| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Indsæt navnet på den registrerede juridiske enhed her | | | | | | | |
| Dokumentnummer:<br>PII06 | | | | | Dokumenttitel:<br>**Politik for håndtering af registreredes rettigheder** | | | | | | | |
| Version:<br>1.0 | | Ikrafttrædelsesdato:<br>01.01.2025 | | | Dokumentejer: | | | | | | | |
| X | Politik | | Standard | | Procedure | | Formular | | Register | | Andet | |

| **Revisionshistorik** | | | | |
|---|---|---|---|---|
| **Revisionsnummer** | **Revisionsdato** | **Ændringer** | **Gennemgået af** | **Procesejer** |
| | | | | |
| | | | | |

| **Godkendelser** | | | |
|---|---|---|---|
| **Navn** | **Stilling** | **Dato** | **Underskrift** |
| | | | |
| | | | |

## Tilpasset relevante standarder og regler

| Standard / regulering | Klausul / kontrol / artikel | Anvendelse | Dækningstype | Kommentar |
|---|---|---|---|---|
| ISO/IEC 27701:2025 | Clause 7.5; Clause 8.1 | Both | Primary | Dokumentation for rettighedsanmodninger og operationel kontrol |
| ISO/IEC 27701:2025 | Clause 9.1; Clause 10.2 | Both | Supporting | Overvågning, afvigelser og korrigerende handling |
| ISO/IEC 27701:2025 | Annex A.1.3.2 | Controller | Primary | Forpligtelser over for registrerede |
| ISO/IEC 27701:2025 | Annex A.1.3.6; Annex A.1.3.7 | Controller | Primary | Indsigelse, indsigt, berigtigelse og sletning |
| ISO/IEC 27701:2025 | Annex A.1.3.8; Annex A.1.3.9 | Controller | Primary | Underretning af tredjeparter og kopi af behandlede personhenførbare oplysninger (PII) |
| ISO/IEC 27701:2025 | Annex A.1.3.10; Annex A.1.3.11 | Controller | Primary | Håndtering af anmodninger og forpligtelser ved automatiseret beslutningstagning |
| ISO/IEC 27701:2025 | Annex A.1.2.9 | Controller | Supporting | Behandlingsregistre for dataansvarlig |
| ISO/IEC 27701:2025 | Annex A.2.2.2; Annex A.2.2.6; Annex A.2.2.7 | Processor | Supporting | Kundeaftale, understøttelse af forpligtelser og databehandlerregistre |
| ISO/IEC 27701:2025 | Annex A.2.3.2 | Processor | Primary | Databehandlers understøttelse af forpligtelser over for registrerede |
| ISO/IEC 27701:2025 | Annex A.3.14 | Both | Supporting | Beskyttelse af registreringer om rettighedsanmodninger |
| GDPR | Article 5(1)(a); Article 5(2) | Controller | Supporting | Gennemsigtighed og ansvarlighed |
| GDPR | Article 11; Article 12 | Controller | Primary | Identifikation, anmodningsformer, tidsfrister og styring af svar |
| GDPR | Article 15; Article 16; Article 17 | Controller | Primary | Indsigt, berigtigelse og sletning |

| | | | | |
|---|---|---|---|---|
| GDPR | Article 18; Article 19; Article 20 | Controller | Primary | Begrænsning, underretning og dataportabilitet |
| GDPR | Article 21; Article 22 | Controller | Primary | Indsigelse og automatiseret beslutningstagning |
| GDPR | Article 24 | Controller | Supporting | Dataansvarliges ansvar og foranstaltninger |
| GDPR | Article 26 | Joint Controller | Supporting | Fordeling af rettigheder mellem fælles dataansvarlige |
| GDPR | Article 28 | Both | Primary | Databehandlers bistand ved rettighedsanmodninger |
| GDPR | Article 30 | Both | Supporting | Sammenhæng med behandlingsregistre |
| GDPR | Article 32 | Both | Supporting | Sikker håndtering af rettighedsdokumentation og videregivelser |
| GDPR | Article 39 | Conditional | Supporting | DPO-rådgivning og overvågning, hvor relevant |
| ISO/IEC 29100:2020 | Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.12 | Both | Supporting | Gennemsigtighed, individuel deltagelse, ansvarlighed og efterlevelse |
| ISO/IEC 29151:2022 | Annex A.10 | Controller | Supporting | Registreredes deltagelse og indsigt |

## 1. Omfang

1.1 Denne politik fastsætter obligatoriske krav til modtagelse, validering, vurdering, opfyldelse, afslag, forlængelse, lukning, overvågning og dokumentation af anmodninger om registreredes rettigheder.

1.2 Denne politik gælder for anmodninger fra registrerede eller bemyndigede repræsentanter vedrørende indsigt, berigtigelse, sletning, begrænsning, dataportabilitet, indsigelse, automatiseret beslutningstagning, routing af tilbagetrækning af samtykke, klager og relaterede forespørgsler.

1.3 Denne politik gælder i kontekster som dataansvarlig, fælles dataansvarlig, databehandler og underdatabehandler. Forpligtelser for databehandlere og underdatabehandlere gælder kun, hvor organisationen understøtter en dataansvarlig, kunde eller opstrøms databehandler efter dokumenterede instrukser.

**1.4 Denne politik erstatter ikke:**

1.4.1 PII03 for fortegnelse over behandlingsaktiviteter og registreringer af behandlingsgrundlag;

1.4.2 PII04 for indhold og offentliggørelse af privatlivsmeddelelse;

1.4.3 PII05 for opfyldelse af samtykke og præferencer;

1.4.4 PII10 for gennemførelse af opbevaring, sletning og bortskaffelse;

1.4.5 PII11 for styring af nøjagtighed og kvalitet;

1.4.6 PII12 for livscyklusstyring af databehandlere og underdatabehandlere;

1.4.7 PII15 for håndtering af hændelser og brud.

## 2. Formål

2.1 Formålet med denne politik er at sikre, at anmodninger om registreredes rettigheder håndteres ensartet, lovligt, sikkert, inden for fastsatte tidsfrister og med revisionsklart bevismateriale.

2.2 Denne politik sikrer, at organisationen kan dokumentere ansvarlighed for modtagelse af anmodninger, identitetsverifikation, vurdering, opfyldelse, afslag, forlængelse, samarbejde med databehandlere, lukning og løbende forbedring.

## 3. Mål

**3.1 Målene med denne politik er at:**

3.1.1 Sikre ensartet modtagelse og sporing af alle anmodninger om registreredes rettigheder.

3.1.2 Verificere anmoderens identitet eller bemyndigelse før videregivelse, berigtigelse, sletning, begrænsning eller dataportabilitet.

3.1.3 Vurdere anmodninger i forhold til behandlingsregistre, rolleklassifikation, retlige forpligtelser, kontraktlige forpligtelser og teknisk gennemførlighed.

3.1.4 Opfylde gyldige anmodninger inden for dokumenterede frister.

3.1.5 Registrere bevismateriale for afslag, delvis opfyldelse, forlængelse og lukning.

3.1.6 Understøtte dataansvarliges forpligtelser, hvor organisationen handler som databehandler eller underdatabehandler.

3.1.7 Beskytte registreringer om rettighedsanmodninger og svarpakker mod uautoriseret videregivelse eller ændring.

3.1.8 Overvåge resultater for rettighedsanmodninger og iværksætte korrigerende handling, hvor det er nødvendigt.

## 4. Politikkerklæringer

**4.1 Modtagelse, logning og klassifikation**

4.1.1 [All] The Privacy Lead / PIMS Manager MUST registrere hver anmodning om registreredes rettigheder i REG06 inden for to arbejdsdage efter modtagelsen.

4.1.2 [All] The Privacy Lead / PIMS Manager MUST klassificere hver anmodningstype, anmodningskanal, anmodningsdato, identitetsreference for anmoderen, tildelt ejer, intern forfaldsdato, lovbestemt eller kontraktlig forfaldsdato og aktuel status i REG06, før vurderingen påbegyndes.

4.1.3 [Controller] The Privacy Lead / PIMS Manager MUST bekræfte modtagelsen eller give den næste krævede kommunikation til anmoderen inden for fem arbejdsdage efter modtagelsen og registrere kommunikationen i REG06.

4.1.4 [Controller] The Process Owner / Business Owner MUST knytte hver anmodning til den relevante REG02-behandlingsaktivitet, før opfyldelseshandlinger tildeles.

4.1.5 [Joint Controller] The Privacy Lead / PIMS Manager MUST identificere den fælles dataansvarlige part, der er ansvarlig for håndtering af anmodningen, i REG02, REG06 eller REG08, før den indholdsmæssige vurdering påbegyndes.

4.1.6 [Processor] The Privacy Lead / PIMS Manager MUST registrere hver kundeinstruks vedrørende en anmodning om registreredes rettigheder i REG06 og REG08, før supportaktivitet påbegyndes.

4.1.7 [Subprocessor] The Vendor / Procurement Owner MUST registrere hver opstrøms instruks vedrørende en anmodning om registreredes rettigheder i REG06 eller REG08, før supportaktivitet fra underdatabehandler påbegyndes.

4.1.8 [All] The Incident Response Coordinator MUST registrere en REG10-eskalering inden for én arbejdsdag, hvor en rettighedsanmodning indikerer en mulig hændelse eller et muligt brud vedrørende personhenførbare oplysninger (PII).

**4.2 Identitetsverifikation, omfang og vurdering**

4.2.1 [Controller] The Privacy Lead / PIMS Manager MUST verificere anmoderens identitet eller repræsentantens bemyndigelse i REG06, før personhenførbare oplysninger (PII) videregives eller en anmodet ændring foretages.

4.2.2 [Controller] The Privacy Lead / PIMS Manager MUST kun anmode om de minimale yderligere oplysninger, der er nødvendige for verifikation, og registrere anmodningen i REG06, når identitet eller bemyndigelse er utilstrækkelig.

4.2.3 [Controller] The Process Owner / Business Owner MUST identificere relevante systemer, registreringer, formål, kategorier af personhenførbare oplysninger (PII), modtagere og opbevaringsbegrænsninger fra REG02, før opfyldelsen vurderes.

4.2.4 [Controller] The Data Protection Officer / Privacy Advisor MUST gennemgå anmodninger med høj risiko samt omtvistede, uklare, overdrevne, gentagne, afviste eller delvist opfyldte anmodninger i REG06, før beslutningen kommunikeres.

4.2.5 [Controller] The System Owner / Application Owner MUST verificere, at foreslåede svarudtræk udelukker uvedkommende personhenførbare oplysninger (PII) og uautoriserede tredjepartsdata, før svarpakken frigives.

4.2.6 [Controller] The Information Security Lead MUST gennemgå metoden til levering af svar i REG06 eller REG12, før personhenførbare oplysninger (PII) i stort omfang, følsomme personhenførbare oplysninger (PII), særlige kategorier af personoplysninger eller personhenførbare oplysninger (PII) med høj risiko videregives.

4.2.7 [Controller] The Data Protection Officer / Privacy Advisor MUST gennemgå anmodninger vedrørende automatiseret beslutningstagning eller profilering i REG06 og REG04 før opfyldelse, afslag eller eskalering.

4.2.8 [Both] The Privacy Lead / PIMS Manager MUST registrere vurderingsresultatet, relevant anmodningstype, beslutning, begrundelse og næste handling i REG06 før opfyldelse eller afslag.

[ ... Afsnit 4.3–8 er ikke inkluderet i denne forhåndsvisning. Køb det fulde dokument for at få adgang til det komplette indhold. ... ]

## 9. Undtagelser

9.1.1 [All] The Process Owner / Business Owner MUST anmode om en undtagelse i REG12, før der afviges fra godkendte krav til modtagelse, verifikation, opfyldelse, svar eller lukning af rettighedsanmodninger.

9.1.2 [All] The Privacy Lead / PIMS Manager MUST godkende eller afvise hver undtagelse vedrørende rettighedshåndtering i REG12 før implementering.

9.1.3 [Controller] The Data Protection Officer / Privacy Advisor MUST gennemgå enhver undtagelse, der involverer afslag, delvis opfyldelse, usikkerhed om identitet, følsomme personhenførbare oplysninger (PII), automatiseret beslutningstagning, anmodninger vedrørende børn eller højrisikobehandling, før godkendelse.

9.1.4 [Both] The System Owner / Application Owner MUST blokere videregivelse, berigtigelse, sletning, begrænsning eller eksport, hvor en krævet undtagelse ikke er godkendt i REG12 før handlingen.

9.1.5 [All] The Privacy Lead / PIMS Manager MUST tildele en udløbsdato, ejer og kompenserende kontrol for hver godkendt undtagelse vedrørende rettighedshåndtering i REG12, før undtagelsen bliver aktiv.

## 10. Håndhævelse

10.1.1 [All] The Privacy Lead / PIMS Manager MUST registrere en afvigelse i REG12 inden for fem arbejdsdage efter identifikation af en forsinket, manglende, ufuldstændig, ikke-verificeret eller ikke-understøttet registrering af rettighedsanmodning.

10.1.2 [Controller] The System Owner / Application Owner MUST suspendere videregivelse af svar, indtil identitets-, bemyndigelses- og svarpakkekontroller er registreret i REG06.

10.1.3 [Both] The Vendor / Procurement Owner MUST eskalere manglende samarbejde fra databehandler, underdatabehandler eller tredjepart i REG08 og REG12 inden for fem arbejdsdage efter identifikation.

10.1.4 [All] Top Management MUST tildele ejerskab for korrigerende handling i REG12, når fejl i rettighedsanmodninger er systemiske, gentagne eller relevante for certificering.

10.1.5 [All] The Internal Audit / Compliance Reviewer MUST verificere lukningsbevis for rettighedsrelaterede korrigerende handlinger i REG12 inden den tildelte forfaldsdato.

10.1.6 [All] The Incident Response Coordinator MUST igangsætte REG10-gennemgang inden for én arbejdsdag, hvor en afvigelse i en rettighedsanmodning indikerer uautoriseret videregivelse, tab, ændring, utilgængelighed eller anden formodet hændelse vedrørende personhenførbare oplysninger (PII).

## 11. Gennemgang og vedligeholdelse

11.1.1 [All] The Privacy Lead / PIMS Manager MUST gennemgå denne politik årligt og registrere resultatet af gennemgangen i REG12.

11.1.2 [All] The Privacy Lead / PIMS Manager MUST gennemgå denne politik inden for 30 dage efter væsentlig ændring af lovgivning om rettighedsanmodninger, omfang af behandlingsaktivitet, rettighedsværktøjer, metode til identitetsverifikation, databehandlers servicemodel eller krav til PIMS-certificering.

11.1.3 [All] The Data Protection Officer / Privacy Advisor MUST gennemgå ændringer af betydning for databeskyttelse i denne politik i REG12 før godkendelse.

11.1.4 [All] Top Management MUST godkende væsentlige ændringer af denne politik i REG12 før offentliggørelse.

11.1.5 [All] The Privacy Lead / PIMS Manager MUST registrere kommunikation af godkendte politikændringer i REG11 inden for 30 dage efter offentliggørelse.

## 12. Relaterede politikker

12.1 Denne politik understøttes af følgende relaterede politikker:

12.2 PII01 - Politik for ledelsessystem for privatlivsinformation

12.3 PII02 - Politik for privatlivsroller, ansvar og ansvarlighed

12.4 PII03 - Politik for fortegnelse over behandling af personhenførbare oplysninger (PII) og behandlingsgrundlag

12.5 PII04 - Politik for privatlivsmeddelelse og gennemsigtighed

12.6 PII05 - Politik for samtykke- og præferencestyring

12.7 PII07 - Politik for risikovurdering vedrørende databeskyttelse og DPIA

12.8 PII08 - Politik for databeskyttelse gennem design og standardindstillinger

12.9 PII09 - Politik for indsamling, brug, videregivelse og deling af personhenførbare oplysninger (PII)

12.10 PII10 - Politik for opbevaring, sletning og bortskaffelse af personhenførbare oplysninger (PII)

12.11 PII11 - Politik for nøjagtighed og kvalitet af personhenførbare oplysninger (PII)

12.12 PII12 - Politik for privatlivsstyring af databehandlere, underdatabehandlere og tredjeparter

12.13 PII13 - Politik for international overførsel af personhenførbare oplysninger (PII)

12.14 PII14 - Politik for sikkerhed og adgangsstyring for personhenførbare oplysninger (PII)

12.15 PII15 - Politik for håndtering af hændelser og brud vedrørende personhenførbare oplysninger (PII)

12.16 PII16 - Politik for træning, bevidstgørelse og kompetence vedrørende databeskyttelse

12.17 PII17 - Politik for dokumenterede oplysninger og styring af bevismateriale i PIMS

12.18 PII18 - Politik for PIMS-overvågning, revision og forbedring

## 13. Referencestandarder og rammeværker

13.1 Denne politik er kortlagt til følgende standarder og reguleringer. Kortlægningen forklarer, hvordan politikken understøtter de nævnte krav, og identificerer de interne klausuler, der implementerer eller understøtter dem.

### 13.2 ISO/IEC 27701:2025

13.2.1 **Clause 7.5; Clause 8.1** - Kortlagt til dokumenterede registreringer af rettighedsanmodninger, operationel arbejdsgang for anmodninger, identitetsverifikation, opfyldelse, svar, lukning og bevismateriale for databehandlersupport. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.1.6; 4.2.1; 4.2.2; 4.2.3; 4.2.8; 4.3.10; 4.4.5; 7.1.1; 7.1.2; 7.1.3].

13.2.2 **Clause 9.1; Clause 10.2** - Kortlagt til metrikker for rettighedsanmodninger, overvågning af forsinkede anmodninger, revisionsstikprøver, registrering af afvigelser, korrigerende handling og verifikation af effektivitet. Addressed by clauses [4.5.6; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 8.1.6; 10.1.1; 10.1.3; 10.1.4; 10.1.5].

13.2.3 **Annex A.1.3.2** - Kortlagt til fastlæggelse og opfyldelse af forpligtelser over for registrerede gennem dokumenterede rettighedskategorier, modtagelseskanaler, verifikation, vurdering,

svar og lukningskriterier. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.2.1; 4.2.8; 4.4.1; 4.4.4; 6.1.1; 7.1.1].

13.2.4 **Annex A.1.3.6; Annex A.1.3.7** - Kortlagt til håndtering af indsigelse, indsigt, berigtigelse, sletning og begrænsning, verifikation, opfyldelse og håndtering af omtvistet nøjagtighed. Addressed by clauses [4.2.1; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.6; 4.4.6].

13.2.5 **Annex A.1.3.8; Annex A.1.3.9** - Kortlagt til underretning af tredjeparter efter rettighedsresultater og levering af kopier eller portabilitetssvarpakker. Addressed by clauses [4.3.5; 4.3.8; 4.5.5].

13.2.6 **Annex A.1.3.10; Annex A.1.3.11** - Kortlagt til dokumenteret håndtering af legitime anmodninger, frister, forlængelser, afslag, lukning og gennemgang af anmodninger vedrørende automatiseret beslutningstagning. Addressed by clauses [4.1.2; 4.2.4; 4.2.7; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5].

13.2.7 **Annex A.1.2.9** - Kortlagt til at knytte rettighedsanmodninger til behandlingsregistre, behandlingsformål, systemer, kategorier, modtagere og opbevaringsbegrænsninger. Addressed by clauses [4.1.4; 4.2.3; 4.3.8; 7.1.3].

13.2.8 **Annex A.2.2.2; Annex A.2.2.6; Annex A.2.2.7** - Kortlagt til instrukser i kundeaftaler, databehandlers understøttelse af kundens forpligtelser og databehandlerregistre for rettighedssupportaktiviteter. Addressed by clauses [4.1.6; 4.1.7; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 7.1.7].

13.2.9 **Annex A.2.3.2** - Kortlagt til databehandlers midler til at understøtte dataansvarliges forpligtelser over for registrerede, herunder support til hentning, berigtigelse, begrænsning, sletning og eksport efter dokumenteret instruks. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 7.1.7].

13.2.10 **Annex A.3.14** - Kortlagt til beskyttelse af registreringer om rettighedsanmodninger, sikker håndtering af svarpakker, kontroller af svarlevering og beskyttelse af lukningsbevis. Addressed by clauses [4.2.5; 4.2.6; 4.4.5; 4.4.7; 7.1.4; 7.1.5; 10.1.2].

**13.3 GDPR**

13.3.1 **Article 5(1)(a); Article 5(2)** - Kortlagt til gennemsigtig rettighedshåndtering, ansvarlighedsbevis, anmodningslogfiler, svarregistreringer, revisionsstikprøver og korrigerende handling. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.4.4; 4.4.5; 8.1.5; 10.1.1].

13.3.2 **Article 11; Article 12** - Kortlagt til identifikation, yderligere oplysninger hvor nødvendigt, svartid, kommunikation, forlængelse, afslag og lukning af anmodninger. Addressed by clauses [4.2.1; 4.2.2; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5].

13.3.3 **Article 15; Article 16; Article 17** - Kortlagt til søgeresultater vedrørende indsigt, berigtigelse, sletning, verifikation, bevismateriale for opfyldelse og levering af svarpakker. Addressed by clauses [4.2.1; 4.3.1; 4.3.2; 4.3.3; 4.3.5; 4.3.10].

13.3.4 **Article 18; Article 19; Article 20** - Kortlagt til begrænsning, underretning om rettighedsresultater til relevante parter og levering af portabilitet eller kopi. Addressed by clauses [4.3.4; 4.3.5; 4.3.8; 4.5.5].

13.3.5 **Article 21; Article 22** - Kortlagt til vurdering af indsigelser og gennemgang af anmodninger vedrørende automatiseret beslutningstagning eller profilering. Addressed by clauses [4.2.7; 4.3.6; 4.3.7].

13.3.6 **Article 24** - Kortlagt til dataansvarliges styringsforanstaltninger, roller, ejerskab af arbejdsgange, gennemgang, undtagelser, korrigerende handling og ledelsesmæssigt tilsyn med rettighedshåndtering. Addressed by clauses [5.1.1; 5.1.2; 6.1.1; 6.1.3; 6.1.4; 9.1.1; 9.1.2; 10.1.4; 11.1.1].

13.3.7 **Article 26** - Kortlagt til identifikation af ansvar hos fælles dataansvarlige for håndtering af anmodninger, før den indholdsmæssige vurdering påbegyndes. Addressed by clauses [4.1.5; 6.1.5].

13.3.8 **Article 28** - Kortlagt til bistand fra databehandlere og underdatabehandlere, dokumenterede kundeinstrukser, supportfrister, intet direkte svar uden autorisation og eskalering af manglende samarbejde. Addressed by clauses [4.1.6; 4.1.7; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.6; 6.1.6].

13.3.9 **Article 30** - Kortlagt til at knytte rettighedsanmodninger til behandlingsregistre, behandlingsaktiviteter, systemer, kategorier af personhenførbare oplysninger (PII), modtagere og databehandlerregistre. Addressed by clauses [4.1.4; 4.2.3; 4.3.8; 4.5.1; 7.1.3].

13.3.10 **Article 32** - Kortlagt til sikker håndtering af rettighedsanmodninger, beskyttelse af svarlevering, forebyggelse af uautoriseret videregivelse og beskyttelse af rettighedsbevismateriale. Addressed by clauses [4.2.5; 4.2.6; 7.1.4; 7.1.5; 10.1.2; 10.1.6].

13.3.11 **Article 39** - Kortlagt til rådgivning og overvågning fra Data Protection Officer / Privacy Advisor for rettighedsanmodninger med høj risiko, omtvistede, afviste, forlængede og relateret til automatiseret beslutningstagning. Addressed by clauses [4.2.4; 4.2.7; 4.3.7; 4.4.3; 6.1.3; 9.1.3; 11.1.3].

**13.4 ISO/IEC 29100:2020**

13.4.1 **Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.12** - Kortlagt til gennemsigtighed i rettighedskanaler, individuel deltagelse og indsigt, ansvarlighed, klage- og genoprejsningsprocedurer, overvågning af efterlevelse af databeskyttelseskrav og revisionsbevismateriale. Addressed by clauses [4.1.3; 4.2.1; 4.3.1; 4.3.2; 4.3.3; 4.3.8; 4.4.6; 7.1.1; 8.1.5; 10.1.1].

**13.5 ISO/IEC 29151:2022**

13.5.1 **Annex A.10** - Kortlagt til registreredes deltagelse og indsigt, identitetsverifikation, indsigt, berigtigelse, sletning, statusopdateringer, databehandlersupport og klage-/genoprejsningsmekanismer. Addressed by clauses [4.1.1; 4.2.1; 4.3.1; 4.3.2; 4.3.3; 4.4.4; 4.5.1; 4.5.4; 8.1.6].

**13.6 Interne krav**

13.6.1 Internt krav - Klausuler, der definerer REG06 som det primære bevisobjekt for rettigheder, træning, godkendelse af ikke-standardiseret arbejdsgang, udløb af undtagelser, politikgennemgang og kommunikation af politikændringer, understøtter ensartet implementering, men er ikke direkte kortlagt til en enkelt ekstern klausul. Addressed by clauses [5.1.2; 6.1.7; 7.1.6; 9.1.4; 9.1.5; 11.1.2; 11.1.4; 11.1.5].