# Personvernkonsekvensvurdering

For modellvalget Azure globalt (inkl. USA) pluss modellprodusentens egen tjeneste: en ledetekst kan behandles i en hvilken som helst Azure-region i verden, også i USA, og, for modellene dere sender dit, hos modellprodusenten utenfor deres Azure-tenant. GDPR artikkel 35.

> **Mal.** Fyll ut hvert felt i hakeparentes, les hver del opp mot hvordan virksomheten bruker Fundarem, og la den ansvarlige signere før dere slår på modellvalget. En DPIA er deres dokument som behandlingsansvarlig; vi fyller bare inn det produktet selv gjør.

BEHANDLINGSANSVARLIG (DERE)

[virksomhetens juridiske navn]

ORGANISASJONSNUMMER
[organisasjonsnummer]

PERSONVERNOMBUD ELLER ANSVARLIG PERSON
[navn og e-post]

DATABEHANDLER

[oppgitt i avtalen vi signerer med dere]

KONTAKT
mg@fundarem.com

## Hva som vurderes

| | |
|---|---|
| MODELLVALG | Azure globalt (inkl. USA) og modellprodusentens egen tjeneste (`global-and-vendor-api`) |
| SENDES TIL MODELLEN | Ledeteksten og konteksten for det ene kallet, med personopplysninger maskert av anonymisereren |
| HVOR DET BEHANDLES | En hvilken som helst Azure-region i verden, også i USA (Azure AI Foundry, Global Standard-utrulling); for modeller som sendes til modellprodusentens egen tjeneste, tjenestens egne steder, utenfor deres Azure-tenant |
| LAGREDE DATA | Bygget for å bli i deres egen Azure-tenant, i EU/EØS-regionen som ble valgt ved installasjon |
| MAL | Versjon 1.1, laget 2026-11-11 |

## 01 Beskrivelse av behandlingen

**Art.** Fundarem kobler sammen virksomhetens systemer, beskriver dataene som ett kart av objekter, koblinger og handlinger, og lar KI-agenter og en assistent lese det og foreslå endringer. Hver endring blir foreslått, godkjent og så utført.

**Formål.** [formålene virksomheten bruker Fundarem til, f.eks. rapportering, oppfølging av fakturaer, spørsmål om kunder]

**Tilkoblede systemer.** [systemene som er koblet til, f.eks. regnskap, CRM, e-post]

**Registrerte.** [hvem dataene i systemene gjelder, f.eks. ansatte, kontaktpersoner hos kunder og leverandører]

**Personopplysninger i ledetekster.** En ledetekst inneholder spørsmålet og postene det trenger. Før hvert modellkall maskerer anonymisereren kolonnene som er merket som personopplysninger, og navn og mønstre den kjenner igjen (navn, fødselsnumre, e-postadresser, telefonnumre, bankkontoer); de maskerte verdiene erstattes med plassholdere og settes tilbake bare inne i deres tenant. [en kolonneklasse administratoren har slått anonymisereren av for på denne ruten, eller «ingen»]

**Særlige kategorier (art. 9).** [om ledetekster kan inneholde helse-, fagforenings-, biometriske eller andre særlige opplysninger; i så fall hold de klassene på en modell inne i deres tenant]

## 02 Nødvendighet og forholdsmessighet

**Hvorfor dette modellvalget.** [grunnen, f.eks. at en modell dere trenger bare tilbys gjennom produsentens egen tjeneste, eller svarkvalitet]

**Alternativer som er vurdert.** Azure Europa (EU-datasonen, hver ledetekst behandles i EU) og en selvdrevet modell i deres egen region holder behandlingen i EU; Azure globalt uten modellprodusentens egen tjeneste holder den innenfor Azure-avtalen. [hvorfor de ikke er nok for dette formålet]

**Behandlingsgrunnlag.** [behandlingsgrunnlaget per formål (art. 6)]

**Dataminimering.** Hver kobling henter bare de felt som er erklært; hver rolle ser bare objekttypene tilgangen tillater; modellen får bare konteksten for ett kall og beholder ingenting mellom kall.

## 03 Overføring ut av EU/EØS

Med dette modellvalget kan en ledetekst behandles utenfor EU/EØS av Microsoft, deres egen leverandør under deres egen Azure-avtale, ikke en underleverandør vi bruker, og, for modellene dere sender til modellprodusentens egen tjeneste, av modellprodusenten etter dens egne vilkår, utenfor Azure-avtalen. Skriv ned overføringsgrunnlaget dere bygger på for hver mottaker (GDPR kapittel V):

- **Tilstrekkelighet:** EU-US Data Privacy Framework, hvis leverandøren er sertifisert etter det. [sjekket på dataprivacyframework.gov den (dato), for Microsoft og for modellprodusenten]
- **Standard personvernbestemmelser:** i Microsofts Data Protection Addendum (Products and Services DPA). [versjon og dato for avtalen dere har godtatt]
- **Modellprodusentens vilkår:** standard personvernbestemmelser eller annet overføringsgrunnlag i modellprodusentens egne databehandlervilkår for tjenesten, som Azure-avtalen deres ikke dekker. [modellprodusentens navn, og versjon og dato for vilkårene dere har godtatt]
- **Supplerende tiltak i produktet:** anonymisereren på hver rute som standard; maskerte verdier forlater aldri deres tenant; et kall som ville bære en ubeskyttet verdi, blir avvist; modellen beholder ingenting.

**Hos leverandøren.** Hvordan hver leverandør lagrer ledetekster (for eksempel for misbruksovervåking), følger deres avtale med den; modellprodusentens tjeneste følger dens egne vilkår, ikke Azure-avtalen deres. [hva Azure-avtalen og modellprodusentens vilkår sier, og et eventuelt unntak dere har søkt om hos en av dem]

## 04 Risikoer og tiltakene mot hver

- **Personopplysninger når modellen og blir eksponert eller gjenbrukt.** Tiltak: anonymisereren på som standard, per kolonneklasse per rute, endringer logget og under deres godkjenningsregel; modellpolicyen avviser en svakere modell. Restrisiko: [lav / middels / høy]
- **Innsyn fra myndigheter i et tredjeland.** Tiltak: maskering før kallet; bare ledeteksten for ett kall går ut; lagrede data er bygget for å bli i deres tenant i EU. Restrisiko: [lav / middels / høy]
- **En ledetekst når en mottaker utenfor Azure-avtalen.** Tiltak: modellvalget angir hvilke modeller som kan brukes; maskering før kallet; bare ledeteksten for ett kall går ut; modellprodusentens vilkår er ført opp over. Restrisiko: [lav / middels / høy]
- **Feil eller urimelig svar brukt i en beslutning.** Tiltak: agenter foreslår, en person godkjenner før noe skrives; hvert svar viser kildene sine. Restrisiko: [lav / middels / høy]
- **Andre risikoer ved deres bruk.** [risiko, tiltak, restrisiko]

## 05 Konklusjon

**Samlet restrisiko.** [lav / middels / høy]

**Beslutning.** [godtatt / godtatt med disse ekstra tiltakene / ikke godtatt]

**Forhåndsdrøfting.** Er restrisikoen fortsatt høy, drøfter den behandlingsansvarlige med tilsynsmyndigheten før behandlingen starter (art. 36; i Norge Datatilsynet). [nødvendig: ja / nei]

**Neste gjennomgang.** [dato, og senest når modellvalget, de tilkoblede systemene eller formålene endres]

> Produktopplysningene i denne malen stemmer med vår DPIA, databehandleravtale og dataflyt på Tillit-siden på nettstedet vårt.

## 06 Signering

Signeres for den behandlingsansvarlige etter at personvernombudet (eller den som er ansvarlig for personvern) har gitt sin uttalelse.

FOR DEN BEHANDLINGSANSVARLIGE

Navn

Stilling

Dato

Signatur

PERSONVERNOMBUDETS UTTALELSE

Navn

Stilling

Dato

Signatur