Privat AI, GDPR og EU's AI-forordning: hvad der ændrer sig når AI kører på jeres egne servere

En praktisk guide til ledere, databeskyttelsesrådgivere og IT: hvor personoplysningerne havner i et AI-system, hvordan jeres arbejde med GDPR og AI-forordningen ændrer sig når AI kører på jeres egne servere, og hvad der stadig er jeres ansvar.

10. november 2026



empisto.ai · lokal · privat · pålidelig

Indhold

01 Resumé

02 Hvor personoplysninger optræder i et AI-system

03 De to veje sammenlignet

04 GDPR, princip for princip

05 EU’s AI-forordning

06 Fortrolighed er mere end databeskyttelse

07 Cloud-AI, hvis I vælger det

08 Sådan forbereder I jeres vurdering

09 Læs mere

01 Resumé

Før eller siden kommer enhver brugbar AI-assistent til at behandle personoplysninger. Kontrakter nævner personer ved navn, e-mails har signaturer, HR-sager og patientnotater er i sagens natur personlige, og de spørgsmål medarbejderne skriver, nævner ofte kolleger og kunder. Alt det er behandling efter GDPR, og efter EU's AI-forordning er selve assistenten et AI-system der medfører forpligtelser.

Den sædvanlige måde at tage AI i brug på er at sende dokumenterne og spørgsmålene til en udbyders servere. Det virker, men det trækker en udbyder ind i hver eneste samtale, ofte også dens underdatabehandlere og nogle gange et andet land, og hver af dem betyder flere kontrakter, flere vurderinger og mere risiko. Kører I AI på jeres egne servere, forsvinder de fleste af disse parter ud af billedet. Compliance kommer ikke af sig selv af den grund, men arbejdet bliver mindre, mere overskueligt og lettere at dokumentere.

Denne guide forklarer hvor personoplysninger optræder i et AI-system, hvordan GDPR's vigtigste principper og AI-forordningens forpligtelser gælder, hvordan Empisto hjælper med hver af dem og hvad der stadig ligger hos jer.

HVOR DATA LIGGER

På jeres egne servere. Dokumenter, spørgsmål, svar og registreringer bliver der.

TREDJEPARTER

Ved normal brug modtager ingen AI-udbyder jeres data. Der sendes intet tilbage til Empisto.

OVERFØRSLER

Ingen som standard. Enhver forbindelse udadtil er valgfri, og det er jer der slår den til.

JERES ROLLE

I er fortsat den dataansvarlige efter GDPR og idriftsætteren efter AI-forordningen.

> **Ikke juridisk rådgivning**
>
> Denne guide beskriver hvordan Empistos design forholder sig til GDPR og EU's AI-forordning. Om en bestemt anvendelse er lovlig, afhænger af jeres formål, jeres data og jeres branche, og den vurdering må I og jeres rådgivere selv foretage.

02 Hvor personoplysninger optræder i et AI-system

Det er en god idé at begynde med en kortlægning. I en AI-assistent der svarer ud fra virksomhedens dokumenter, kan personoplysninger optræde fire steder, og for hvert sted skal de samme tre spørgsmål besvares: hvor ligger de, hvem kan se dem, og hvor længe opbevares de.



Figur 1. De fire steder hvor personoplysninger optræder i en AI-assistent. Med Empisto bliver alle fire på jeres servere.

Med en typisk cloud-AI-tjeneste går i hvert fald spørgsmålene, de uddrag der sendes med, og svarene gennem udbyderen, og alt efter tjenesten kan dokumenter og registreringer også blive gemt der. Med Empisto bliver alle fire på jeres egen infrastruktur, under de adgangsregler I selv fastsætter.

03 De to veje sammenlignet



Figur 2. De to veje. Forskellen ligger ikke kun i hvor modellen kører, men også i hvor mange parter der ser jeres data.

Forskellen viser sig i de spørgsmål en databeskyttelsesrådgiver skal kunne svare på.

Spørgsmål	Typisk cloud-AI	Empisto på jeres servere
Hvem behandler data?	I, AI-udbyderen og som regel dens underdatabehandlere	I selv, på jeres egen infrastruktur
Sker der en international overførsel?	Ofte, afhængigt af udbyderen og dens underdatabehandlere	Ikke ved normal brug
Kan data bruges til at træne eller forbedre udbyderens modeller?	Det afhænger af udbyderen, abonnementet og indstillingerne	Nej. Empisto har ingen adgang til jeres data
Hvor opbevares spørgsmål og svar?	På udbyderens systemer, på udbyderens vilkår	I jeres database, under jeres kontrol
Hvem kan ændre vilkårene?	Udbyderen	I selv, ud fra jeres egne politikker

04 GDPR, princip for princip

GDPR stiller de samme krav til et AI-system som til enhver anden behandling. Kører I det på jeres egne servere, ændrer det hvor meget af svaret I selv styrer.

GDPR-princip eller artikel	Hvad det kræver	Sådan hjælper Empisto	Det står I fortsat for
Lovlighed og formålsbegrænsning (art. 5 og 6)	Et behandlingsgrundlag for hvert formål og ingen brug til andre formål	Data bruges kun til at besvare jeres medarbejderes spørgsmål. Ingen udbyder genbruger dem til egne formål	At vælge behandlingsgrundlag og fastlægge formålene
Dataminimering (art. 5)	Kun de data der er nødvendige for formålet	Biblioteker og arbejdsområder afgrænser hvilke dokumenter en assistent kan trække på, team for team	At beslutte hvilke kilder der kobles på, og for hvem
Opbevaringsbegrænsning (art. 5)	Data opbevares ikke længere end nødvendigt	Alt gemmes på jeres servere. Der kan fastsættes opbevaringsperioder for hver type data, og platformen følger dem	At fastsætte opbevaringsperioder og anvende dem
Integritet og fortrolighed (art. 5 og 32)	Et sikkerhedsniveau der passer til risikoen	Adgang styret af bibliotek og rolle før hver søgning; login via jeres identityprovider; en auditlog der ikke kan ændres gennem Empisto; adgangskoder og nøgler opbevaret i en secrets vault	Sikring af serverne, diskkryptering og netværksdesign
Databeskyttelse gennem design og standardindstillinger (art. 25)	Indbygget beskyttelse og de mest beskyttende indstillinger som standard	Cloud-AI slået fra som standard; forbindelser udadtil slået fra indtil de slås til; personlige arbejdsområder som ingen administrator kan læse	At konfigurere arbejdsområder og adgang så de passer til jeres behov
Databehandlere (art. 28)	En kontrakt med alle der behandler data på jeres vegne	Ingen AI-udbyder behandler jeres data ved normal brug. Empistos teknikere får kun adgang til en installation efter aftale med jer	At aftale vilkårene for enhver leverandøradgang, herunder en databehandleraftale hvor det er nødvendigt
Fortegnelse over behandlingsaktiviteter (art. 30)	En fortegnelse over hvad der behandles og hvorfor	Et klart overblik over hvad der er gemt hvor, og en auditlog over aktiviteten	At føre jeres fortegnelse over behandlingsaktiviteter

GDPR-princip eller artikel	Hvad det kræver	Sådan hjælper Empisto	Det står I fortsat for
Konsekvensanalyse (art. 35)	En konsekvensanalyse når behandlingen sandsynligvis vil indebære en høj risiko	Færre parter og datastrømme at vurdere, og dokumentation af arkitekturen	At afgøre om en konsekvensanalyse er nødvendig, og gennemføre den
Internationale overførsler (kapitel V)	Garantier for data der forlader EU	Ingen overførsel ved normal brug, fordi data bliver på jeres servere	At vælge hvor jeres servere står
De registreredes rettigheder (art. 15 til 22)	Indsigt, berigtigelse, sletning og dataportabilitet efter anmodning	Brugerne kan eksportere deres samtaler, og én persons data kan eksporteres eller slettes på tværs af platformen efter anmodning	At håndtere anmodningerne og kontrollere identiteten

05 EU's AI-forordning

AI-forordningen regulerer AI-systemer ud fra den risiko de indebærer, og den lægger forskellige forpligtelser på den virksomhed der leverer et system (udbyderen), og på den der bruger det (idriftsætteren). Når I bruger Empisto, er Empisto udbyder af platformen, og I er idriftsætteren.

Forpligtelserne indfases over flere år, og den digitale omnibus om AI (forordning (EU) 2026/1744, i kraft siden 27. juli 2026) har flyttet flere datoer. Forbuddet mod visse former for AI-praksis og pligten vedrørende AI-færdigheder har gældt siden februar 2025; omnibussen omformulerede den sidste til en pligt til at støtte medarbejderne i at opbygge AI-færdigheder og tilføjede nye forbud fra 2. december 2026. Gennemsigtighedsforpligtelserne gælder fra august 2026, og udbydere af generative systemer der allerede var bragt i omsætning før da, har frist til 2. december 2026 til at mærke det indhold de genererer. Reglerne for højrisikoanvendelser gælder fra 2. december 2027 for anvendelserne i bilag III og fra 2. august 2028 for AI indbygget i produkter omfattet af bilag I. Jeres rådgivere kan bekræfte hvilke datoer der gælder for jer.

Hvad der normalt gælder for en intern AI-assistent

En assistent der hjælper medarbejderne med at finde information i virksomhedens dokumenter, er som udgangspunkt ikke et højrisikosystem. Det er typisk disse forpligtelser der har betydning.

Forpligtelse efter AI-forordningen	Hvad den kræver	Sådan hjælper Empisto	Det står I fortsat for
AI-færdigheder (art. 4)	Tiltag der hjælper medarbejdere som bruger AI, med at opbygge AI-færdigheder; et bestemt niveau skal ikke garanteres	Svarene viser deres kilder, så folk lærer at tjekke dem	At klæde jeres medarbejdere på

Forpligtelse efter AI-forordningen	Hvad den kræver	Sådan hjælper Empisto	Det står I fortsat for
Gennemsigtighed (art. 50)	Folk ved hvornår de har med AI at gøre, og genereret indhold er markeret	Svar, eksporterede dokumenter og genereret lyd markeres som AI-genereret	At fortælle medarbejdere og andre hvordan I bruger AI
Forbudte former for AI-praksis (art. 5)	Ingen forbudte anvendelser, som for eksempel manipulation eller social bedømmelse	Platformen er bygget til at svare ud fra dokumenter og arbejde med forretningssystemer	Ikke at bruge den til forbudte formål

Hvis I bruger den til et højrisikoformål

Nogle anvendelser er højrisiko efter forordningen, for eksempel inden for rekruttering og personaleledelse, kreditvurdering eller adgang til uddannelse og væsentlige tjenester. Bruger I et AI-system til et sådant formål, gælder forpligtelserne for idriftsættere i art. 26 fra 2. december 2027, blandt andet menneskeligt tilsyn, overvågning og opbevaring af logfiler. Empisto understøtter det arbejde med svar der henviser til deres kilder, så et menneske kan gennemgå dem, med bekræftelse før et værktøj ændrer noget, med arbejdsområder der holder følsomme anvendelser adskilt, og med en auditlog som I opbevarer på jeres egne servere. Beslutningen om at bruge AI til et sådant formål og den vurdering der hører med, er fortsat jeres.

06 Fortrolighed er mere end databeskyttelse

Meget af det virksomheder vil spørge en AI-assistent om, er fortroligt uden at være personoplysninger: kontraktvilkår, priser, planer, juridisk rådgivning, kundemateriale under en fortrolighedsaftale og oplysninger omfattet af tavshedspligt. Sender I det til en ekstern AI-tjeneste, kan I komme til at bryde et løfte I allerede har givet, uanset hvordan det ser ud med databeskyttelsen. Når AI kører på jeres egne servere, bliver den slags materiale inden for den fortrolighed I allerede har lovet.

Det samme gælder branchespecifikke regler der begrænser outsourcing eller kræver kontrol med hvor data behandles. Den slags regler er almindelige inden for finans, sundhed, juridiske ydelser og den offentlige sektor. Færre eksterne parter betyder færre leverandører der skal godkendes, registreres og overvåges.

07 Cloud-AI, hvis I vælger det

Nogle teams vil måske gerne bruge en cloudmodel til opgaver der ikke er følsomme, for eksempel udkast til tekster der skal offentliggøres. Empisto tilbyder det pr. arbejdsområde og slået fra som standard: følsomme dokumenter holdes inde, personoplysninger fjernes før noget sendes, og hver forespørgsel logges. Bruger et arbejdsområde en cloudmodel, gælder GDPR-spørgsmålene i tabellen ovenfor igen for netop det arbejdsområde, og udbyderen skal med i jeres vurdering.

08 Sådan forbereder I jeres vurdering

En databeskyttelsesrådgiver eller complianceansvarlig kan gennemgå følgende punkter sammen med os. Hvert punkt indgår som regel i en konsekvensanalyse eller en leverandørgennemgang.

1. **Datastrømmene.** Hvilke biblioteker og systemer der er koblet på, hvilke teams der bruger dem, og en bekræftelse af at ingen forbindelse udadtil er slået til medmindre I har besluttet det.
2. **Adgangsmodellen.** Arbejdsområder, biblioteker og roller afstemt med jeres teams og grupperne i jeres brugerkatalog.
3. **Fortegnelse og log.** Jeres fortegnelse over behandlingsaktiviteter, auditloggen og hvor længe I vil opbevare hver type data.
4. **Mennesker.** Hvordan I informerer medarbejderne, hvordan I håndterer anmodninger fra registrerede, og hvordan I opbygger AI-færdigheder.
5. **Leverandørvilkår.** Licensen, support og den adgang vores teknikere eventuelt får brug for, med en databehandleraftale hvor jeres rådgivere vurderer at der er behov for en.

Arkitekturbeskrivelsen gør rede for hvor data gemmes og for hver forbindelse udadtil, og den er et nyttigt bilag til en sådan vurdering.

09 Læs mere

Arkitekturbeskrivelsen forklarer hvordan platformen er bygget og hvor data gemmes. Sikkerhedssiden besvarer de seks spørgsmål sikkerhedsteams stiller først. Vil I drøfte jeres vurdering med stifterne, så start her.