

TELENORS PRODUKTSPECIFIKKE DATABEHANDLERVILKÅR FOR TELENOR UNIFIED ENDPOINT MANAGEMENT (UEM)

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 ("**Telenor Unified Endpoint Management (UEM)**") i henhold til den, mellem Databehandleren og den Dataansvarlige, indgåede aftale vedrørende levering af Telenor Unified Endpoint Management (UEM) ("**Aftale for Telenor Unified Endpoint Management (UEM)**"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 Telenor UEM.
- 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 Telenor UEM og den tilhørende løsning til den Dataansvarlige, jf. Aftalen for Telenor Unified Endpoint Management (UEM).

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 implementere og oprette den Dataansvarliges Telenor UEM samt 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 primært i opsætning af Telenor UEM for den Dataansvarlige samt mulighed for efterfølgende at kunne servicere og supportere den Dataansvarlige i forbindelse med brugen af løsningen.

Telenor UEM giver adgang til en platform, hvor den Dataansvarlige kan administrere og beskytte enheder.

Managed Service – OneSupport Admin, OneSupport Admin 24/7 og OneSupport All, Device Management

Hvis den Dataansvarlige tilvælger Service by Telenor, som udgør en separat serviceaftale med Databehandleren, kan karakteren af behandlingen ligeledes bestå af administration, opsætning og efterfølgende service.

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 Telenor UEM.

Ved oprettelse af den Dataansvarliges brugere i Telenor UEM benyttes nedenstående personoplysninger:

- Fulde navn
- E-mail
- Bruger ID

- Telefonnummer
- Eventuelt attributter, hvis den Dataansvarlige anvender en bruger-database

Ved den Dataansvarliges løbende brug af løsningen behandles følgende personoplysninger:

- Navn
- E-mail
- MSISDN
- Serienummer
- IMEI-nummer
- MAC adresse
- IP Adresse
- IMSI-nummer
- Autentifikationsoplysninger (hvilke type autentifikation der benyttes)
- Geolokation, hvis dette er aktiveret af den Dataansvarlige
- Kalenderoplysninger, hvis den Dataansvarlige aktiverer dette
- Apps, som medarbejderen har downloadet, vil fremgå af loggen. Databehandleren og underdatabehandlerne kan se apps, men ikke indholdet af downloadede apps

Et udtømmende overblik over behandling og lagring af oplysninger fremgår af Bilag E.

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

Den Dataansvarlige er ansvarlig for, at løsningen ikke benyttes til behandling af særlige kategorier af personoplysninger, andre personoplysninger underlagt særlig beskyttelse eller øvrige former for personoplysninger, som løsningen ikke er beregnet til.

A.4. Behandlingen omfatter følgende kategorier af registrerede

Der behandles personoplysninger om den Dataansvarliges brugere af løsningen. Dette vil ofte være medarbejdere hos den Dataansvarlige, men den Dataansvarlige administrerer selv, hvem der skal være en del af løsningen og kan derfor inkludere den Dataansvarliges eksterne partnere.

Den Dataansvarlige er ansvarlig for at tildele de registrerede den korrekte rolle i løsningen, da rollen kan have betydning for den enkeltes brug af løsningen.

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 Telenor Unified Endpoint Management (UEM) opsiges eller ophæves af en af parterne. Personoplysningerne vil efter ophør af Aftale for Telenor Unified Endpoint Management (UEM) blive opbevaret i løsningens backup indtil udløbet af backuppen 30 dage efter opsigelse eller udløb af aftalen.

Den Dataansvarlige er ansvarlig for løbende sletning og oprettelse af nye brugere.

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			
IBM Danmark ApS (cvr. Nr. 65305216)	Kongevejen 495B, 2840 Holte, Danmark	Levering af løsningen.	Oplysningerne oplyst i pkt. A.3 ovenfor.
UNDERDATABEHANDLERENS UNDERDATABEHANDLERE (IBM AFFILIATES)			
IBM Deutschland GmbH	Beim Strohhause 17, 20097, Hamburg, Tyskland	Løsningen hostes og overvåges af underdatabehandleren, der ligeledes har en back-up af løsningen. Data forbliver hos underdatabehandleren – også under support.	Oplysningerne oplyst i pkt. A.3 ovenfor.
IBM Nederland B.V.	Johan Huizingalaan 765, 1066 VH, Amsterdam, Holland	Backup af løsningen.	Oplysningerne oplyst i pkt. A.3 ovenfor.
IBM Canada Limited	3600 Steeles Ave E, Markham, ON L3R 9Z7, Canada	Development: Fejlmeldinger og håndtering af forbedringsforslag.	Development: Underdatabehandleren har som udgangspunkt ikke adgang til løsningen, men

			fejlmeldinger og/eller forslag til forbedringer kan indeholde kontaktoplysninger på den eller de, der har været involveret i sagen.
IBM Business Transformation Center s.r.l.	Norte de Mall Real Cariari Calle La Rusia Heredia, Heredia, 40103, Costa Rica	Customer support: Underdata-behandleren kan bistå med 3rd level support. Operations: Sikring af løsnings drift.	Customer Support: Underdatabehandleren har som udgangspunkt ikke adgang til løsningen og behandler ikke personoplysninger på fast basis, men kan, i tilfælde af support og fejlretning i 3. led få tildelt adgang til personoplysningerne af den Dataansvarlige og dermed behandle oplysninger relateret til fejlen. Oplysningerne overføres ikke til underdatabehandleren, men kan tilgås af underdatabehandleren. Dette kan være alle oplysningerne nævnt i pkt. A.3 ovenfor, men vil kun være de oplysninger der er relevante for den specifikke supportsag. Operations: Ved operations er der som udgangspunkt ikke adgang til løsningen, men service requests kan

			indeholde kontakt-oplysninger på den person, der laver forespørgslen.
Compagnie IBM France, S.A.S	17, avenue de l'Europe, 92275 Bois-Colombes Cedex, Frankrig	Operations: Sikring af løsnings drift.	Operations: Ved operations er der som udgangspunkt ikke adgang til løsningen, men service requests kan indeholde kontaktoplysninger på den person, der laver forespørgslen.
IBM India Private Limited	Subramanya Arcade-2, 12, Bannerghatta Main Road, Bangalore, 560029, Indien	Customer support: Underdatabehandleren kan bistå med 3rd level support. Development: Fejlmeldinger og håndtering af forbedringsforslag. Operations: Sikring af løsnings drift.	Customer Support: Underdatabehandleren har som udgangspunkt ikke adgang til løsningen og behandler ikke personoplysninger på fast basis, men kan, i tilfælde af support og fejlretning i 3. led få tildelt adgang til personoplysningerne af den Dataansvarlige og dermed behandle oplysninger relateret til fejlen. Oplysningerne overføres ikke til underdatabehandleren, men kan tilgås af underdatabehandleren. Dette kan være alle oplysningerne nævnt i pkt. A.3 ovenfor, men vil kun være de oplysninger der er relevante for den

			specifikke supportsag. Development: Underdatabehandleren har som udgangspunkt ikke adgang til løsningen, men fejlmeldinger og/eller forslag til forbedringer kan indeholde kontaktoplysninger på den eller de, der har været involveret i sagen. Operations: Ved operations er der som udgangspunkt ikke adgang til løsningen, men service requests kan indeholde kontaktoplysninger på den person, der laver forespørgslen.
IBM Ireland Limited	Charlemont Exchange, WeWork Office Space, Temple Bar, Dublin, Irland	Customer support: Underdatabehandleren kan bistå med 3rd level support.	Customer Support: Underdatabehandleren har som udgangspunkt ikke adgang til løsningen og behandler ikke personoplysninger på fast basis, men kan, i tilfælde af support og fejlretning i 3. led få tildelt adgang til personoplysningerne af den Dataansvarlige og dermed behandle oplysninger relateret til fejlen. Oplysningerne overføres ikke til

			underdatabehandleren, men kan tilgås af underdatabehandleren. Dette kan være alle oplysningerne nævnt i pkt. A.3 ovenfor, men vil kun være de oplysninger der er relevante for den specifikke supportsag.
International Business Machines Corporation	1 New Orchard Road Armonk, New York 10504-1722, USA	Customer support: Underdatabehandleren kan bistå med 3rd level support. Operations: Sikring af løsnings drift.	Customer Support: Underdatabehandleren har som udgangspunkt ikke adgang til løsningen og behandler ikke personoplysninger på fast basis, men kan, i tilfælde af support og fejlretning i 3. led få tildelt adgang til personoplysningerne af den Dataansvarlige og dermed behandle oplysninger relateret til fejlen. Oplysningerne overføres ikke til underdatabehandleren, men kan tilgås af underdatabehandleren. Dette kan være alle oplysningerne nævnt i pkt. A.3 ovenfor, men vil kun være de oplysninger der er relevante for den specifikke supportsag.

			Operations: Ved operations er der som udgangspunkt ikke adgang til løsningen, men service requests kan indeholde kontaktoplysninger på den person, der laver foresøgslen.
--	--	--	---

UNDERDATABEHANDLERENS UNDERDATABEHANDLERE

Akamai Technologies, Inc.	145 Broadway, Cambridge, MA 02142	Content distribution, caching, security, performance, and other gateway services	Oplysningerne oplyst i pkt. A.3 ovenfor.
Amazon Web Services, Inc.	2021 7th Ave, Seattle, WA 98121	Hosting, storage, backup and other computing resources Content distribution, caching, security, performance, and other gateway services	Oplysningerne oplyst i pkt. A.3 ovenfor.
Equinix	Redwood City, Californien, USA	Hosting, storage, backup, and other computing resources Content distribution, caching, security, performance, and other gateway services	Oplysningerne oplyst i pkt. A.3 ovenfor.

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 10 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:

Instruksen er defineret i disse Produktspecifikke Databehandlervilkår, Aftalen for Telenor Unified Endpoint Management (UEM) og den Dataansvarliges og dennes brugeres brug og konfiguration af løsningen.

Databehandleren distribuerer Telenor UEM, der er udviklet, leveres og driftes af Underdatabehandleren nævnt i pkt. B.1 ovenfor.

Databehandleren instrueres i at oprette og implementere Telenor UEM på enheder hos den Dataansvarlige.

Databehandleren opsætter Telenor UEM på den Dataansvarliges mobile enheder via konfiguration og den Dataansvarliges kravspecifikationer. Når Databehandleren skal opsætte løsningen, får Databehandleren adgang til personoplysninger herunder navn, mailadresse og eventuelle attributter fra den Dataansvarliges Active Directory (AD) på den Dataansvarliges relevante medarbejdere.

Når løsningen er opsat, har Databehandleren adgang til den Dataansvarliges løsning med henblik på håndtering af 2nd line support.

Den Dataansvarlige er ansvarlig for lovligheden af behandlingen og at løsningen ikke bruges på en måde, der overtræder Databeskyttelsesforordningen eller anden lovgivning.

Databehandleren er kun databehandler for behandling af personoplysningerne i forbindelse med levering af Telenor UEM. Øvrig behandling af Kundens teleoplysninger, der behandles som led i Telenors fremføring af kommunikation i netværket, er ikke omfattet af de generelle Databehandlervilkår eller disse Produktspecifikke Databehandlervilkår.

C.2. Behandlingssikkerhed

Der skal etableres et sikkerhedsniveau, der afspejler behandlingens omfang og at Telenor UEM 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 sikre en forsvarlig, fysisk sikkerhed på alle kontorer, hvorfra Databehandleren udfører sine opgaver.

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

Underdatabehandleren har etableret yderligere sikkerhedsforanstaltninger, der afspejler underdatabehandlerens databehandling.

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 UEM-løsning.

Den Dataansvarlige skal fremsætte en skriftlig anmodning om enhver bistand i relation til disse Produktspecifikke Databehandlervilkår.

C.4 Opbevaringsperiode/sletterutine

Den Dataansvarlige kan selv slette personoplysningerne i løsningen løbende og inden aftalens ophør. En bruger slettes fra løsningen, når brugeren fjernes fra den Dataansvarliges AD.

Personoplysningerne fjernes ved aftalens ophør og slettes senest 30 dage herefter i løsningens back-up. Når løsningen lukkes, vil der ikke længere være adgang til personoplysningerne for den Dataansvarlige og Databehandleren.

Den Dataansvarlige kan lave en kopi af sine oplysninger i løsningen til enhver tid inden aftalens ophør gennem løsningens self-service-muligheder.

C.5 Lokaltitet 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
DATABASEHANDLEREN		
Telenor A/S (cvr. 19433692)	Danmark	N/A
DATABASEHANDLERENS UNDERDATABASEHANDLER		
IBM Danmark ApS (cvr. 65305216)	Danmark	N/A
UNDERDATABASEHANDLERENS UNDERDATABASEHANDLERE (IBM AFFILIATES)		
IBM Deutschland GmbH	Tyskland	N/A
IBM Nederland B.V.	Holland	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	Frankrig	N/A
IBM India Private Limited	Indien	EU SCC
IBM Ireland Limited	Irland	N/A
International Business Machines Corporation	United States	EU SCC
UNDERDATABASEHANDLERENS UNDERDATABASEHANDLERE		
Akamai Technologies, Inc.	United States	EU SCC

NAVN	LOKALITET FOR BEHAND- LING	OVERFØRSELS- GRUNDLAG
DATABASEHANDLEREN		
Amazon Web Services, Inc.	United States	EU SCC
Equinix	United States	EU SCC

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.

Databehandleren kan via brugen af Underdatabehandleren (IBM) samt dennes underdatabehandlere overføre personoplysninger til lande uden for EU/EØS i forbindelse med levering af Telenor UEM.

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 kan anmode om Underdatabehandlerens seneste certificering og/eller en opsummering af revisionserklæring(er) for at teste, vurdere og evaluere effektiviteten af de aftalte tekniske og organisatoriske foranstaltninger. Underdatabehandleren vil derudover, med rimelighed, bistå med tilgængelig information om de aftalte tekniske og organisatoriske foranstaltninger.

Bilag D Parternes regulering af andre forhold

Ansvarsbegrænsning

Parterne er enige om, at de vilkår for ansvar, som er fastsat i Aftale for Telenor Unified Endpoint Management (UEM) også finder anvendelse på disse Produktspecifikke Databehandlervilkår.

Bistand

Den Dataansvarlige skal lave en skriftlig anmodning om enhver bistand beskrevet i Telenors Generelle Databehandlervilkår og disse Produktspecifikke Databehandlervilkår. Databehandleren kan opkræve et rimeligt vederlag for at yde sådan en bistand i overensstemmelse med Databehandlernes gældende satser.

Kontakt

Databehandleren fungerer som kontaktpunkt for Underdatabehandleren.

Tilsvarende vil Underdatabehandleren fungerer som kontaktpunkt for Databehandleren.

Bilag E Information om lagring af oplysninger på UEM server

Brugeroplysninger

- Fulde navn
- E-mail
- Bruger ID
- Telefonnummer
- Evt. AD attributter, hvis den Dataansvarlige anvender Ldap mapping, men den Dataansvarlige bestemmer selv hvilke felter der ønskes importeret data fra, hvis ldap sync anvendes

Enhedsoplysninger, når der er tale om iOS/iPad OS enheder

- OS platform
- OS version
- Firmware ID
- Apple Product ID for modellen
- Model type (iPhone 11, iPhone 12 osv.)
- DEP-status
- IMEI-nummer
- Serie nummer
- MAC adresser
- Er der iTunes konto aktiveret på enheden (dvs. om der anvendes en Apple id på enheden Ja/Nej, vi kan ikke se hvilket Apple id)
- Sprogvalg
- Tidszone indstilling
- Enhedens navn som bruger måtte have døbt denne i Indstillinger - > Generelt -> Om
- Hukommelses forbrug i procent og disponibel i Gb og total i Gb
- Hvis simkort er isat, så aflæses ICCID på simkort og hvilken operatør dette er fra såvel operatørens MNC og MCC-kode
- Telefonnummer på det simkort der sidder i enheden (hvis operatøren understøtter dette)
- Hvilket mobilnetværk enheden via simkort er forbundet til
- Om enheden er i roaming Ja/Nej
- Batteristatus på enheden
- Er find min iPhone aktiveret Ja/Nej
- ActiveSync id hvis der er mail på enheden via den indbyggede native Apple email app
- Om brugeren har en låsekode på enheden Ja/Nej
- Er enheden Supervised Ja/Nej
- Lost mode tilstand aktiveret Ja/Nej
- Er enhedens OS valid og krypteringen ok
- Må enheden forstyrres Ja/Nej
- Har der været udført et simkort skifte på enheden

- Lever enheden op til den låsekode politik som er påført enheden Ja/Nej
- Apps der er installeret på enheden
 - *Her skelnes imellem apps som EMM har installeret som har status "Managed" og apps som brugeren har installeret som har status "ikke managed". På Instansen kan Privacy modes aktiveres af Telenor i forskellige niveauer, hvilket bl.a. kan skjule bruger installerede apps. EMM-løsningen kan se dette, data ligger i clouden, men EMM admin kan ikke se dette.*
- Konfigurationer, certifikater eller opsætninger der er udrullet fra EMM serveren
- IP-adressen fra hvor port 443 EMM-trafikken fra enheden kommer fra
- Hvis enheden er Supervised aktiveret, så kan Lost mode-funktionen gennemtvinge en GPS-lokalisering af enheden, selvom Find my iPhone/iPad ikke er aktiveret på enheden

*Følgende data behandles **ikke***

- Beskeder (alle former for beskeder, på nær det som EMM har sendt til enheden)
- Mails, SMS og MMS
- Fotos
- Opkaldshistorik
- Hvor lang tid brugeren benytter enheden
- Brug af apps (tid og hyppighed)
- Se data der ligger inde i apps
- Private Apple id-oplysninger på enheden
- Browser historik
- Noter

Enhedsoplysninger, når der er tale om Android enheder

- OS platform
- Management tilstand (enhed, administreret enhed, arbejdsprofil, arbejdsprofil på firmaejet enhed)
- OS version
- Firmware ID
- Product model ID for enheden
- Er der en AE (Managed Google Play) konto på enheden og ID + status for denne
- IMEI-nummer – til og med OS12, herefter er det et tilfældig Android ID
- Serienummer
- Push status
- Managed Google Play auto update politik/status
- MAC adresser – hvis OS versionen tillader udlæsning af dette

- Sprogvalg
- Tidszone indstilling
- Enhedens navn som bruger måtte have døbt denne i Indstillinger -> Generelt -> Om
- Hukommelses forbrug på RAM, Flash hukommelsen og på eventuelt isat SD kort
- Hvis simkort er isat, så aflæses IMSI og ICCID på simkort såvel hvilken operator dette er fra såvel operatørens MNC og MCC-kode
- Telefonnummer på det simkort, der sidder i enheden (hvis operatøren understøtter dette og enheden ligeså)
- Hvilket mobilnetværk enheden via simkort er forbundet til
- Om enheden er i roaming Ja/Nej
- Er mobilhotspot aktiveret Ja/Nej
- Batteristatus på enheden
- Låsetid for låseskærm, hvis enheden understøtter dette
- ActiveSync ID hvis der er mail på enheden via den indbyggede native email app (primært Samsung)
- GPS-status og GPS-tilladelse
- Kiosk tilstand aktiveret Ja/Nej
- Om brugeren har en låsekode på enheden Ja/Nej og evt. også hvis der er tilknyttet en profil
- Er enhedens OS valid og krypteringen ok
- Har der været udført et simkort skifte på enheden
- Lever enheden op til den låsekode politik som er påført enheden Ja/Nej
- Apps der er installeret på enheden.
 - *Her skelnes imellem apps som EMM har installeret som har status "Managed" og apps som brugeren har installeret som har status "ikke managed". På Instansen kan Privacy modes aktiveres af Telenor i forskellige niveauer, hvilket bl.a. kan skjule bruger installerede apps. EMM-løsningen kan se dette, data ligger i clouden, men EMM admin kan ikke se dette.*
- Konfigurationer, certifikater eller opsætninger der er udrullet fra EMM serveren
- IP-adressen fra hvor port 443 EMM-trafikken fra enheden kommer fra

Følgende data behandles *ikke*

- Beskeder (alle former for beskeder, på nær det som EMM har sendt til enheden)
- Mails, SMS og MMS
- Fotos
- Opkaldshistorik
- Hvor lang tid brugeren benytter enheden
- Brug af apps (tid og hyppighed)

- Se data der ligger inde i apps
- Private Google konto - oplysninger på enheden
- Browser historik
- Noter