

				Indsæt navnet på den registrerede juridiske enhed her							
Dokumentnummer: PII05				Dokumenttitel: Politik for styring af samtykke og præferencer							
Version: 1.0		Ikrafttrædelsesdato: 01.01.2025		Dokumentejer:							
X	Politik		Standard		Procedure		Formular		Register		Andet

Revisionshistorik				
Revisionsnummer	Revisionsdato	Ændringer	Gennemgået af	Procesejer

Godkendelser			
Navn	Stilling	Dato	Underskrift

Juridisk meddelelse (ophavsret og brugsbegrænsninger)
(C) 2025 Clarysec LLC. All rights reserved.

Dette dokument er Clarysec LLC's intellektuelle ejendom. Ingen del af dette dokument må kopieres, genbruges, distribueres eller ændres til kommercielle eller implementeringsmæssige formål uden udtrykkelig skriftlig tilladelse.

Uautoriseret brug er strengt forbudt og kan medføre retslige skridt.

For licensiering kontakt: info@clarysec.com

Tilpasset relevante standarder og regler

Standard / Regulation	Clause / Control / Article	Applicability	Coverage Type	Comment
ISO/IEC 27701:2025	Clause 7.5; Clause 8.1	Both	Primary	Dokumenterede oplysninger og operationel styring af dokumentation for samtykke
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Overvågning, afvigelse, korrigerende handling og forbedring
ISO/IEC 27701:2025	Annex A.1.2.3	Controller	Supporting	Sammenkobling med behandlingsgrundlag
ISO/IEC 27701:2025	Annex A.1.2.4; Annex A.1.2.5	Controller	Primary	Fastlæggelse, indhentning og registrering af samtykke
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Primary	Dataansvarliges registreringer over behandling
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.7	Processor	Supporting	Databehandleraftaler, kundens formål og databehandlerregistreringer
ISO/IEC 27701:2025	Annex A.2.3.2	Processor	Supporting	Databehandlers støtte til dataansvarliges forpligtelser over for registrerede
ISO/IEC 27701:2025	Annex A.3.14	Both	Supporting	Beskyttelse af registreringer over behandling af personhenførbare oplysninger (PII)
GDPR	Article 4(11)	Controller	Supporting	Kriterier for samtykke
GDPR	Article 5(1)(a); Article 5(2)	Controller	Supporting	Lovlighed, rimelighed, gennemsigtighed og ansvarlighed
GDPR	Article 6(1)(a); Article 6(4)	Controller	Primary	Samtykke som behandlingsgrundlag og sammenkobling ved ændret formål
GDPR	Article 7	Controller	Primary	Betingelser for samtykke og tilbagetrækning
GDPR	Article 8	Conditional	Supporting	Eskalering ved børns samtykke
GDPR	Article 9(2)(a)	Conditional	Supporting	Udtrykkeligt samtykke ved behandling af særlige kategorier af personoplysninger

GDPR	Article 24	Controller	Supporting	Dataansvarliges ansvar og foranstaltninger
GDPR	Article 28	Both	Supporting	Sammenkobling med databehandlerinstruks og bistand
GDPR	Article 30	Both	Supporting	Sammenkobling med fortegnelser over behandlingsaktiviteter
ISO/IEC 29100:2020	Clause 5.2; Clause 5.8; Clause 5.12	Both	Supporting	Principper for samtykke og valg, gennemsigtighed og efterlevelse
ISO/IEC 29151:2022	Annex A.3	Both	Supporting	Kontroller for samtykke og valg
ISO/IEC TS 27560:2023	Clause 5.2; Clause 6.2; Clause 6.3; Clause 6.4	Conditional	Supporting	Struktur for samtykkeregistrering og samtykkekvittering, hvor de anvendes

1. Omfang

- 1.1 Denne politik fastsætter obligatoriske krav til at afgøre, hvornår samtykke kræves, anmode om samtykke, indsamle dokumentation for samtykke, styre præferencer, behandle tilbagetrækninger, vedligeholde samtykkeregistreringer og gennemgå samtykkemekanismer.
- 1.2 Denne politik gælder for behandling af personhenførbare oplysninger (PII), hvor samtykke vælges eller kræves som behandlingsgrundlag, hvor udtrykkeligt samtykke kræves, hvor samtykkepræferencer indsamles, eller hvor organisationen administrerer samtykkeregistreringer på vegne af en dataansvarlig.
- 1.3 Denne politik gælder i sammenhænge med dataansvarlig, fælles dataansvarlig, databehandler og underdatabehandler.
- 1.4 Forpligtelser for databehandler og underdatabehandler gælder kun, hvor samtykkeregistreringer, præferencestatuser eller instrukser om tilbagetrækning af samtykke administreres efter dokumenterede instrukser fra en dataansvarlig eller kunde.
- 1.5 Denne politik gør ikke samtykke til standardbehandlingsgrundlaget for behandling af personhenførbare oplysninger (PII).
- 1.6 Fastlæggelse af behandlingsgrundlag er fortsat reguleret af PII03 - Politik for fortegnelse over behandling af personhenførbare oplysninger (PII) og behandlingsgrundlag.

2. Formål

- 2.1 Formålet med denne politik er at sikre, at styring af samtykke og præferencer er lovlig, gennemsigtig, dokumenterbar, kan tilbagekaldes, kan håndhæves teknisk og understøttes af kontrolleret bevismateriale.
- 2.2 Denne politik sikrer, at der kun anmodes om samtykke, hvor det er relevant, at samtykkeregistreringer er fuldstændige og sporbare, at tilbagetrækninger respekteres, og at dokumentation for samtykke fortsat er tilgængelig til revision, forespørgsler og ansvarlighedsformål.

3. Mål

3.1 Målene med denne politik er at:

- 3.1.1 Sikre, at samtykke kun anvendes, når det er det relevante behandlingsgrundlag, eller når det kræves for behandlingsaktiviteten.
- 3.1.2 Sikre, at anmodninger om samtykke er specifikke, informerede, adskilte og knyttet til den relevante privatlivsmeddelelse.
- 3.1.3 Sikre, at samtykke- og præferenceregistreringer indsamles og vedligeholdes i REG05.
- 3.1.4 Sikre, at tilbagetrækning og ændringer af præferencer effektueres inden for fastsatte driftsmæssige frister.
- 3.1.5 Sikre, at samtykkeregistreringer er knyttet til behandlingsformål i REG02 og versioner af privatlivsmeddelelser i REG07.
- 3.1.6 Sikre, at databehandleres og underdatabehandleres aktiviteter til støtte for samtykke følger dokumenterede instrukser fra dataansvarlig eller kunde.
- 3.1.7 Sikre, at samtykkemekanismer overvåges, gennemgås, korrigeres og kan revideres.

4. Politikerkklæringer

4.1 Samtykkets anvendelighed og behandlingsgrundlag

- 4.1.1 [Controller] Process Owner / Business Owner SKAL registrere i REG02, om samtykke kræves eller er valgt, før enhver ny eller væsentligt ændret behandlingsaktivitet vedrørende personhenførbare oplysninger (PII), der bygger på samtykke, påbegyndes.

- 4.1.2 [Controller] Privacy Lead / PIMS Manager SKAL verificere i REG02 og REG05, at samtykke ikke er valgt som standardbehandlingsgrundlag, før en ny eller væsentligt ændret samtykkebaseret behandlingsaktivitet godkendes.
- 4.1.3 [Controller] Data Protection Officer / Privacy Advisor SKAL gennemgå samtykkegrundlaget i REG04 før idriftsættelse, hvor behandlingen omfatter særlige kategorier af personoplysninger, tjenester rettet mod børn, højrisikobehandling eller en ubalance mellem organisationen og den registrerede.
- 4.1.4 [Joint Controller] Privacy Lead / PIMS Manager SKAL dokumentere den part, der er ansvarlig for at indhente, registrere, forny og respektere samtykke, i REG02 og REG05, før behandling som fælles dataansvarlig påbegyndes.
- 4.1.5 [Processor] Privacy Lead / PIMS Manager SKAL registrere kundeinstrukser for indsamling af samtykke, præferencestyling eller støtte til tilbagetrækning i REG08 og REG05, før en samtykkemekanisme implementeres på vegne af en dataansvarlig.
- 4.1.6 [Subprocessor] Vendor / Procurement Owner SKAL registrere samtykkerelaterede forpligtelser for underdatabehandlere i REG08, før en underdatabehandler får tilladelse til at håndtere samtykkeregistreringer, præferencestatusser eller instrukser om tilbagetrækning af samtykke.

4.2 Anmodning om og indsamling af samtykke

- 4.2.1 [Controller] Process Owner / Business Owner SKAL sikre, at hver anmodning om samtykke er formålsspecifik og knyttet til den relevante version af REG07-privatlivsmeddelelsen, før anmodningen om samtykke præsenteres for en registreret.
- 4.2.2 [Controller] System Owner / Application Owner SKAL konfigurere samtykkemekanismer, så de kræver en bekræftende handling, før behandling påbegyndes, hvor udtrykkeligt samtykke eller opt-in-samtykke kræves.
- 4.2.3 [Controller] Process Owner / Business Owner SKAL registrere reference til den registrerede, formål, kategori af personhenførbare oplysninger (PII), samtykkeordlyd eller -version, version af privatlivsmeddelelse, indsamlingskanal, tidsstempel, metode, status og relevant gyldighedsperiode i REG05, når samtykke indsamles.
- 4.2.4 [Conditional] Privacy Lead / PIMS Manager SKAL registrere logik for alderssikring eller autorisation i REG05 og udløse REG04-gennemgang før idriftsættelse, hvor samtykket vedrører behandling rettet mod børn.
- 4.2.5 [Conditional] Privacy Lead / PIMS Manager SKAL markere samtykke som udtrykkeligt i REG05, før behandling påbegyndes, hvor udtrykkeligt samtykke kræves for det valgte formål.
- 4.2.6 [Both] System Owner / Application Owner SKAL forhindre behandling, der bygger på samtykke, i at fortsætte, før REG05 viser en aktiv samtykkestatus for det relevante formål.

[... 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] Process Owner / Business Owner SKAL anmode om en undtagelse i REG12, før der afviges fra et godkendt krav til indsamling af samtykke, præferencestyling, tilbagetrækning eller bevismateriale.
- 9.1.2 [All] Privacy Lead / PIMS Manager SKAL godkende eller afvise hver samtykkerelateret undtagelse i REG12 før implementering og tildele en udløbsdato og en kompenserende kontrol for enhver godkendt undtagelse.

- 9.1.3 [Conditional] Data Protection Officer / Privacy Advisor SKAL gennemgå undtagelsen i REG04 eller REG12 før godkendelse, hvor undtagelsen omfatter udtrykkeligt samtykke, behandling rettet mod børn, højrisikobehandling eller en mekanisme til tilbagetrækning.
- 9.1.4 [Both] System Owner / Application Owner SKAL blokere frigivelse til produktionsmiljøet eller deaktivere den berørte samtykkemekanisme, når en undtagelse, der kræves efter denne politik, ikke er godkendt i REG12 før idriftsættelse.

10. Håndhævelse

- 10.1.1 [All] Privacy Lead / PIMS Manager SKAL registrere en samtykkerelateret afvigelse i REG12 inden for fem arbejdsdage efter identifikation af manglende, ugyldig, ikke-tilknyttet eller upålidelig dokumentation for samtykke.
- 10.1.2 [Controller] Process Owner / Business Owner SKAL suspendere eller afhjælpe behandling for det berørte formål, før yderligere samtykkebaseret behandling fortsætter, hvor samtykke kræves, men ikke kan dokumenteres i REG05.
- 10.1.3 [Both] System Owner / Application Owner SKAL deaktivere eller korrigere en ikke-overensstemmende mekanisme til indsamling af samtykke, præferencer eller tilbagetrækning inden for den frist, der er tildelt i REG12.
- 10.1.4 [Processor] Vendor / Procurement Owner SKAL eskalere fejl i kundeinstrukser, der omfatter samtykkeregistreringer, præferencestatuser eller støtte til tilbagetrækning, i REG08 og REG12 inden for fem arbejdsdage efter identifikation.
- 10.1.5 [All] Internal Audit / Compliance Reviewer SKAL verificere lukningsbevis for samtykkerelaterede korrigerende handlinger i REG12 senest på den tildelte forfaldsdato.

11. Gennemgang og vedligeholdelse

- 11.1.1 [All] Privacy Lead / PIMS Manager SKAL gennemgå denne politik årligt og registrere resultatet af gennemgangen i REG12.
- 11.1.2 [All] Privacy Lead / PIMS Manager SKAL gennemgå denne politik inden for 30 dage efter en væsentlig ændring i samtykkelovgivning, samtykketeknologi, værktøjer til præferencestyring, struktur for privatlivsmeddelelser eller krav til PIMS-certificering.
- 11.1.3 [All] Data Protection Officer / Privacy Advisor SKAL gennemgå privatlivsmæssigt væsentlige ændringer af denne politik i REG12 før godkendelse.
- 11.1.4 [All] Top Management SKAL godkende væsentlige ændringer af denne politik i REG12 før offentliggørelse.
- 11.1.5 [All] Privacy Lead / PIMS Manager SKAL 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 styringssystem for databeskyttelse
- 12.3 PII02 - Politik for roller, ansvar og ansvarlighed vedrørende databeskyttelse
- 12.4 PII03 - Politik for fortegnelse over behandling af personhenførbare oplysninger (PII) og behandlingsgrundlag
- 12.5 PII04 - Politik for privatlivsmeddelelse og gennemsigtighed
- 12.6 PII06 - Politik for styring af registreredes rettigheder
- 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 PII14 - Politik for sikkerhed og adgangsstyring for personhenførbare oplysninger (PII)
- 12.14 PII16 - Politik for databeskyttelsestræning, bevidstgørelse og kompetence
- 12.15 PII17 - Politik for PIMS-dokumenterede oplysninger og styring af bevismateriale
- 12.16 PII18 - Politik for PIMS-overvågning, revision og forbedring

13. Referencestandarder og rammeværker

- 13.1 Denne politik er mappet til følgende standarder og regler. Mappingen forklarer, hvordan politikken understøtter de citerede 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** - Mappet til dokumenterede oplysninger og operationel styring ved fastlæggelse af samtykkets anvendelighed, indsamling af dokumentation for samtykke, håndtering af tilbagetrækning, versionering af samtykkeregistreringer, test af mekanismer og vedligeholdelse af REG05. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.2.3; 4.2.6; 4.3.1; 4.3.2; 4.3.3; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.5.2; 4.5.3; 4.5.4; 7.1.1; 7.1.2; 7.1.3; 7.1.6].
- 13.2.2 **Clause 9.1; Clause 10.2** - Mappet til overvågning af samtykke, metrikker, revisionsstikprøver, registrering af afvigelser, korrigerende handling og verifikation af effektivitet. Addressed by clauses [4.5.5; 6.1.3; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 10.1.1; 10.1.2; 10.1.3; 10.1.4; 10.1.5].
- 13.2.3 **Annex A.1.2.3** - Mappet til bekræftelse af, hvornår samtykke er et relevant behandlingsgrundlag, og til at knytte samtykkeregistreringer til REG02-registreringer af behandlingsgrundlag. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.4.2; 4.5.3].
- 13.2.4 **Annex A.1.2.4; Annex A.1.2.5** - Mappet til at fastlægge, hvornår og hvordan samtykke indhentes, indsamle samtykke, registrere bevis, håndtere udtrykkeligt samtykke, tilbagetrækning, fornyelse og samtykkestatus. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.2.6; 4.3.1; 4.3.2; 4.3.3; 4.3.6; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5].
- 13.2.5 **Annex A.1.2.9** - Mappet til dataansvarliges registreringer for samtykkebaseret behandling, samtykkehistorik, sammenkobling med meddelelser, opbevaring af bevismateriale og revisionsklare samtykkeregistreringer. Addressed by clauses [4.2.3; 4.3.6; 4.5.1; 4.5.3; 7.1.1; 8.1.1; 8.1.3].
- 13.2.6 **Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.7** - Mappet til databehandlers kundeaftaler, overensstemmelse med kundens formål og instrukser samt databehandlerregistreringer, hvor tjenester til samtykke støtte udføres for en dataansvarlig. Addressed by clauses [4.1.5; 4.1.6; 4.3.4; 4.3.5; 4.5.4; 6.1.4; 7.1.4; 8.1.4; 10.1.4].
- 13.2.7 **Annex A.2.3.2** - Mappet til databehandlers støtte til dataansvarliges forpligtelser over for registrerede, hvor tilbagetrækning af samtykke, ændringer af præferencer eller dokumentation for samtykke håndteres efter kundeinstruks. Addressed by clauses [4.3.4; 4.3.5; 4.5.4; 6.1.4; 8.1.4].
- 13.2.8 **Annex A.3.14** - Mappet til beskyttelse af samtykke- og præferenceregistreringer mod uautoriseret ændring og til bevarelse af revisionssporbevis. Addressed by clauses [4.5.2; 5.1.6; 7.1.2; 10.1.5].

13.3 GDPR

- 13.3.1 **Article 4(11)** - Mappet til samtykkekriterier, der kræver, at samtykke er specifikt, informeret, bekræftende hvor krævet og knyttet til det relevante formål og den relevante version af meddelelsen. Addressed by clauses [4.1.2; 4.2.1; 4.2.2; 4.2.3; 4.2.5].
- 13.3.2 **Article 5(1)(a); Article 5(2)** - Mappet til lovlighed, rimelighed, gennemsigtighed, ansvarlighedsbevis, revisionsstikprøver, korrigerende handling og bevis for samtykkebaseret behandling. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.2.3; 4.5.3; 4.5.5; 8.1.1; 8.1.5; 10.1.1; 10.1.5].
- 13.3.3 **Article 6(1)(a); Article 6(4)** - Mappet til samtykke som behandlingsgrundlag for specifikke formål og til revurdering eller fornyet samtykke, hvor formål eller behandlingsbetingelser ændres væsentligt. Addressed by clauses [4.1.1; 4.1.2; 4.4.1; 4.4.2; 4.5.3].
- 13.3.4 **Article 7** - Mappet til dokumenterbarhed, adskilte anmodninger om samtykke, tilbagetrækning, let adgang til tilbagetrækning, samtykkets gyldighed og bevaret samtykkehistorik. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.3.1; 4.3.2; 4.3.3; 4.3.6; 4.4.4; 4.4.5; 10.1.2].
- 13.3.5 **Article 8** - Mappet til eskalering ved samtykke i tjenester rettet mod børn, logik for alderssikring eller autorisation og gennemgang af privatlivsrisiko før idriftsættelse. Addressed by clauses [4.1.3; 4.2.4; 9.1.3].
- 13.3.6 **Article 9(2)(a)** - Mappet til håndtering af udtrykkeligt samtykke, hvor udtrykkeligt samtykke vælges for behandling af særlige kategorier af personoplysninger. Addressed by clauses [4.1.3; 4.2.5; 9.1.3].
- 13.3.7 **Article 24** - Mappet til styringsforanstaltninger for dataansvarlige, gennemgang, godkendelse, undtagelser, korrigerende handling og ledelsestilsyn med samtykkekontroller. Addressed by clauses [5.1.1; 5.1.2; 6.1.1; 6.1.2; 6.1.3; 9.1.1; 9.1.2; 11.1.1; 11.1.4].
- 13.3.8 **Article 28** - Mappet til håndtering af databehandlerinstrukser, dokumentation for samtykkestøtte, støtte til tilbagetrækning, underdatabehandlerforpligtelser og eskalering af kundeinstrukser. Addressed by clauses [4.1.5; 4.1.6; 4.3.4; 4.3.5; 4.5.4; 6.1.4; 7.1.4; 10.1.4].
- 13.3.9 **Article 30** - Mappet til sammenkobling af samtykkeregistreringer med behandlingsformål, dataansvarliges registreringer, støtteregistreringer for databehandlere og REG02/REG05-sporbarhed. Addressed by clauses [4.1.1; 4.5.3; 4.5.4; 7.1.1; 8.1.1].

13.4 ISO/IEC 29100:2020

- 13.4.1 **Clause 5.2; Clause 5.8; Clause 5.12** - Mappet til samtykke og valg, gennemsigtighed og sammenkobling med meddelelser, tilbagetrækning, ansvarlighed og bevismateriale for efterlevelse af databeskyttelse. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.3.1; 4.3.2; 4.3.3; 4.5.3; 4.5.5; 8.1.1; 10.1.1].

13.5 ISO/IEC 29151:2022

- 13.5.1 **Annex A.3** - Mappet til kontroller for samtykke og valg, der kræver meningsfuldt, informeret og utvetydigt samtykke, ændring af præferencer og rettidige behandlingsændringer efter ændring eller tilbagetrækning af samtykke. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.3.1; 4.3.2; 4.3.3; 4.4.5].

13.6 ISO/IEC TS 27560:2023

- 13.6.1 **Clause 5.2; Clause 6.2; Clause 6.3; Clause 6.4** - Mappet til begreber for samtykkeregistrering og samtykkekvittering, registrering af samtykke, struktur for samtykkeregistrering, samtykkestatus, sammenkobling med version af meddelelse, kvitteringsstruktur og fortolkning af samtykkekvittering, hvor sådanne registreringer eller kvitteringer anvendes. Addressed by clauses [4.2.3; 4.3.2; 4.3.6; 4.4.3; 4.4.4; 4.5.2; 4.5.3; 7.1.6].

13.7 Internal Requirements

13.7.1 Internal requirement - Klausuler, der definerer REG05 som det autoritative bevisobjekt, godkendelse af ikke-standardiseret bevismateriale, blokering af driftsmæssig frigivelse, træning, vedligeholdelse af politik og kommunikation, understøtter ensartet implementering, men er ikke direkte mappet til en enkelt ekstern klausul. Addressed by clauses [4.5.1; 5.1.2; 7.1.5; 9.1.4; 11.1.2; 11.1.3; 11.1.5].