

Egenerklæring – mSystems ApS

ISO 27001 · GDPR · Databehandleraftaler

Resumé

Denne egenerklæring giver et overordnet indblik i virksomhedens arbejde med informationssikkerhed og databeskyttelse.

Virksomheden er en EU-baseret SaaS-virksomhed, der opererer som **databehandler** for sine kunder. Der er etableret et Information Security Management System (ISMS) baseret på **ISO/IEC 27001**.

Virksomheden behandler **almindelige personoplysninger samt CPR-numre** på vegne af kunder. Behandlingen sker i overensstemmelse med **GDPR**, og der er implementeret tekniske og organisatoriske sikkerhedsforanstaltninger.

Der indgås **databehandleraftaler (DBA)** med kunder i henhold til **GDPR artikel 28**, og eventuelle underdatabehandlere anvendes kontrolleret og inden for EU.

Denne erklæring er udarbejdet til brug for kunder og samarbejdspartnere som dokumentation for virksomhedens modenhed og ansvarlighed inden for informationssikkerhed og databeskyttelse.

Ledelseserklæring

Ledelsen erklærer hermed, at oplysningerne i denne egenerklæring er korrekte og retvisende på tidspunktet for underskrift.

Dato: 20-02-2026

Navn: Anja Kjeldahl Østergaard

Titel: Direktør

Underskrift:



Bilag A – Self-assessment

Modenhedsskala:

0 = Ikke etableret

1 = Delvist etableret

2 = Implementeret

3 = Implementeret og dokumenteret

ISO 27001 – Informationssikkerhed

Der foreligger en godkendt informationssikkerhedspolitik

0 1 2 3

Kommentar / forklaring:

- Vi er compliant på ISO 27001 standarden

Roller og ansvar for informationssikkerhed er defineret

0 1 2 3

Kommentar / forklaring:

Der gennemføres systematiske risikovurderinger

0 1 2 3

Kommentar / forklaring:

- Mindst 1 gang årligt eller ved større ændringer i systemer eller forretningen.

Adgangsstyring er baseret på mindst privilegie

0 1 2 3

Kommentar / forklaring:

Der findes procedure for håndtering af sikkerhedshændelser

0 1 2 3

Kommentar / forklaring:

- Disse fremgår af Anneks A.16

Leverandører og underdatabehandlere vurderes sikkerhedsmæssigt

0 1 2 3

Kommentar / forklaring:

- Ja, alle leverandører og underdatabehandlere vurderes nøje inden et samarbejde indledes. Vi modtager opdateringer, hvis en leverandørs/underdatabehandlers compliance eller DBA ændrer sig, og vi vurderer om disse ændringer betyder, at leverandøren/underdatabehandleren ikke længere kan være leverandør/underdatabehandler for os. Derudover fører vi tilsyn med dem mindst en gang årligt.

GDPR

Virksomhedens rolle som databehandler er klart defineret

0 1 2 3

Kommentar / forklaring:

Der føres fortegnelse over behandlingsaktiviteter (ROPA)

0 1 2 3

Kommentar / forklaring:

Tekniske og organisatoriske foranstaltninger er implementeret

0 1 2 3

Kommentar / forklaring:

Der findes procedure for registreredes rettigheder

0 1 2 3

Kommentar / forklaring:

Der findes en oversigt over sikkerhedshændelser, med angivelse af, om den enkelte hændelse medførte et brud på persondatasikkerheden?

0 1 2 3

Kommentar / forklaring:

- Dette fremgår af vores hændelseslog, som altid er opdateret.

Der findes procedure for brud på persondatasikkerheden

0 1 2 3

Kommentar / forklaring:

- Dette fremgår af Anneks A.16

Er der konstateret brud på persondatasikkerheden de sidste 12 måneder?

0 1 2 3

Kommentar / forklaring:

- Nej

Behandling af CPR-numre sker kontrolleret og dokumenteret

0 1 2 3

Kommentar / forklaring:

- Behandlingen af CPR Nummer er som følger:
 - Den dataansvarlige modtager kundens samtykke på behandlingen heraf, hvis ikke dette godkendes behandles CPR ikke.
 - CPR nummer maskeres ved scanning af kundens kørekort således, at CPR nummeret ikke kan ses igen.
 - CPR nummer gemmes ingen steder i databasen, med mindre dette er indtastet manuelt af medarbejderen i fx. ekstern note, intern note eller øvrige felter, der kan skrives fritekst i.

Databehandleraftaler (DBA)

Der indgås databehandleraftaler med alle kunder

0 1 2 3

Kommentar / forklaring:

- mSystems gældende standard DBA ligger tilgængelig på vores hjemmeside.
<https://msystems.dk/>

Databehandleraftaler lever op til GDPR artikel 28

0 1 2 3

Kommentar / forklaring:

Underdatabehandlere er identificeret og dokumenteret

0 1 2 3

Kommentar / forklaring:

- Disse fremgår af Bilag B i DBA

Underdatabehandlere er placeret inden for EU

0 1 2 3

Kommentar / forklaring:

- Ja

Der føres kontrol med underdatabehandlers sikkerhedsniveau

0 1 2 3

Kommentar / forklaring:

- Der føres kontrol mindst 1 gang årligt.

Der er udskiftet underdatabehandlere det seneste år

0 1 2 3

Kommentar / forklaring:

- Ja SMTP2GO og Brevo er tilføjet og erstatter Scannet's SMTP løsning. Der er ført kontrol med SMTP2GO og Brevo før implementation. SMTP2GO og Brevo fremgår af gældende DBA.
- Criipto har skiftet navn til Idura