Transfer Impact Assessment – Microsoft Cognitive Services, speech to text.

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 slutbrugeren kan anvende funktionen tale til tekst i produktet IntoWords, via Microsofts Cognitive services.

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 konvertere indtalt lyd til tekst. Funktionaliteten tale-til-tekst.

Behandlingen omfatter følgende typer af personoplysninger om de registrerede:

- Alle former for indtalt tekst behandles, når brugeren anvender tale-til-tekst.
- Brugeren selv er anonymiseret, den indtalte tekst er ikke ændret.

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:

- Microsoft Azure Cognitive Services I Nordeuropa, Irland.

Generelt vurderes risikoen som værende meget lav, da Microsoft i deres løsningsbeskrivelse erklærer, at data ikke gemmes, men behandles og slettes.

https://docs.microsoft.com/en-us/legal/cognitive-services/speech-service/speech-to-text/data-privacy-security#data-storage-and-retention

https://azure.microsoft.com/en-us/support/legal/cognitive-services-compliance-and-privacy/

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 Microsoft Azure 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 Microsoft Azure, 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 set-up 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 set-up, som er et miks af kontroller hos Microsoft Azure 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 databehandlerens systemer er sikret med MFA og alle databehandlerens medarbejdere med adgang til driftsmiljøer har underskrevet en udvidet fortrolighedserklæring.
- Som primære driftsmiljø for tale-til-tekst anvendes Microsoft Azure i Irland, hvor data behandles.
- 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.
- Databehandler foretager løbende driftsovervågning af IT-systemer.
- Adgang til databehandlerens 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.