Transfer Impact Assessment – Amazon Web Services

Vurdering er udført med udgangspunkt i EDPB's anbefalinger til trin-for-trin-guide jf. trin 1 – 6 nedenfor.

Trin 1 – Kend dine overførsler

Formålet med databehandlerens behandling af personoplysninger på vegne af den dataansvarlige er:

- at den dataansvarlige kan anvende løsningen, som ejes og administreres af databehandleren, til at indsamle og behandle oplysninger om bruger-id i forbindelse med user-sessions.

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

- Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige drejer sig primært om, at der for hver bruger oprettes en konto-/brugeradgang. Denne log-in/registrering af bruger medvirker til, at produktet udarbejder en statistik for den pågældende bruger. Dette sker ved, at produkterne/services ved brug registrerer brugerens handlinger, herunder hvor mange ordforslag brugeren foreslås, at der sker tekstoplæsning, samt at billeder konverteres til tekst. Hvilke ord og billeder der er tale om, registreres dog ikke. Det er således funktionen, som registreres, men ikke indholdet af funktionerne, der registreres.

Behandlingen omfatter følgende typer af personoplysninger om de registrerede:

- Databehandlers produkter indsamler og registrerer data om brugeren ved oprettelse af log-in-/brugerkonto samt ved brugen af produktet/services for at levere den aftalte ydelse.
- Ved Erhverv- og Privatkunde registreres navn og e-mail på bruger for at oprette brugeradgang. Data opbevares så længe brugeradgang er aktiv. Herefter anonymiseres og slettes data.

- Ved Kommune-kunde er data pseudonymiseret. Navn og e-mail på bruger registreres midlertidigt under login-processen. Disse data opbevares så længe brugeradgang er aktiv, dvs. den aktive brugersession. Brugerens login-hash fra idP gemmes permanent, dog kun så længe brugeren er tilknyttet databehandlers login, eller den underliggende kontrakt er aktiv. Statistisk data er pseudonymiseret og alene tilknyttet login-hash fra idP. Disse data slettes automatisk ved aftaleophør.

Behandlingen omfatter følgende kategorier af registrerede:

- Ansatte tilknyttet dataansvarlige.
- Elever tilknyttet dataansvarlige.
- Kunder.
- Børn i alderen 6-17 år.
- Kunder/private brugere.

Data overføres ved datafangst i løsningerne, da der er tale om en SaaS løsning.

Data overføres til:

- Amazon Web Services - datacenter Greenhills Road, Tymon North, Dublin, Ireland.

Data er aftalt opbevaret i Vesteuropa (Amsterdam eller Dublin).

Generelt vurderes risikoen som værende lav, idet data kun foreligger i løsningerne i forbindelse med aktive user-sessions. Løsningerne udbydes som SaaS, og for alle løsninger er der etableret en række tekniske og organisatoriske kontroller, som afdækker risici i relation til de registreredes data. Der laves minimum årligt en risikovurdering af de forskellige løsninger i relation til de registreredes rettigheder omfattende områder som bl.a. sletning af data, uautoriseret adgang til data, uberettiget videregivelse af data. Ved væsentlige ændringer til løsningerne foretages der fornyede risikovurderinger.

Trin 2 – Kend dine overførselsgrundlag

Da overførsel potentielt kan ske til USA, er der ikke pt. et overførselsgrundlag, som støtter dette qua Schrems II afgørelsen. Aftalen med Amazon Web Services er dog specifikt på opbevaring af data i Europa.

Der er derfor i trin 3 foretaget en vurdering af, hvorvidt oplysningerne beskyttes på et tilsvarende niveau, som hvis oplysningerne blev i EU.

Der er indhentet standarddatabehandler fra Amazon Web Services, og der er indgået aftale om brug af deres teknologi. Leverandøren er udvalgt ud fra, at de er en anerkendt leverandør med en række certificeringer i relation til informationssikkerhed og GDPR samt relevante revisionserklæringer. Der foretages opfølgning på performance løbende.

Trin 3 – Tredjelandets databeskyttelsesniveau

Næste trin indebærer en vurdering af, om databeskyttelsesniveauet i det pågældende tredjeland er på højde med EU's beskyttelsesniveau.

EU-Domstolen fastslog i Schrems II-dommen, at da amerikanske efterretningstjenester har vide rammer for at få adgang til data, kan der ikke sendes data til USA, medmindre der implementeres yderligere sikkerhedsforanstaltninger og kontroller, som sikrer et beskyttelsesniveau svarende til det i EU.

Der er derfor foretaget vurdering af de kontroller, som findes i det nuværende setup med henblik på at identificere og implementere supplerende foranstaltninger, som vil bringe beskyttelsen op på EU-niveau. Dette vil kunne ske på baggrund af risikovurderingen i trin 1.

Vurderingen er foretaget med afsæt i Datatilsynets liste over sikre tredjelande: https://www.datatilsynet.dk/internationalt/tredjelandsoverfoersler

Trin 4 – Supplerende foranstaltninger

Baseret på en vurdering af det nuværende setup, som er et miks af kontroller hos Amazon Web Services samt egne etablerede kontroller, er det vores vurdering, at kontrollerne er dækkende ift. risikobilledet for overførslen.

Der er implementeret følgende kontrolforanstaltninger for at afdække risikoen:

- Adgang til alle databehandlers systemer er sikret med MFA og alle databehandlers medarbejdere med adgang til driftsmiljøer har underskrevet en udvidet fortrolighedserklæring.
- Som primære driftsmiljø anvendes AWS i Irland, hvor data hostes, og hvor AWS indbyggede CloudTrail er aktiveret. Det betyder, at alle databehandlers medarbejderes log-ins og handlinger udført i driftsmiljøer bliver logget i 90 dage. Audit-log bliver løbende overvåget.
- Produkterne anvender både kryptering "in transit" og "at rest". Det betyder blandt andet, at alle forbindelser til "backend" er krypteret med TLS v1.3 "in transit". Kryptering "at rest" afhænger af medie, men AES256 er oftest benyttet.
- Udstedelse af krypteringsnøgler og certifikater sker via Let's Encrypt, AWS KMS eller ACM.
- Databehandler foretager løbende driftsovervågning af IT-systemer.
- Adgang til databehandlers netværk sikres blandt andet ved brug af firewall, VPN-klient og beskyttet WiFi.

Baseret herpå vurderes det, at overførslen af personoplysninger kan opretholdes.

Trin 5 – Processuelle skridt

Vi vurderer ikke, at de supplerende foranstaltninger er modstridende med det overførselsgrundlag, man benytter, og at foranstaltningerne reelt sikrer, at det beskyttelsesniveau, der garanteres i GDPR, ikke undermineres.

Trin 6 – Revurdér beskyttelsesniveauet

Vi vil kontinuerligt – og minimum årligt - gennemføre en revurdering af beskyttelsesniveauet for de data, der overføres til tredjelande, og at det overvåges, om der har været eller vil være en udvikling, der kan påvirke beskyttelsesniveauet.