutschland GmbH	Beim Strohhause 17, 20097, Hamburg, Germany	The solution is hosted and monitored by the sub-processor, who also maintains a backup of the solution. Data remains with the sub-processor – including during support.	The information listed in section A.3 above.
IBM Nederland B.V.	Johan Huizingalaan 765, 1066 VH, Amsterdam, The Netherlands	Backup of the solution.	The information listed in section A.3 above.
BM Canada Limited	3600 Steeles Ave E, Markham, ON L3R 9Z7, Canada	Development: Error reporting and improvement suggestions.	Development: The sub-processor generally does not have access to the solution, but error reports and/or suggestions for improvements may contain contact

			information about the person(s) involved in the matter.
IBM Business Transformation Center s.r.l.	Norte de Mall Real Cariari Calle La Rusia Heredia, Heredia, 40103, Costa Rica	Customer support: The sub-processor can assist with 3rd level support. Operations: Ensuring the operation of the solution.	Customer Support: The sub-processor generally does not have access to the solution and does not process personal data on a regular basis, but in cases of 3rd level support and error handling, access to personal data may be granted by the Data Controller, thereby allowing the sub-processor to process data related to the error. The data is not transferred to the sub-processor but may be accessed by the sub-processor. This may include all information mentioned in section A.3 above, but only the data relevant to the specific support case will be accessed. Operations: During operations, there is generally no access to the solution, but service requests may contain contact information

			of the person making the request.
Compagnie IBM France, S.A.S	17, avenue de l'Europe, 92275 Bois-Colombes Cedex, France	Operations: Ensuring the operation of the solution.	Operations: During operations, there is generally no access to the solution, but service requests may contain contact information of the person making the request.
IBM India Private Limited	Subramanya Arcade-2, 12, Bannerghatta Main Road, Bangalore, 560029, India	Customer support: The sub-processor can assist with 3rd level support. Development: Error reporting and improvement suggestions. Operations: Ensuring the operation of the solution.	Customer Support: The sub-processor generally does not have access to the solution and does not process personal data on a regular basis, but in cases of 3rd level support and error handling, access to personal data may be granted by the Data Controller, allowing the sub-processor to process data related to the error. The data is not transferred to the sub-processor but may be accessed by the sub-processor. This may include all information mentioned in section A.3 above, but only the data relevant to the specific support

			case will be accessed. Development: The sub-processor generally does not have access to the solution, but error reports and/or suggestions for improvements may contain contact information of the person(s) involved in the matter. Operations: During operations, there is generally no access to the solution, but service requests may contain contact information of the person making the request
IBM Ireland Limited	Charlemont Exchange, WeWork Office Space, Temple Bar, Dublin, Ireland	Customer support: The sub-processor can assist with 3rd level support.	Customer Support: The sub-processor generally does not have access to the solution and does not process personal data on a regular basis, but in cases of 3rd level support and error handling, access to personal data may be granted by the Data Controller, thereby allowing the sub-processor to process data related to the error. The data is not transferred to

			the sub-processor but may be accessed by the sub-processor. This may include all information mentioned in section A.3 above, but only the data relevant to the specific support case will be accessed.
International Business Machines Corporation	1 New Orchard Road Armonk, New York 10504-1722, USA	Customer support: The sub-processor can assist with 3rd level support. Operations: Ensuring the operation of the solution.	Customer Support: The sub-processor generally does not have access to the solution and does not process personal data on a regular basis, but in cases of 3rd level support and error handling, access to personal data may be granted by the Data Controller, thereby allowing the sub-processor to process data related to the error. The data is not transferred to the sub-processor but may be accessed by the sub-processor. This may include all information mentioned in section A.3 above, but only the data relevant to the specific support

			case will be accessed. Operations: During operations, there is generally no access to the solution, but service requests may contain contact information of the person making the request.
SUB-PROCESSOR'S SUB-PROCESSORS			
Akamai Technologies, Inc.	45 Broadway, Cambridge, MA 02142, USA	Content distribution, caching, security, performance, and other gateway services	The information listed in section A.3 above.
Amazon Web Services, Inc.	2021 7th Ave, Seattle, WA 98121, USA	Hosting, storage, backup and other computing resources Content distribution, caching, security, performance, and other gateway services	The information listed in section A.3 above.
Equinix	Redwood City, California, USA	Hosting, storage, backup, and other computing resources Content distribution, caching, security, performance, and other gateway services	The information listed in section A.3 above.

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 instructions are defined in these Product-specific Data Processor Terms, the Agreement for Telenor Unified Endpoint Management (UEM), and the Data Controller's and its users' use and configuration of the solution.

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

The Data Processor is instructed to implement Telenor UEM on devices belonging to the Data Controller.

The Data Processor configures Telenor UEM on the Data Controller's mobile devices according to the Data Controller's specifications. When setting up the solution, the Data Processor has access to personal data including names, email addresses, and any attributes from the Data Controller's Active Directory (AD) of the relevant employees.

Once the solution is configured, the Data Processor has access to the Data Controller's solution for the purpose of handling 2nd line support.

The Data Controller is responsible for the legality of the processing and ensuring that the solution is not used in a manner that violates the GDPR or any other legislation.

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 UEM. Other processing of the Customer's telecommunications data processed as part of Telenor's transmission of communications 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 processing and the fact that Telenor UEM is designed for the processing of general (non-sensitive) personal data, as specified 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 ensure adequate physical security at all offices from which the Data Processor performs its tasks.

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 sub-processor has implemented additional security measures that reflect the sub-processor's data processing.

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 UEM-solution.

The Data Controller must submit a written request for any assistance related to these Product-specific Data Processor Terms.

C.4. Storage period/erasure procedures

The Data Controller can delete personal data in the solution on an ongoing basis and before the termination of the agreement. A user is deleted from the solution when the user is removed from the Data Controller's Active Directory (AD).

Personal data is removed upon termination of the agreement and deleted

no later than 30 days thereafter from the solution's backup. When the solution is closed, neither the Data Controller nor the Data Processor will have access to personal data anymore.

The Data Controller can make a copy of the data in the solution at any time before the termination of the agreement through the solution's self-service options.

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		
IBM Danmark ApS (company reg. no. 65305216)	Denmark	N/A
SUB-PROCESSOR'S SUB-PROCESSORS (IBM AFILIATES)		
IBM Deutschland GmbH	Germany	N/A
IBM Nederland B.V.	The Netherlands	N/A
IBM Canada Limited	Canada	EU SCC
IBM Business Transformation Center s.r.l.	Costa Rica	EU SCC
Compagnie IBM France, S.A.S	France	N/A
IBM India Private Limited	India	EU SCC
IBM Ireland Limited	Ireland	N/A
International Business Machines Corporation	USA	EU SCC

SUB-PROCESSOR'S SUB-PROCESSORS		
Akamai Technologies, Inc.	USA	EU SCC
Amazon Web Services, Inc.	USA	EU SCC
Equinix	USA	EU SCC

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.

The Data Processor may, by using the sub-processor (IBM) and its sub-processors, transfer personal data to countries outside the EU/EEA.

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 audit gives rise to such notification.

The Data Processor may request the sub-processor's latest certifications and/or a summary of audit reports in order to test, assess, and evaluate the effectiveness of the agreed technical and organizational measures. Furthermore, the sub-processor will, within reasonable limits, assist with available information about the agreed technical and organizational measures.

Appendix D Regulation of other matters between the Parties

Limitation of Liability

The Parties agree that the liability terms set out in the Agreement for Telenor Unified Endpoint Management (UEM) shall also apply to these Product-specific Data Processing Terms.

Assistance

The Data Controller must submit a written request for any assistance described in Telenor's General Data Processing Terms and these Product-specific Data Processing Terms. The Data Processor may charge a reasonable fee for providing such assistance in accordance with the Data Processor's current rates.

Contact

The Data Processor acts as the contact point for the sub-processor.

Likewise, the sub-processor acts as the contact point for the Data Processor.

Appendix E Information on data storage on the UEM Server

User Information

- Full 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 UEM and "Unmanaged" apps installed by the user. Privacy modes can be activated by Telenor to hide user-installed apps. UEM can*

detect this, and data is stored in the cloud, but UEM admins cannot view it.

- Configurations, certificates, or setups deployed from the UEM 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 <u>not</u> processed

- Messages (except those sent by UEM)
- 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 UEM and "Unmanaged" apps installed by the user. Privacy modes can be activated by Telenor to hide user-installed apps. UEM can detect this, and data is stored in the cloud, but UEM admins cannot view it.*
- Configurations, certificates, or setups deployed from the UEM server
- IP address from which port 443 EMM traffic originates

Following information is <u>not</u> processed

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