Databeskyttelseskonsekvensvurdering (DPIA) for *Sensedesk Assist*

Sist oppdatert: 05.01.2025

1. Introduksjon

1.1 Formål med DPIA-en

Denne DPIA-en er utarbeidet for å identifisere og vurdere de personvernrelaterte risikoene ved bruk av vår Windows-baserte fjernstyringsapplikasjon *Sensedesk Assist*, samt for å beskrive hvilke tiltak som er implementert – eller planlegges – for å redusere disse risikoene. Formålet er å sikre at behandlingen av personopplysninger skjer i samsvar med GDPR og andre relevante regelverk.

1.2 Om applikasjonen

- Plattform: Windows 10/11
- Utviklingsrammeverk: .NET 8
- Hovedfunksjonalitet: Fjernstyring av andre Windows-PC'er og servere
- Autentisering: Brukere autentiserer seg som gjest via Sense Data Entra ID
- Kommunikasjonsprotokoll: HTTPS/TLS 1.2
- Servere: Kommunikasjonen går via IIS relay-servere lokalisert i Norge, der dataflyten benytter .ASHX/SSE-teknologi
- Kryptering: All kommunikasjon er ende-til-ende-kryptert
- Brannmur: Kun port 443 benyttes, slik at ingen andre porter kreves åpnet

2. Beskrivelse av behandlingsaktiviteten

2.1 Formål og funksjonalitet

Applikasjonen er utviklet for å muliggjøre:

- Effektiv IT-drift og systemadministrasjon
- Fjernsupport og vedlikehold av Windows-baserte PC'er og servere
- Sikker tilgang for autoriserte brukere uten at brukerne trenger å være fysisk til stede

2.2 Behandlingsgrunnlag

Behandlingen av data i applikasjonen er basert på følgende rettsgrunnlag:

- Samtykke: Brukeren gir aktivt samtykke ved å logge inn som gjest via Entra ID.
- Kontrakt: Oppfyllelse av en kontrakt (f.eks. IT-supportavtale) der fjernstyring er nødvendig for å levere tjenesten.
- Legitim interesse: Effektiv systemadministrasjon og beskyttelse av IT-miljøet.

2.3 Hvilke data behandles

Følgende datakategorier kan behandles:

- Autentiseringsdata: Bruker-ID, påloggingsinformasjon, autentiseringstoken fra Entra ID.
- Tilgangs- og tilkoblingslogger: Tidsstempler, enhets- og sesjonsdata.
- Fjernstyringsdata: Overførte kommandoer, skjermbilder, tastetrykk og annen interaksjonsdata under sesjonen.
- Metadata: Informasjon knyttet til tilkoblingskvalitet, eventuelle feilmeldinger og systemloggdata for feilsøking.

2.4 Dataflyt og behandlingsprosesser

Autentisering:

- Brukeren autentiserer seg via Entra ID og får tildelt nødvendige rettigheter for fjernstyring.

Etablering av tilkobling:

- Etter autentisering etableres en sikker forbindelse via HTTPS/TLS 1.2.
- Ved permanent fjernstyring der Sensedesk Assist startes «med Windows»: Bruker angi et (minimum) 12-tegn passord for tilgang til enhet. Whitelisting av brukertilgang er mulig per enhet som fjernstyres.

Dataoverføring:

- Kommunikasjonen mellom klienten og den fjernstyrte enheten går via våre IIS relay-servere i Norge, med alle data kryptert ende-til-ende.

Logging:

- Tilkoblings- og autentiseringsdata logges for sikkerhets- og feilsøkingsformål, med tilgang begrenset til autorisert personell og i samsvar med lovpålagte oppbevaringsfrister.

3. Risikoanalyse

3.1 Identifiserte risikoer

Uautorisert tilgang:

- Dersom autentiseringsmekanismene (Entra ID), enhets-ID og passord kompromitteres, kan uvedkommende få tilgang til sensitive systemer.

Datainnbrudd:

- Risiko for at sensitiv informasjon, som autentiseringsdata og tilkoblingslogger, kan bli avlyttet eller eksponert ved et eventuelt sikkerhetsbrudd.

Misbruk av fjernstyringsfunksjonalitet:

- En autorisert bruker med ondsinnet hensikt kan utnytte funksjonaliteten for å utføre uautoriserte handlinger på fjernstyrte systemer.

Systemfeil og datatap:

- Feil i systemet kan føre til tap av logger eller andre data, noe som kan hindre muligheten for å spore hendelser og gjenopprette systemtilstanden.

3.2 Sannsynlighet og konsekvens

Sannsynlighet:

- Med dagens sikkerhetstiltak (TLS 1.2, ende-til-ende kryptering, begrensede porter og autentisering via Entra ID), samt passordbeskyttelse og *Whitelisting*, vurderes risikoen for uautorisert tilgang og datainnbrudd som lav. Likevel må det gjennomføres kontinuerlig overvåking og periodiske sikkerhetstester.

Konsekvens:

- Et eventuelt brudd kan medføre betydelig skade, blant annet tap av sensitiv informasjon, kompromittering av systemadministrasjon og negativ påvirkning på virksomhetens omdømme.

4. Risikoreduserende tiltak

4.1 Tekniske tiltak

Sterk kryptering:

- All kommunikasjon foregår over HTTPS/TLS 1.2 med ende-til-ende kryptering, noe som hindrer avlytting og datatap under overføring.

Autentisering via Entra ID:

- Brukere må autentisere seg som gjennom Entra ID, som sikrer at kun autoriserte brukere får tilgang. Ved permanent fjernstyring, der Sensedesk Assist startes «med Windows», kreves det også et 12-tegns passord for tilgang.

Begrenset nettverkseksponering:

- Kun port 443 er åpnet, noe som reduserer angrepsflaten mot uautoriserte inntrengere.

Logging og overvåking:

- Kontinuerlig overvåking av tilkoblingslogger og sikkerhetshendelser for raskt å identifisere og respondere på mistenkelig aktivitet.

Regelmessige oppdateringer:

- Systemet og tilhørende infrastruktur oppdateres jevnlig for å sikre at kjente sårbarheter blir adressert.

4.2 Organisatoriske tiltak

Opplæring og bevisstgjøring:

- Ansatte som har tilgang til systemet får regelmessig opplæring i IT-sikkerhet og personvern.

Strenge tilgangskontroller:

- Interne retningslinjer for hvem som har tilgang til sensitive logger og systemadministrasjonsdata.

Revisjon og internkontroll:

- Gjennomføring av jevnlige revisjoner for å evaluere sikkerhetsprosedyrer og sikre at retningslinjer etterleves.

Sikkerhetspolicyer:

- Implementering av omfattende sikkerhetspolicyer og beredskapsplaner for å håndtere eventuelle sikkerhetsbrudd.

5. Vurdering av nødvendighet og forholdsmessighet

Behandlingen av data gjennom applikasjonen er vurdert som nødvendig for å:

- Opprettholde effektiv IT-drift og administrasjon
- Gi rask tilgang til støtte og feilsøking av kritiske systemer
- Oppfylle kravene til sikkerhet og sporbarhet i en IT-driftssammenheng
- Dataminimering er ivaretatt ved at kun nødvendige data samles inn og lagres, og alle tiltak er utformet for å sikre integritet, konfidensialitet og tilgjengelighet i tråd med GDPR-prinsippene.

6. Overføring av data og tredjepartsbehandling

6.1 Lokalisering av data

All datakommunikasjon skjer via IIS relay-servere lokalisert i Norge. Dette sikrer at data behandles innenfor EØS og i henhold til norsk lovgivning.

6.2 Tredjepartsleverandører

Dersom det benyttes tredjepartsleverandører for logging, overvåking eller andre formål, vil det etableres nødvendige databehandleravtaler for å sikre at disse partene oppfyller GDPR-kravene.

6.3 Internasjonale overføringer

Ingen data overføres til land utenfor EØS med mindre det er etablert tilstrekkelige sikkerhetstiltak og garantier for databeskyttelse.

7. Oppfyllelse av individets rettigheter

7.1 Informasjon og transparens

- Brukere informeres tydelig om hvilke data som behandles, formålet med behandlingen og deres rettigheter gjennom tydelige personvernerklæringer.

7.2 Rett til innsyn, retting og sletting

- Brukere har rett til å be om innsyn i egne data, be om korrigering av eventuelle feil og i visse tilfeller kreve sletting av data, med unntak der lovpålagte oppbevaringskrav foreligger.

7.3 Begrensning av behandling

- Ved forespørsel kan behandlingen begrenses, for eksempel ved midlertidig deaktivering av fjernstyring eller ved anonymisering av data.

7.4 Sikkerhet ved overføring

- Gjennomgående bruk av kryptering og sikre kommunikasjonskanaler sikrer at dataoverføringer ikke utsetter de registrerte for unødvendig risiko.

8. Konklusjon og anbefalinger

På bakgrunn av vurderingene ovenfor konkluderes det med at:

- Applikasjonen, med implementerte tekniske og organisatoriske tiltak, i dag ivaretar de grunnleggende kravene i GDPR.
- Risikoen for uautorisert tilgang, datainnbrudd og misbruk av fjernstyringsfunksjonalitet er lav, gitt korrekt og kontinuerlig drift samt regelmessige sikkerhetstiltak.
- Tiltakene for logging, overvåking og oppdatering er essensielle for å opprettholde et høyt sikkerhetsnivå.

Anbefalinger:

- Kontinuerlig overvåking og revisjon: Sikre at systemet gjennomgår periodiske sikkerhetsrevisjoner og sårbarhetstester.
- Oppdatering av tilgangskontroller: Gjennomgå og oppdater tilgangskontrollene regelmessig for å tilpasse eventuelle endringer i brukerroller og rettigheter.
- Opplæring: Fortsett med regelmessig opplæring av personell knyttet til IT-sikkerhet og personvern.
- Dokumentasjon: Hold DPIA-dokumentasjonen oppdatert, spesielt ved endringer i systemarkitektur eller nye funksjonaliteter.