25.04.2018

Tjenestespesifikke vilkår for behandling av personopplysninger
Nordic Connect Firewall og Internet

Telenors leveranse av 'Nordic Connect Firewall og Internet' (Tjenesten) kan innebære behandling av personopplysninger på vegne av kunden. For de deler av Tjenesten som ikke er telekommunikasjon er Telenor da databehandler, og kunden er behandlingsansvarlig under personopplysningsloven.

Når Telenor er databehandler på vegne av kunden er behandlingen av personopplysninger regulert av særskilte databehandlervilkår. Databehandlervilkårene fremgår av punktet Behandling av personopplysninger, jf. punkt 22 i Generelle vilkår i Telenors Tjenesteavtale eller annen særskilt forhandlet tjenesteavtale (for kunder som har forhandlet en kundespesifikk avtale med Telenor), eller punkt 9 i Alminnelige vilkår for bedrifter for øvrige kunder.

For tjenester og/eller prosesser hvor Kunden delvis eller i sin helhet er behandlingsansvarlig er det Kundens ansvar å sikre lovlig formål og rettslig grunnlag (hjemmel) for behandlingen av personopplysninger. Kunden skal også sikre at egne brukere av Tjenesten er informert om Tjenesten og hvordan denne fungerer. Endelig har Kunden ansvar for at abonnement som skal ha Tjenesten er registrert hos Telenor med korrekt navn på Bruker.

Oversikten under inneholder opplysninger som er av relevans for Partenes oppfølgning av databehandlervilkårene.

Navn på tjeneste/prosess regulert av databehandlervilkårene	'Nordic Connect Firewall og Internet'
Hva er formålet med databehandlers behandling av personopplysninger på vegne av behandlingsansvarlig?	'Nordic Connect Firewall og Internet' har til formål å gi kunden tilgang til Internett. Tjenesten gir også kunden mulighet til å sikre kommunikasjons- og IT-løsningene mot datainnbrudd og andre sikkerhetstrusler, og dermed bidra til at kundens kommunikasjons- og IT-løsninger fungerer som de skal, uten at konfidensiell eller personsensitiv informasjon kommer på avveie eller blir manipulert med.
Hvilke typer av personopplysninger behandles?	Dataene som behandles i tjenesten er ikke et systematisert sett av personopplysninger, men de data som kunden/bedriften/brukeren velger å kommuniserer gjennom tjenesten. Personopplysninger kan forekomme i dette datagrunnlaget, men er ikke strukturert ifht. dette. Informasjonen er dermed sammenlignbar med den trafikken som en kunde/bedrift velger å sende over en bredbåndsaksess levert av Telenor.
Hvordan behandler Databehandler personopplysningene?	Ref. forrige punkt, så utfører ikke Telenor noen lagring eller systematisering av personopplysninger ifm. tjenesten. Det kan imidlertid forekomme at personopplysninger blir synlig for Telenors driftspersonell når feil på tjenesten og eventuelle sikkerhetshendelser må analyseres for å gjøre tjenesten operativ igjen, eller kunne avverge et dataangrep. Hvis dette blir tilfelle, så er det etablert rutiner om å slette det analyserte innholdet når feilen eller situasjonen er løst.

	Plattformen kan i noen tilfeller åpne kryptert kommunikasjon for å analysere innhold og utføre tjenestens funksjoner, for deretter å gjenopprette den krypterte sesjonen videre til mottaker. Dette skjer kun etter avtale med kunde, og kunden er ansvarlig for å informere egne ansatte, ref. det som er skrevet innledningsvis i dette kapitlet. Logg fra den tekniske plattformen kan også presenteres i en portal som Telenor tilgjengeliggjør for en administrator hos kunden, eventuelt kan logg sendes som en datastrøm til et IT-system spesifisert av kunden.
Bruker databehandler underleverandører til behandling av personopplysningene?	Nei
I hvilke land behandles personopplysningene?	Norge
Har Databehandler inngått avtale med underleverandør i henhold til EUs prinsipper for standardavtale om overføring av personopplysninger til land utenfor EU/EØS?	Nei, se punktet over.
Hvordan og når slettes personopplysningene?	Ref. det som er beskrevet her, så er ikke dataene gruppert på personnivå, dvs at datagrunnlaget håndteres på generelt grunnlag. Lagringstid av dataene kan være inntil 12 måneder. Dette er nødvendig for å kunne avdekke skadeomfang, utføre feilretting, og rydde opp i konfigurasjon dersom hacking og datainnbrudd blir oppdaget.