

				Indsæt navnet på den registrerede juridiske enhed her							
Dokumentnummer: PII21				Dokumenttitel: <b>Politik for databeskyttelse ved AI og automatiseret beslutningstagning</b>							
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

<p><b>Juridisk meddelelse (ophavsret og brugsbegrænsninger)</b>  (C) 2025 Clarysec LLC. All rights reserved.</p> <p>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.</p> <p>Uautoriseret brug er strengt forbudt og kan medføre retslige skridt.</p> <p>For licensiering kontakt: <a href="mailto:info@clarysec.com">info@clarysec.com</a></p>
--

## 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 bevismateriale for behandling vedrørende AI, profilering og automatiseret beslutningstagning
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Overvågning, afvigelser og korrigerende handlinger for databeskyttelseskontroller vedrørende AI
ISO/IEC 27701:2025	Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.9	Controller	Primary	Formål, behandlingsgrundlag, konsekvensanalyse vedrørende databeskyttelse og registreringer hos den dataansvarlige
ISO/IEC 27701:2025	Annex A.1.2.7; Annex A.1.2.8	Controller	Supporting	Databehandleraftaler og fælles dataansvarliges ansvar for AI-relateret behandling af PII
ISO/IEC 27701:2025	Annex A.1.3.2; Annex A.1.3.3; Annex A.1.3.4	Controller	Primary	Forpligtelser over for registrerede og gennemsigtighed ved AI-relateret behandling
ISO/IEC 27701:2025	Annex A.1.3.6; Annex A.1.3.7; Annex A.1.3.10; Annex A.1.3.11	Controller	Primary	Indsigelse, indsigt, berigtigelse, sletning, håndtering af anmodninger og forpligtelser ved automatiseret beslutningstagning
ISO/IEC 27701:2025	Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5	Controller	Primary	Begrænsninger for indsamling, behandling og minimering af AI-input, output og afledte data
ISO/IEC 27701:2025	Annex A.1.5.2; Annex A.1.5.3; Annex A.1.5.4; Annex A.1.5.5	Conditional	Supporting	Routing af internationale overførsler, videregivelse og anmodninger om videregivelse vedrørende AI-relateret PII

ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.6; Annex A.2.2.7	Processor	Primary	Databehandleraftale, dokumenterede instrukser, understøttelse af kundens forpligtelser og registreringer
ISO/IEC 27701:2025	Annex A.2.3.2; Annex A.2.5.2; Annex A.2.5.3; Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6	Processor	Supporting	Databehandlers understøttelse af forpligtelser over for registrerede, routing af overførsler og håndtering af videregivelse
ISO/IEC 27701:2025	Annex A.3.14; Annex A.3.25	Both	Supporting	Beskyttelse af registreringer og logning vedrørende AI-relateret behandling af PII
GDPR	Article 4(4); Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(1)(d); Article 5(2)	Controller	Primary	Profiling, rimelighed, gennemsigtighed, formålsbegrænsning, minimering, nøjagtighed og ansvarlighed
GDPR	Article 6; Article 9; Article 10	Controller	Primary	Lovlighed, særlige kategorier af oplysninger og sikkerhedsforanstaltninger for oplysninger om straffedømte og lovovertrædelser
GDPR	Article 12; Article 13; Article 14; Article 15	Controller	Primary	Gennemsigtige oplysninger, indsigt og meningsfulde oplysninger om automatiseret beslutningstagning
GDPR	Article 16; Article 17; Article 18; Article 21; Article 22	Controller	Primary	Berigtigelse, sletning, begrænsning, indsigelse og rettigheder ved automatiseret beslutningstagning
GDPR	Article 24; Article 25; Article 26; Article 28; Article 30; Article 32; Article 35; Article 39	Both	Supporting	Den dataansvarliges ansvar, databeskyttelse gennem design og standardindstillinger, fælles dataansvarlige, databehandlere, fortegnelser, sikkerhed, DPIA og DPO-opgaver
GDPR	Article 44	Conditional	Referenced	Routing af internationale overførsler ved AI-relateret behandling af PII

ISO/IEC 29100:2020	Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6; Clause 5.7	Both	Primary	Principper for formål, indsamling, minimering, brug, opbevaring, videregivelse, nøjagtighed og kvalitet
ISO/IEC 29100:2020	Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.11; Clause 5.12	Both	Supporting	Gennemsigtighed, individuel deltagelse, ansvarlighed, informationsikkerhed og efterlevelse af databeskyttelse
ISO/IEC 29134:2020	Clause 5.1; Clause 6.2; Clause 6.3	Both	Supporting	PIA-nytte, tærskelvurdering og forberedelse til AI- relateret vurdering af privatlivrisici
ISO/IEC 29151:2022	Annex A.4; Annex A.5; Annex A.7; Annex A.8; Annex A.10	Both	Supporting	Kontroller for formål, indsamling, minimering, brug, opbevaring, videregivelse, nøjagtighed og registreredes deltagelse

## 1. Omfang

1.1 Denne politik fastlægger obligatoriske databeskyttelseskrav for behandlingsaktiviteter vedrørende kunstig intelligens, profilering, scoring, anbefalinger, beslutningsstøtte og automatiseret beslutningstagning, som anvender, udleder, genererer, videregiver eller på anden måde behandler PII inden for PIMS-omfang.

### 1.2 Denne politik gælder for følgende:

1.2.1 AI-understøttede systemer, applikationer, modeller, tjenester, arbejdsgange, beslutningsmotorer, scoringsværktøjer, anbefalingssystemer, analysemodeller og processer for automatiseret beslutningstagning, der behandler PII;

1.2.2 profilering, segmentering, klassifikation, forudsigelse, inferens, personalisering, rangordning, egnethedsvurdering, svigdetektion, risikoscore, adgangsbeslutninger, ansættelsesrelateret vurdering, børnerelateret profilering, markedsføringspersonalisering og lignende behandling, hvor PII indgår;

1.2.3 AI-relateret PII, der anvendes til træning, test, validering, finjustering, overvågning, inferens i produktion, gennemgang af output, måling af performance, undersøgelse af hændelser eller udfasning af modeller;

1.2.4 kontekster med dataansvarlig, fælles dataansvarlig, databehandler og underdatabehandler;

1.2.5 AI-relaterede leverandører, databehandlere, underdatabehandlere, modtagere i datadelingsordninger og internationale overførselsruter, der behandler PII.

1.3 Denne politik etablerer ikke en fuldstændig styringsramme for AI, et AI-ledelsessystem, en AI-fortegnelse, en modelfortegnelse, et modelrisikoregister, et fairness-register, et algoritmeregister, et AI-hændelsesregister, en AI-komité, en rolle som modelejer, en rolle som AI-systemejer, en arbejdsgang for juridisk rådgivning eller en særskilt AI-godkendelsesformular.

### 1.4 Denne politik erstatter ikke følgende:

1.4.1 PII03 for fortegnelse over behandlingsaktiviteter, behandlingsgrundlag og ejerskab af ROPA;

1.4.2 PII04 for styring af privatlivsmeddelelser;

1.4.3 PII05 for styring af samtykke og præferencestyring;

1.4.4 PII06 for arbejdsgang vedrørende registreredes rettigheder;

1.4.5 PII07 for risikovurdering vedrørende databeskyttelse og DPIA-metodik;

1.4.6 PII08 for kontrolporte vedrørende databeskyttelse gennem design og standardindstillinger;

1.4.7 PII09 for kontroller vedrørende indsamling, brug, videregivelse og deling;

1.4.8 PII10 for gennemførelse af opbevaring, sletning og bortskaffelse;

1.4.9 PII11 for kontroller vedrørende nøjagtighed og kvalitet;

1.4.10 PII12 for livscyklusstyring af databehandlere, underdatabehandlere og tredjeparter;

1.4.11 PII13 for kontroller vedrørende internationale overførsler;

1.4.12 PII14 for sikkerhed og adgangsstyring;

1.4.13 PII15 for håndtering af hændelser og brud;

1.4.14 PII18 for overvågning, revision og forbedring;

1.4.15 PII19 for medarbejderes privatliv;

1.4.16 PII20 for børns privatliv;

1.4.17 PII22 for privatliv ved markedsføring og cookies.

## 2. Formål

- 2.1 Formålet med denne politik er at sikre, at aktiviteter med AI, profilering og automatiseret beslutningstagning, der involverer PII, identificeres, dokumenteres, risikovurderes, er gennemsigtige, kan bestrides, overvåges og styres gennem PIMS uden at skabe overlappende AI-specifikke styringsartefakter.
- 2.2 Denne politik sikrer, at databeskyttelsesforpligtelser for AI-relateret behandling af PII kan dokumenteres gennem REG02, REG04, REG06, REG07, REG08, REG09, REG10 og REG12.

### **3. Mål**

#### **3.1 Målene for denne politik er at:**

- 3.1.1 identificere behandling med AI, profilering og automatiseret beslutningstagning, der involverer PII, i REG02;
- 3.1.2 dokumentere AI-relaterede formål, behandlingsgrundlag, PII-kategorier, datakilder, udledte data, output, modtagere og beslutningseffekter i REG02;
- 3.1.3 udløse screening af risici vedrørende databeskyttelse og DPIA-routing gennem REG04;
- 3.1.4 sikre, at AI-relaterede privatlivsmeddelelser og meningsfulde oplysninger registreres i REG07;
- 3.1.5 route rettighedsanmodninger, indsigelser, menneskelig gennemgang og mulighed for at bestride afgørelsen gennem REG06;
- 3.1.6 styre AI-relaterede databehandlere, underdatabehandlere, leverandører og datadelingsordninger gennem REG08;
- 3.1.7 route AI-relaterede internationale overførsler gennem REG09;
- 3.1.8 eskalere mistanke om AI-relaterede PII-hændelser, misbrug, uautoriseret videregivelse og negative databeskyttelsesresultater gennem REG10 og REG12;
- 3.1.9 registrere overvågning, undtagelser, afvigelser, korrigerende handlinger og forbedringer i REG12.

### **4. Politikkerklæringer**

#### **4.1 Identifikation af AI, profilering og automatiseret beslutningstagning**

- 4.1.1 [Controller] Når et nyt eller væsentligt ændret system, en applikation, model, arbejdsgang, tjeneste eller forretningsproces foreslås, skal Process Owner / Business Owner afgøre, om den anvender AI, profilering, scoring, anbefalinger, beslutningsstøtte eller automatiseret beslutningstagning, der involverer PII, og registrere afgørelsen i REG02.
- 4.1.2 [Controller] Før AI-relateret behandling af PII påbegyndes, skal Process Owner / Business Owner dokumentere behandlingsformål, PII-kategorier, kategorier af registrerede, datakilder, kategorier af udledte eller afledte data, outputkategorier, modtagerkategorier, behandlingsgrundlag og kobling til opbevaringsplan i REG02.
- 4.1.3 [Controller] Før profilering, scoring, anbefalinger, beslutningsstøtte eller automatiseret beslutningstagning anvendes i produktion, skal Process Owner / Business Owner dokumentere beslutningskonteksten, den forventede effekt på registrerede, menneskelig involvering og rettighedsrute i REG02 og REG04.
- 4.1.4 [Joint Controller] Før AI-relateret behandling af PII udføres sammen med en fælles dataansvarlig, skal Privacy Lead / PIMS Manager dokumentere ansvaret for fastlæggelse af formål, privatlivsmeddelelse, håndtering af rettigheder, DPIA-understøttelse, databehandlerstyring og eskalering af hændelser i REG08.
- 4.1.5 [Processor] Før PII behandles gennem en AI-relateret tjeneste for en kunde, skal Process Owner / Business Owner bekræfte, at kundens instrukser, tilladte formål, forbudte anvendelser, håndtering af output og bistandsforpligtelser er dokumenteret i REG08.

- 4.1.6 [Both] Før AI-relateret behandling af PII aktiveres, skal Privacy Lead / PIMS Manager bekræfte, at behandlingen er knyttet til de relevante kanoniske bevisobjekter, og at der ikke oprettes et særskilt AI-specifikt register uden for REG02, REG04, REG06, REG07, REG08, REG09, REG10 eller REG12.

## 4.2 Risikovurdering vedrørende databeskyttelse og DPIA-routing

- 4.2.1 [Controller] Før AI-relateret behandling af PII lanceres eller ændres væsentligt, skal Privacy Lead / PIMS Manager gennemføre screening af risici vedrørende databeskyttelse og registrere DPIA-beslutningen i REG04.
- 4.2.2 [Conditional] Når AI-relateret behandling involverer profilering, automatiserede beslutninger, evaluering i stor skala, særlige kategorier af oplysninger, oplysninger om straffedomme og lovovertrædelser, sårbare registrerede, medarbejdervurdering, børn, adfærdsovervågning, lokationsdata, biometriske data, scoring med stor betydning eller væsentlige virkninger, skal Data Protection Officer / Privacy Advisor gennemgå privatlivsrisikoen og registrere rådgivning i REG04.
- 4.2.3 [Controller] Før idriftsættelse i produktionsmiljøet for AI-relateret behandling af PII skal Process Owner / Business Owner dokumentere risikobehandlingshandlinger, status for restrisiko og bevismateriale for klarhed til idriftsættelse i REG04 eller REG12.
- 4.2.4 [Controller] Før PII genbruges til AI-træning, test, validering, finjustering, overvågning eller modelforbedring til et nyt eller væsentligt ændret formål, skal Process Owner / Business Owner gennemføre en databeskyttelsesgennemgang og registrere beslutningen i REG02 og REG04.
- 4.2.5 [Conditional] Når restrisiko vedrørende databeskyttelse fortsat er høj efter planlagt behandling, skal Top Management godkende, afvise eller kræve yderligere behandling før brug i produktion og registrere beslutningen i REG04 og REG12.

[ ... 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 [All] Før der afviges fra et AI-relateret databeskyttelseskrav i denne politik, skal den anmodende Process Owner / Business Owner indsende en begrundelse for undtagelsen og bevismateriale for kompenserende kontroller i REG12.
- 9.2 [Conditional] Når en undtagelse påvirker profilering, automatiseret beslutningstagning, menneskelig gennemgang, mulighed for at bestride afgørelsen, gennemsigtighed, DPIA-resultat, scoring med stor betydning, børnerelateret behandling, medarbejderrelateret behandling, databehandlerbegrænsninger eller internationale overførsler, skal Data Protection Officer / Privacy Advisor gennemgå undtagelsen og registrere rådgivning i REG04 eller REG12.
- 9.3 [Conditional] Når en undtagelse skaber eller opretholder høj restrisiko vedrørende databeskyttelse, skal Top Management godkende eller afvise undtagelsen og registrere beslutningen i REG04 og REG12.
- 9.4 [All] Før en godkendt AI-relateret databeskyttelsesundtagelse udløber, skal Privacy Lead / PIMS Manager gennemgå status for lukning, fornyelse eller korrigerende handling og registrere resultatet i REG12.

## 10. Håndhævelse

- 10.1 [All] Når manglende overholdelse af denne politik identificeres, skal Privacy Lead / PIMS Manager registrere afvigelsen og den korrigerende handling i REG12.
- 10.2 [Both] Når der er mistanke om uautoriseret AI-relateret behandling af PII, videregivelse, adgang, modelmisbrug, svigt i rettighedshåndtering eller negativt databeskyttelsesresultat, skal

Incident Response Coordinator indlede hændelseseskalering og registrere bevismateriale i REG10 og REG12.

10.3 [Both] Når en databehandler, underdatabehandler, leverandør eller modtager i en datadelingsordning ikke opfylder AI-relaterede databeskyttelsesforpligtelser, skal Vendor / Procurement Owner registrere afhjælpning, eskalering eller opsigelseshandling i REG08 og REG12.

10.4 [All] Når gentagne eller systemiske AI-relaterede privatlivsafvigelser forekommer, skal Top Management gennemgå forholdet og registrere ledelseshandlingen i REG12.

## 11. Gennemgang og vedligeholdelse

11.1 [All] Mindst årligt skal Privacy Lead / PIMS Manager gennemgå denne politik for fortsat egnethed og registrere resultatet af gennemgangen i REG12.

11.2 [Conditional] Når love, tjenester, modeller, datakilder, profileringspraksisser, logik for automatiseret beslutningstagning, leverandørordninger, overførselsruter eller privatlivsrisici ændres væsentligt, skal Privacy Lead / PIMS Manager gennemgå berørte AI-relaterede databeskyttelseskontroller og registrere resultatet i REG02, REG04 eller REG12.

11.3 [Controller] Mindst årligt og efter væsentlige ændringer i AI-relaterede brugerrejser skal Process Owner / Business Owner gennemgå bevismateriale for gennemsigtighed, meningsfulde oplysninger, menneskelig gennemgang og rettighedsrute og registrere gennemgangen i REG06 og REG07.

11.4 [All] Efter AI-relaterede korrigerende handlinger vedrørende databeskyttelse er lukket, skal Internal Audit / Compliance Reviewer verificere effektiviteten og registrere bevismateriale for verifikation i REG12.

## 12. Relaterede politikker

- 12.1 PII01 - Politik for Privacy Information Management System
- 12.2 PII02 - Politik for roller, ansvar og ansvarlighed vedrørende databeskyttelse
- 12.3 PII03 - Politik for fortegnelse over PII-behandling og behandlingsgrundlag
- 12.4 PII04 - Politik for privatlivsmeddelelse og gennemsigtighed
- 12.5 PII05 - Politik for samtykke og præferencestyring
- 12.6 PII06 - Politik for håndtering 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 PII
- 12.10 PII10 - Politik for opbevaring, sletning og bortskaffelse af PII
- 12.11 PII11 - Politik for nøjagtighed og kvalitet af PII
- 12.12 PII12 - Politik for databehandlere, underdatabehandlere og tredjeparters databeskyttelsesstyring
- 12.13 PII13 - Politik for international overførsel af PII
- 12.14 PII14 - Politik for PII-sikkerhed og adgangsstyring
- 12.15 PII15 - Politik for håndtering af PII-hændelser og brud
- 12.16 PII17 - Politik for dokumenterede oplysninger og bevisstyring i PIMS
- 12.17 PII18 - Politik for overvågning, revision og forbedring i PIMS
- 12.18 PII19 - Politik for medarbejderes privatliv
- 12.19 PII20 - Politik for børns privatliv
- 12.20 PII22 - Politik for privatliv ved markedsføring og cookies

### 13. Referencestandarder og rammeværker

- 13.1 ISO/IEC 27701:2025 - Clause 7.5; Clause 8.1. Addressed by clauses [4.1.6; 4.8.1; 6.1; 7.1; 7.5; 11.1].
- 13.2 ISO/IEC 27701:2025 - Clause 9.1; Clause 10.2. Addressed by clauses [4.6.2; 4.6.5; 4.8.2; 6.5; 8.1; 8.2; 8.3; 8.4; 8.5; 10.1; 11.4].
- 13.3 ISO/IEC 27701:2025 - Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.9. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.2.1; 4.2.3; 4.2.4; 4.8.1; 7.1; 7.2].
- 13.4 ISO/IEC 27701:2025 - Annex A.1.2.7; Annex A.1.2.8. Addressed by clauses [4.1.4; 4.7.1; 4.7.2; 4.7.3; 5.7; 6.3; 7.6].
- 13.5 ISO/IEC 27701:2025 - Annex A.1.3.2; Annex A.1.3.3; Annex A.1.3.4. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 7.3; 11.3].
- 13.6 ISO/IEC 27701:2025 - Annex A.1.3.6; Annex A.1.3.7; Annex A.1.3.10; Annex A.1.3.11. Addressed by clauses [4.1.3; 4.3.2; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 7.4; 11.3].
- 13.7 ISO/IEC 27701:2025 - Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5. Addressed by clauses [4.2.4; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 7.1; 7.5].
- 13.8 ISO/IEC 27701:2025 - Annex A.1.5.2; Annex A.1.5.3; Annex A.1.5.4; Annex A.1.5.5. Addressed by clauses [4.7.3; 4.7.4; 4.7.5; 7.7].
- 13.9 ISO/IEC 27701:2025 - Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.6; Annex A.2.2.7. Addressed by clauses [4.1.5; 4.3.5; 4.5.5; 4.7.1; 4.7.2; 5.7; 6.3; 7.6].
- 13.10 ISO/IEC 27701:2025 - Annex A.2.3.2; Annex A.2.5.2; Annex A.2.5.3; Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6. Addressed by clauses [4.3.5; 4.5.5; 4.7.1; 4.7.2; 4.7.4; 4.7.5; 7.6; 7.7].
- 13.11 ISO/IEC 27701:2025 - Annex A.3.14; Annex A.3.25. Addressed by clauses [4.4.4; 4.6.1; 4.6.3; 4.8.1; 5.4; 7.5; 7.8; 10.2].
- 13.12 GDPR - Article 4(4); Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(1)(d); Article 5(2). Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.3.1; 4.4.1; 4.4.2; 4.4.5; 4.8.1; 8.1].
- 13.13 GDPR - Article 6; Article 9; Article 10. Addressed by clauses [4.1.2; 4.2.4; 4.4.3; 4.7.3; 7.1].
- 13.14 GDPR - Article 12; Article 13; Article 14; Article 15. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.5.2; 4.5.3; 7.3; 11.3].
- 13.15 GDPR - Article 16; Article 17; Article 18; Article 21; Article 22. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 7.4].
- 13.16 GDPR - Article 24; Article 25; Article 26; Article 28; Article 30; Article 32; Article 35; Article 39. Addressed by clauses [4.1.4; 4.1.5; 4.2.1; 4.2.2; 4.2.5; 4.4.4; 4.7.1; 4.8.2; 5.3; 6.2; 6.4; 7.2].
- 13.17 GDPR - Article 44. Addressed by clauses [4.7.4; 7.7; 8.4].
- 13.18 ISO/IEC 29100:2020 - Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6; Clause 5.7. Addressed by clauses [4.1.2; 4.2.4; 4.4.1; 4.4.2; 4.4.4; 4.4.5; 4.7.5].
- 13.19 ISO/IEC 29100:2020 - Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.11; Clause 5.12. Addressed by clauses [4.3.1; 4.3.2; 4.5.1; 4.5.2; 4.6.3; 4.8.1; 4.8.2; 8.5; 10.1].
- 13.20 ISO/IEC 29134:2020 - Clause 5.1; Clause 6.2; Clause 6.3. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.5; 4.6.4; 6.4; 7.2; 9.2].
- 13.21 ISO/IEC 29151:2022 - Annex A.4; Annex A.5; Annex A.7; Annex A.8; Annex A.10. Addressed by clauses [4.3.1; 4.3.2; 4.4.1; 4.4.2; 4.4.4; 4.4.5; 4.5.2; 4.5.4; 4.7.5].