

TELENORS PRODUKTSPECIFIKKE DATABEHANDLERVILKÅR FOR MOBILE THREAT DEFENCE

1. Indledning

- 1.1 Disse produktspecifikke databehandlervilkår ("**Produktspecifikke Databehandlervilkår**") finder anvendelse på den behandling af personoplysninger som Telenor A/S (cvr. 19433692, Frederikskaj 8, 2450 København SV) ("**Databehandler**") foretager på vegne af Kunden ("**Dataansvarlig**") med henblik på at levere produktet ("**Mobile Threat Defence**") i henhold til den, mellem Databehandleren og den Dataansvarlige, indgåede aftale vedrørende levering af Mobile Threat Defence ("**Aftale for Mobile Threat Defence**¹").
- 1.2 Disse Produktspecifikke Databehandlervilkår er fastsat i henhold til databeskyttelsesforordningens artikel 28, stk. 3 ("**GDPR**") og fastsætter, sammenholdt med de generelle databehandlervilkår, den Dataansvarlige og Databehandlerens rettigheder og forpligtelser, når der foretages behandling af personoplysninger på vegne af den Dataansvarlige i forbindelse med leveringen af Mobile Threat Defence.
- 1.3 Disse Produktspecifikke databehandlervilkår er en integreret del af Telenors Generelle Databehandlervilkår og finder anvendelse på tidspunktet for de generelle databehandlervilkårs ikrafttræden.

¹ Aftalen kan blandt andet være udfærdiget som en produktaftale, en SKI-aftale, vilkår eller anden aftaletype. Det afhænger af den specifikke aftaletype, der er indgået mellem Telenor og Kunden.

Bilag A Oplysninger om behandlingen

Databehandleren leverer konfiguration, administration og support til Mobile Threat Defence og licenser til løsningen til den Dataansvarlige, jf. Aftalen for Mobile Threat Defence.

A.1. Formålet med databehandlerens behandling af personoplysninger på vegne af den dataansvarlige

Formålene med Databehandlerens behandling af personoplysninger på vegne af den Dataansvarlige er at kunne assistere den Dataansvarlige med opsætning af den Dataansvarliges Mobile Threat Defence løsning og eventuelt administrere og supportere den Dataansvarliges brug af løsningen.

A.2. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige drejer sig primært om (karakteren af behandlingen)

Karakteren af behandlingen af personoplysninger, som Databehandleren foretager på vegne af den Dataansvarlige består i opsætning, administration og support af løsningen, Check Point Harmony Mobile.

Check Point Harmony Mobile er et sikkerhedsprodukt, der scanner den Dataansvarliges mobile enheder og rapporterer om eventuelle sårbarheder fundet på enheden. Selve levering og brug af løsningen er reguleret af den databehandleraftale, som den Dataansvarlige indgår direkte med Check Point, som beskrevet ovenfor.

A.3. Behandlingen omfatter følgende typer af personoplysninger om de registrerede

Løsningen er udviklet til at omfatte behandling af almindelige personoplysninger omfattet af GDPR artikel 6. Følgende typer af almindelige personoplysninger behandles i forbindelse med Databehandlerens levering af opsætning, administration og support af løsningen.

Ved oprettelse af den Dataansvarliges brugere i løsningen benyttes nedenstående personoplysninger:

- Brugerens navn
- Arbejds-mail
- Arbejds-telefonnummer

I forbindelse med løbende administration og support behandles følgende personoplysninger:

- Brugernavn

- Enhedsdata
- Operativsystem, version
- Sikkerhedsstatus
- Netværksforbindelser og konfigurationer
- Ved alerts: Apps, filer og beskeder – *Databehandleren kan ikke se indholdet i apps, filer og beskeder*

Løsningen er ikke udviklet med henblik på at behandle særlige kategorier af personoplysninger efter GDPR artikel 9 (følsomme personoplysninger).

A.4. Behandlingen omfatter følgende kategorier af registrerede

Brugere af den Dataansvarliges mobile enheder.

A.5. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige kan påbegyndes efter disse databehandlervilkårs ikrafttræden. Behandlingen har følgende varighed

Varigheden af behandlingen af personoplysninger svarer til varigheden af leveringen af ydelsen. Behandlingen er således ikke tidsbegrænset, men varer indtil Aftalen for Mobile Threat Defence opsiges eller ophæves af en af parterne.

Bilag B Underdatabehandlere

B.1. Godkendte underdatabehandlere

Ved disse Produktspecifikke Databehandlervilkårs ikrafttræden har den Dataansvarlige godkendt brugen af følgende underdatabehandlere for den beskrevne behandlingsaktivitet:

NAVN	ADRESSE	BESKRIVELSE AF BEHANDLING	PERSONOPLYSNINGER, DER BEHANDLES
DATABASEHANDLERENS UNDERDATABEHANDLER			
Check Point Software Technologies Ltd.	Shlomo Kaplan, Tel-Aviv, Israel	Support	De personoplysninger der er nævnt under pkt. A.3. samt eventuelt øvrige oplysninger, som den Dataansvarlige oplysninger i support-ticket.
UNDERDATABEHANDLERENS UNDERDATABEHANDLERE			
Check Point affiliates	Global	Support	De personoplysninger der er nævnt under pkt. A.3. samt eventuelt øvrige oplysninger, som den Dataansvarlige oplysninger i support-ticket.
Amazon Web Services, Inc. (AWS)	EU	Support	De personoplysninger der er nævnt under pkt. A.3. samt eventuelt øvrige oplysninger, som den Dataansvarlige oplysninger i support-ticket.
IBM Aspera	EU	Support	De personoplysninger der er nævnt under pkt. A.3. samt eventuelt øvrige oplysninger, som den Dataansvarlige oplysninger i support-ticket.
SalesForce	EU	Support og CRM	De personoplysninger der er nævnt under pkt. A.3. samt eventuelt øvrige oplysninger, som den Dataansvarlige oplysninger i support-ticket.

Databehandleren må ikke – uden den Dataansvarliges skriftlige godkendelse – gøre brug af en underdatabehandler til en anden behandlingsaktivitet end den beskrevne og aftalte eller gøre brug af en anden underdatabehandler til denne behandlingsaktivitet.

B.2. Varsel for indsigelse mod underdatabehandlere

Den Dataansvarlige skal inden 5 dage fra datoen for Databehandlerens underretning om eventuelle planlagte ændringer vedrørende tilføjelse eller udskiftning af underdatabehandlere skriftligt til Databehandleren gøre indsigelse mod den eller de pågældende underdatabehandlere.

Hvis den Dataansvarlige gør indsigelse, skal indsigelsen indeholde den Dataansvarliges specifikke grunde til indsigelsen.

Bilag C Instruks vedrørende behandling af personoplysninger

C.1. Behandlingens genstand/instruks

Databehandlerens behandling af personoplysninger på vegne af den Dataansvarlige sker ved, at Databehandleren udfører følgende:

Opsætning af brugere, administration og support af den Dataansvarliges Mobile Threat Defence løsning.

C.2. Behandlingssikkerhed

Der skal etableres et sikkerhedsniveau, der afspejler behandlingens omfang og at løsningen er udviklet med henblik på behandling af almindelige og ikke-følsomme personoplysninger, som angivet i Bilag A.

Databehandleren er herefter berettiget og forpligtet til at træffe beslutninger om, hvilke tekniske og organisatoriske sikkerhedsforanstaltninger, der skal gennemføres for at etablere det nødvendige sikkerhedsniveau.

Databehandleren skal dog – under alle omstændigheder og som minimum – gennemføre følgende foranstaltninger, som er aftalt med den dataansvarlige:

Databehandleren skal opretholde adgangsbegrænsning, hvilket indebærer, at antallet af medarbejdere hos Databehandleren, der har adgang til den Dataansvarliges personoplysninger skal begrænses til det nødvendige.

Databehandleren skal sikre en forsvarlig, fysisk sikkerhed på alle kontorer, hvorfra Databehandleren udfører sine opgaver.

Adgang til løsningen er rollebaseret og kræver to-faktor autentifikation.

C.3 Bistand til den dataansvarlige

Databehandleren skal så vidt muligt – inden for det nedenstående omfang og udstrækning – bistå den Dataansvarlige ved at gennemføre følgende foranstaltninger:

Databehandleren bistår, så vidt muligt og inden for rimeligt omfang, den Dataansvarlige med tilgængelig information til brug for den Dataansvarliges overholdelse af de registreredes rettigheder.

Skulle Databehandleren blive mødt med henvendelser eller anmodninger fra de registrerede, vil Databehandleren videreformidle disse henvendelser og anmodninger til den Dataansvarlige.

Databehandleren bistår, uden unødigt forsinkelse, den Dataansvarlige med oplysninger relevante for den Dataansvarliges indberetning af brud på persondatasikkerheden i tilfælde, hvor bruddet er sket i relation til den Dataansvarliges Mobile Threat Defence løsning.

C.4 Opbevaringsperiode/sletterutine

Personoplysninger opbevares i løsningen og slettes efter terminering af den Dataansvarliges Mobile Threat Defence løsning.

Almindelig drift: Ved skift af brugere hos den Dataansvarlige, slettes personoplysninger vedrørende den tidligere brugere straks efter brugerens enhed fjernes fra løsningen.

C.5 Lokalitet for behandling

Behandling af de omfattede personoplysninger kan ikke uden den Dataansvarliges forudgående skriftlige godkendelse ske på andre lokaliteter end følgende:

NAVN	LOKALITET FOR BEHANDLING	OVERFØRSELS-GRUNDLAG
DATABEHANDLEREN		
Telenor A/S (cvr. 19433692)	Danmark	N/A
DATABEHANDLERENS UNDERDATABEHANDLER		
Check Point Software Technologies Ltd.	Israel	Tilstrækkeligheds-afgørelse
UNDERDATABEHANDLERENS UNDERDATABEHANDLERE		
Check Point affiliates	Global	EU-Kommissionens standardkontraktbestemmelser
Amazon Web Services, Inc. (AWS)	EU	N/A
IBM Aspera	EU	N/A
SalesForce	EU	N/A

C.6 Instruks vedrørende overførsel af personoplysninger til tredje-lande

Hvis Databehandleren benytter underdatabehandlere i overensstemmelse med Bilag B og brugen af disse underdatabehandlere kræver overførsel til tredjelande, skal Databehandleren sikre, at der findes et overførselsgrundlag efter Kapitel 5 i GDPR.

Når overførsel af personoplysninger finder sted til lande, hvor Europa-Kommissionen har fastslået, at landet har et tilstrækkeligt beskyttelsesniveau ("sikre tredjelande"), er overførselsgrundlaget artikel 45 i GDPR.

C.7 Procedurer for den dataansvarliges revisioner med behandlingen af personoplysninger, som er overladt til databehandleren

Den Dataansvarlige kan, en gang om året, foretage et skriftligt tilsyn med Databehandleren for at sikre, at behandlingen af personoplysninger sker i overensstemmelse med de gældende databehandlervilkår, GDPR og databeskyttelsesloven.

C.8 Procedurer for revisioner, herunder inspektioner, med behandling af personoplysninger, som er overladt til underdatabehandlere

Databehandleren fører tilsyn med underdatabehandleren og underretter den Dataansvarlige, såfremt et gennemført tilsyn giver anledning hertil. Databehandleren foretager skriftligt tilsyn med underdatabehandleren.