TELENOR'S PRODUCT-SPECIFIC DATA PROCESSING TERMS FOR MOBILE THREAT DEFENCE

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 ("**Mobile Threat Defence**") in accordance with the agreement between the Data Controller and the Data Processor ("**Agreement for Mobil Threat Defence**[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 Mobile Threat Defence.

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 Processor handles configuration, administration and provides support to Mobile Threat Defence and licenses to the solution to the Data Controller, as per the Agreement for Mobile Threat Defence.

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 assist the Data Controller with the configuration of the Data Controller's Mobile Threat Defence and, if necessary, to manage 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 consists of configuration, administration and support of the solution, Check Point Harmony Mobile.

Check Point Harmony Mobile is a security product that scans the Data Controller's mobile devices and reports any vulnerabilities found on the device. The delivery and use of the solution is governed by the data processing agreement that the Data Controller enters into directly with Check Point.

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 configuration, administration and support of the solution.

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

- The users name
- Email address (for work)
- Telephone number (for work)

During the ongoing administration and support, the following personal data is processed:

- Username
- Device data
- Operating system, version
- Security status
- Network connections and configurations
- During alerts: Apps, files and messages – *the Data Processor cannot see the content of the apps, files or messages*

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).

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

Users of the Data Controller's mobile devices.

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 Mobile Threat Defence is terminated or cancelled by either party.

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			
Check Point Software Technologies Ltd.	Shlomo Kaplan, Tel-Aviv, Israel	Support	The personal data listed under section A.3 as well as any additional information provided by the Data Controller in a support ticket
SUB-PROCESSOR'S SUB-PROCESSORS			
Check Point affiliates	Global	Support	The personal data listed under section A.3 as well as any additional information provided by the Data Controller in a support ticket
Amazon Web Services, Inc. (AWS)	EU	Support	The personal data listed under section A.3 as well as any additional information provided by the Data Controller in a support ticket
IBM Aspera	EU	Support	The personal data listed under section A.3 as well as any additional information provided by the Data Controller in a

			support ticket
Salesforce	EU	Support and CRM	The personal data listed under section A.3 as well as any additional information provided by the Data Controller in a support ticket

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 5 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:

Configuration of users, administration and support of the Data Controller's Mobile Threat Defence solution.

C.2. Security of processing

The level of security shall reflect the scope of the processing and the fact that the solution 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 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 the Data Processor performs its tasks.

Access to the solution 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 Mobile Threat Defence.

C.4. Storage period/erasure procedures

Personal data is stored in the solution and will be deleted after the termination of the Data Controller's Mobile Threat Defence.

Daily operations: When the Data Controller changes users, the personal data related to the former user is deleted immediately after the user's device is removed from the solution.

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		
Check Point Software Technologies Ltd.	Israel	GDPR Article 45 (Adequacy decision)
SUB-PROCESSOR'S SUB-PROCESSORS (IBM AFILIATES)		
Check Point affiliates	Global	EU Commission's Standard Contractual Clauses
Amazon Web Services, Inc. (AWS)	EU	N/A
IBM Aspera	EU	N/A
Salesforce	EU	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 audit gives rise to such notification. The audits may be written audits.