EmbedPolicy – Privacy by Design og Privacy by Default

Version: 0.1
Status: Foreløbig dokumentation
Dokumentejer: Beezy365 A/S

1. Formål

EmbedPolicy udvikles med henblik på at understøtte organisationers arbejde med databeskyttelse og oplysningspligt.

Dette dokument beskriver, hvordan principperne om Privacy by Design og Privacy by Default indgår i løsningens arkitektur, funktioner og videreudvikling.

Principperne følger GDPR artikel 25.

2. Privacy by Design

Privacy by Design betyder, at databeskyttelse skal indarbejdes i systemets design og udvikling.

For EmbedPolicy er følgende designvalg særligt relevante.

Kundeadskillelse

EmbedPolicy anvender særskilte databaser for de enkelte kunder.

Arkitekturen er valgt for at understøtte logisk adskillelse af oplysninger mellem organisationer.

Central administration

Virksomheds- og kontaktoplysninger kan vedligeholdes centralt og anvendes i flere privatlivspolitikker.

Dette kan reducere behovet for gentagen manuel indtastning og begrænse risikoen for uoverensstemmelser.

Versionsstyring

EmbedPolicy understøtter versionsstyring, så ændringer i privatlivspolitikker kan administreres og historiske versioner bevares.

Dette understøtter sporbarhed og kontrol med offentliggjort information.

Adgangsstyring

Løsningen anvender brugerroller og adgangsrettigheder.

Formålet er at begrænse adgangen til relevante funktioner og oplysninger efter brugerens arbejdsopgaver.

Dataminimering

EmbedPolicy er designet til administration af privatlivspolitikker og tilhørende organisatoriske oplysninger.

Løsningen er ikke beregnet til at fungere som register over konkrete borgere, patienter eller personalesager.

3. Privacy by Default

Privacy by Default betyder, at systemets standardindstillinger skal understøtte beskyttelse af personoplysninger uden at kræve unødige handlinger fra brugeren.

For EmbedPolicy omfatter dette især følgende principper.

Begrænset offentliggørelse

Oplysninger i administrationsmiljøet skal ikke automatisk være offentligt tilgængelige.

Offentliggørelse skal ske gennem systemets relevante publiceringsfunktioner.

Adgang efter behov

Brugere skal som udgangspunkt kun have adgang til de funktioner og oplysninger, der er nødvendige for deres opgaver.

Standardroller og rettighedstildeling skal verificeres i den konkrete implementering.

Begrænset indsamling

Systemets standardfunktioner skal ikke kræve flere personoplysninger end nødvendigt for den tilsigtede anvendelse.

Kontrol før publicering

Brugeren skal have mulighed for at kontrollere indholdet, inden det offentliggøres.

Det gælder også indhold, der er udarbejdet med AI-understøttelse.

4. AI og databeskyttelse

AI-understøttet indholdsproduktion kan være en hjælp ved udarbejdelse af privatlivspolitikker.

Anvendelsen kræver dog særlig opmærksomhed på, hvilke oplysninger der sendes til eksterne tjenester.

EmbedPolicy er ikke beregnet til, at brugerne indtaster følsomme eller unødvendige personoplysninger i AI-prompts.

Der arbejdes med at dokumentere dataflow, instrukser og relevante beskyttelsesforanstaltninger i forbindelse med AI-funktionaliteten.

AI-genereret indhold skal kontrolleres af kunden inden offentliggørelse.

5. Løbende udvikling

Databeskyttelse indgår som et hensyn ved udvikling af nye funktioner og ændringer i eksisterende funktionalitet.

Ved relevante ændringer skal det vurderes, om der opstår nye risici for personoplysninger eller behov for yderligere sikkerhedsforanstaltninger.

Erfaringer fra kunder, herunder offentlige organisationer, vil indgå i videreudviklingen.

6. Ansvarsfordeling

EmbedPolicy stiller funktioner til rådighed, som kan understøtte kundens arbejde med databeskyttelse.

Kunden har fortsat ansvaret for sine behandlingsaktiviteter, indholdet af privatlivspolitikkerne og overholdelsen af den relevante oplysningspligt.

Anvendelse af EmbedPolicy medfører ikke i sig selv, at en organisation opfylder alle krav i GDPR.

7. Konklusion

EmbedPolicy er udviklet med fokus på struktureret håndtering af privatlivspolitikker, kundeadskillelse, adgangsstyring, versionskontrol og central vedligeholdelse af oplysninger.

Disse designvalg kan understøtte principperne om Privacy by Design og Privacy by Default.

De konkrete standardindstillinger og sikkerhedskontroller skal dokumenteres og verificeres som led i den løbende udvikling og sikkerhedsgennemgang.

Dokumentstatus: Foreløbig dokumentation. Beskrivelsen er ikke en certificering eller garanti for, at alle krav i GDPR artikel 25 er opfyldt.