Tilleggstiltak iht. anbefalinger fra EDPB

Versjon v2
Sist oppdatert 20.04.2023

Tilleggstiltak iht. anbefalinger fra EDPB

1. Innledning

Ledidis løsninger oppfyller kravene i Normen, og er utviklet med innebygget personvern og informasjonssikkerhet som standard (GDPR art. 25 og 32). Løsningene benytter ende-til-ende kryptering med beskyttet prosessering (confidential computing) iht. kravene om tilleggstiltak fra EDPB som kom i kjølvannet av Schrems-II dommen juli 2020. Ledidi benytter i tillegg tjenester som er sertifisert iht. CISPE Code of conduct (GDPR art. 28, 32, 40 og 41). CISPE Code of conduct (adferdsregler) er et regelverk for sertifisering av skytjenester som ble godkjent av EDPB mai 2021, og som trådte i kraft februar 2022.

2. Bakgrunn

GDPR artikkel 25 og 32 krever "state of the art" sikkerhetsteknologier for å ivareta personvernet ved behandling av personopplysninger. GDPR artikkel 28 stiller også krav til at databehandlere gir tilstrekkelige garantier for at de vil gjennomføre egnede tekniske og organisatoriske tiltak som sikrer databehandlingen.

For å klargjøre hva som i praksis skal forstås med «state of the art», utgir EUs organ for cybersecurity (ENISA) i samarbeid med Teletrust (IT Security Association Germany) veiledningen State of the art – Technical and organisational measures relatert til kravene i GDPR art. 25 og 32. Veiledningen angir hvilke teknologier (eks. kryptering, autentisering) som oppfyller de juridiske kravene til datasikkerhet iht. GDPR:

«*These guidelines are intended to provide companies using it and providers (manufacturers, service providers) alike with assistance in determining the "state of the art" within the meaning of the IT Security Act (ITSiG) and the General Data Protection Regulation (GDPR). The document can serve as a reference for contractual agreements, procurement procedures or the classification of security measures implemented".*

"The "state of the art" refers to the best performance of an IT security measure available on the market to achieve the legal IT security objective".

https://www.teletrust.de/fileadmin/user_upload/2021-09_TeleTrusT_Guideline_State_of_the_art_in_IT_security_EN.pdf

3. Schrems II-dommen og anbefalinger om tilleggstiltak fra EDPB

Schrems II-dommen fra 20. juni 2020 kjente Privacy Shield som dataoverføringsgrunnlag ugyldig.

18. juni 2021 publiserte Det europeiske personvernrådet (EDPB) publiserte anbefalinger om tilleggstiltak ved bruk av allmenne skyløsninger (https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf). Endelig versjon av disse anbefalingene kom etter at EU-kommisjonen hadde utgitt nye standardavtaler for regulering av dataoverføring. Kravene til tilleggstiltak gjelder hvis bl.a. hvis skyleverandøren er et amerikansk selskap. Ledidi benytter AWS (datasenter i Frankfurt, Tyskland) som infrastrukturleverandør, og kravene til tilleggstiltak gjør seg derfor gjeldende.

Tilleggstiltakene fra EDPB kategoriseres i tre grupper: Tekniske, kontraktuelle og organisatoriske. Tiltakene kan benyttes alene eller i kombinasjon. Kontraktuelle og organisatoriske tiltak bidrar til den totale datasikkerheten og personvernet, men kun teknisk

beskyttelse av dataene kan garantere sikkerheten. Ledidi forventer at de tekniske tilleggskravene vil bli gjeldende bransjestandard selv med en ny dataoverføringsavtale mellom EU og USA (https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_6045).

Ledidi har implementert både tekniske, organisatoriske og kontraktuelle tilleggstiltak.

4. Tekniske tilleggstiltak – confidential computing

I tillegg til tradisjonell kryptering av data under transport og ved lagring, krever EDPB i sine retningslinjer (Use case 6) at det iverksettes tilleggstiltak for å beskytte data under prosessering (data in use). På det tidspunktet retningslinjene ble utgitt var det uklart hvordan dette skulle løses. I september 2021 kom det imidlertid ny utgave av ENISAs veiledning hvor «confidential computing» er tatt inn som state of the art for beskyttelse av data under prosessering i public cloud (punkt 3.2.25 side 58). Dette korresponderer med tilleggstiltaket som må iverksettes iht. Use Case 6.

Privileged access by administrators to data during processing is traditionally only secured with organizational or reactive measures against misuse of the privilege. With the help of confidential data processing (Confidential Computing), this data is tamper-proof and preventively protected against unauthorized access. This is particularly important for applications in the field of cloud computing. Confidential data processing corresponds to the protection requirement when cloud services are used for critical infrastructures or for sensitive data processing processes, e.g. in medicine, industry or in regulated areas (e.g. regTech).

EDPB henviser forøvrig eksplisitt til ENISAs veileder:

"...data exporters can rely on technical guidance published by official cybersecurity authorities of the EU and its member states. See e.g. ENISA Report « What is "state of the art" in IT security? », 2019, https://www.enisa.europa.eu/news/enisa-news/what-is-state-of-the-art-in-it- security"

I Ledidi Core er dataene beskyttet med kryptering under transport, ved lagring og ved hjelp av confidential computing under prosessering, og oppfyller således kravene fra EDPB og ENISA til informasjonssikkerhet ved behandling av sensitive data.

For confidential computing benyttes tjenesten AWS EC2 Nitro:

"We've designed the Nitro System to have no operator access. With the Nitro System, there's no mechanism for any system or person to log in to EC2 servers (the underlying host infrastructure), read the memory of EC2 instances, or access any data stored on instance storage and encrypted EBS volumes. If any AWS operator, including those with the highest privileges, needs to do maintenance work on the EC2 server, they can do so only by using a strictly limited set of authenticated, authorized, and audited administrative APIs. None of these APIs have the ability to access customer data on the EC2 server. Because these technological restrictions are built into the Nitro System itself, no AWS operator can bypass these controls and protections. For additional defense-in-depth against physical attacks at the memory interface level, we offer memory encryption on various EC2 instances."

Med confidential computing beskyttes all prosessering, ledsagende kryptografiske prosesser og administrasjonen av kryptonøkler.

Med bruk av confidential computing på AWS EC2 Nitro har AWS ingen teknisk mulighet til å kunne å lese dekrypterte data, utlevere dekrypterte data eller få tilgang til krypteringsnøkler. Dette gjelder også ved et rettslig pålegg fra amerikanske, europeiske eller noe annet lands myndigheter.

5. Organisatoriske tilleggstiltak – CISPE Code of conduct

Bransjeorganisasjonen Cloud Infrastructure Services Providers in Europe (CISPE) har i samarbeid med det franske datatilsynet (CNIL) på vegne av alle tilsynsmyndighetene i EU/EØS utviklet Code of conduct for skyinfrastruktur tjenester (Infrastructure as a Service, IaaS) iht. GDPR art. 28, 32, 40 og 41. EDPB godkjente regelverket 19. mai 2021, og det ble operativt 3. februar 2022. Regelverket sikrer at sertifiserte tjenester oppfyller kravene til databehandlere iht. GDPR art. 28.

CNIL skriver på sine sider (https://www.cnil.fr/en/cnil-approves-first-european-code-conduct-cloud-infrastructure-service-providers-iaas):

"A code of conduct is a compliance instrument: it helps members to demonstrate that they meet the requirements of Article 28 of the GDPR, which requires data controllers to use only contractors who provide sufficient guarantees regarding the implementation of appropriate technical and organisational measures".

I sin godkjenning skriver EDPB (https://edpb.europa.eu/system/files/2021-05/edpb_opinion_202117_cispecode_en_0.pdf):

«The objective of the CISPE Code is to help CISPs to demonstrate compliance with article 28 GDPR and make it easier and more transparent for customers to analyze whether cloud services are appropriate for their use case in line with article 28.1 GDPR which provides that controllers shall use only processors providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of the GDPR...»

"By way of conclusion, the EDPB considers that the draft code complies with the GDPR, since the CISPE code of conduct fulfills the requirements imposed by Article 40 and 41 GDPR."

Sertifiseringen av infrastrukturtjenestene gjøres av uavhengige kontrollorganer ("monitoring bodies") akkreditert av det franske datatilsynet.

Sertifiseringen innebærer bl.a. sertifiserte tjenester utelukkende behandler dataene i Europa, inkludert tilgang til data. Dette medfører at GDPR kap. 5 (overføring til 3. land) ikke kommer til anvendelse for sertifiserte tjenester.

Alle infrastruktur- og plattformtjenester fra AWS som benyttes i Ledidi Core til prosessering og lagring av innholdsdata (eksempelvis særlige kategorier av personopplsyninger) er sertfisert iht. til CISPE Code of conduct (se tabell for oversikt).

6. Kontraktuelle tilleggstiltak - Tillegg til databehandleravtalen med AWS

Gjennom et tillegg til sin databehandleravtale, gir AWS kontraktsmessige forpliktelser om nødvendige garantier i henhold til retningslinjer for tilleggstiltak fra EDPB (https://d1.awsstatic.com/Supplementary_Addendum_to_the_AWS_GDPR_DPA.pdf).

Gjeldende tillegg til databehandleravtalen inneholder bestemmelser som forplikter AWS til å utfordre eventuell forespørsel fra et myndighetsorgan om datautlevering, samt varsle Ledidi umiddelbart om en eventuell forespørsel fra et myndighetsorgan, slik at Ledidi kunne bruke passende rettsmiddel til å hindre myndighetens tilgang til data.

AWS gjennomfører også tredjepartssertifiseringer og revisjoner som bekrefter at AWS oppfyller sine forpliktelser i samsvar med den signerte databehandleravtalen.

7. Oversikt tilleggstiltak

Følgende AWS tjenester benyttes til behandling av personopplysninger:

Tjeneste	Ledidis anvendelse	Persondata	CISPE Code of conduct	Sikkerhetstiltak
AWS EC2 Nitro	Prosessering av brukernes datasett og metadata	Potensielt sensitive data	Sertifisert	Confidential computing Kryptert lagring Kryptert transport
	Lagring av brukernes datasett og metadata på AWS Nitro EC2 instanser i et selvkonfigurert cluster på AWS RDS	Potensielt sensitive data		
	Prosessering og lagring av krypteringsnøkler på AWS Nitro EC2 innenfor CloudHSM cluster	Ikke relevant		
AWS S3	Fillagring i brukernes datasett (ikke prosessering)	Potensielt sensitive data	Sertifisert	Kryptert lagring Kryptert transport
AWS Lambda	Prosessering	Ikke sensitive data (brukeropplysninger): Fornavn, etternavn, bruker ID, e-post, telefonnummer, organisasjonstilhørighet og personlige innstillinger (eks. språk)	Sertifisert	Kryptert lagring Kryptert transport
AWS CloudTrail	Logging for auditing	Ikke sensitive data (brukeropplysninger): Bruker ID	Sertifisert	Kryptert lagring Kryptert transport
AWS Cognito	Autentisering av brukere	Ikke sensitive data (brukeropplysninger): Bruker ID, e-post	Sertifisert	Kryptert lagring Kryptert transport

8. Oppsummering

Det er kun AWS (Frankfurt, Tyskland) som er underleverandør av infrastrukturtjenester som benyttes til behandling av innholdsdata (prosjekt-/registerdata) i Ledidis løsninger (inkl. Ledidi Core). Det er implementert effektive og tilstrekkelige tekniske, organisatoriske og kontraktuelle tilleggstiltak. Blant annet medfører confidential computing som tilleggstiltak at det ikke er teknisk mulig for AWS å dekryptere innholdsdataene i Ledidis løsninger eller å aksessere krypteringsnøkler. Det er dermed heller ikke teknisk mulig for AWS å etterkomme et eventuelt rettslig krav fra et myndighetsorgan om utlevering av data. Dette gjelder uavhengig om kravet skulle komme fra amerikanske, europeiske eller et annet lands myndigheter. Confidential

computing oppfyller sikkerhetskravene til ENISA for prosessering av særlige kategorier av personopplysninger:

"*Confidential data processing corresponds to the protection requirement when cloud services are used for critical infrastructures or for sensitive data processing processes, e.g. in medicine, industry or in regulated areas (e.g. regTech).*"

Ledidi benytter i tillegg underleverandører som behandler kundedata og opplysninger om brukerne av våre løsninger. Disse leverer tjenester som system for kundehåndtering og for administrasjon av abonnementer. Noen av disse er multinasjonale selskaper med virksomhet utenfor EØS og kravene om overføringsgrunnlag i GDPR og anbefalingene fra EDPB gjelder. Ledidi har kun valgt leverandører med drift hos AWS med datalagring og behandling i EU / EØS (Frankfurt, Tyskland). Ledidi har utført Transfer Impact Assessment (TIA) for de aktuelle underleverandører (inklusive AWS) og innført nødvendige tilleggstiltak.