

				Voer hier de naam van de geregistreerde rechtspersoon in							
Documentnummer: PII21				Documenttitel: <b>Privacybeleid voor AI en geautomatiseerde besluitvorming</b>							
Versie: 1.0		Ingangsdatum: 01.01.2025		Documenteigenaar:							
X	Beleid		Standaard		Procedure		Formulier		Register		Overig

Revisiegeschiedenis				
Revisienummer	Revisiedatum	Wijzigingen	Beoordeeld door	Proceseigenaar

Goedkeuringen			
Naam	Functie	Datum	Handtekening

**Juridische kennisgeving (auteursrecht en gebruiksbeperkingen)**  
(C) 2025 Clarysec LLC. All rights reserved.

Dit document is intellectueel eigendom van Clarysec LLC. Geen enkel deel van dit document mag zonder voorafgaande uitdrukkelijke schriftelijke toestemming worden gekopieerd, hergebruikt, verspreid of gewijzigd voor commerciële of implementatiedoeleinden.

Ongeautoriseerd gebruik is strikt verboden en kan leiden tot juridische stappen.

Neem voor licentiëring contact op via: [info@clarysec.com](mailto:info@clarysec.com)

## Afgestemd op normen en regelgeving

Norm/regelgeving	Clausule/beheersmaatregel/artikel	Toepasselijkheid	Dekkingssoort	Opmerking
ISO/IEC 27701:2025	Clause 7.5; Clause 8.1	Both	Primary	Gedocumenteerde informatie en operationele beheersing voor bewijsmateriaal over verwerking met AI, profilering en geautomatiseerde besluitvorming
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Monitoring, non-conformiteit en corrigerende maatregelen voor privacybeheersmaatregel en voor 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	Doel, rechtsgrondslag, privacy-impactbeoordeling en registraties van de verwerkingsverantwoordelijke
ISO/IEC 27701:2025	Annex A.1.2.7; Annex A.1.2.8	Controller	Supporting	Verwerkerscontracten en verantwoordelijkheden van gezamenlijke verwerkingsverantwoordelijken voor AI-gerelateerde verwerking van PII
ISO/IEC 27701:2025	Annex A.1.3.2; Annex A.1.3.3; Annex A.1.3.4	Controller	Primary	Verplichtingen jegens betrokkenen en transparantie voor AI-gerelateerde verwerking
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	Bezwaar, inzage, rectificatie, wissing, verzoekafhandeling en verplichtingen inzake geautomatiseerde besluitvorming
ISO/IEC 27701:2025	Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5	Controller	Primary	Grenzen voor verzameling, verwerking en minimalisatie voor AI-invoer, uitvoer en afgeleide gegevens
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 van internationale doorgiften, verstrekkingen en verzoeken om

				verstrekking voor AI-gerelateerde 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	Verwerkersovereenkomst, gedocumenteerde instructies, ondersteuning van klantverplichtingen en registraties
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	Ondersteuning door verwerkers voor verplichtingen jegens betrokkenen, routing van doorgiften en afhandeling van verstrekkingen
ISO/IEC 27701:2025	Annex A.3.14; Annex A.3.25	Both	Supporting	Bescherming van registraties en logging met betrekking tot AI-gerelateerde verwerking van 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	Profilering, behoorlijkheid, transparantie, doelbinding, minimalisatie, juistheid en verantwoordingsplicht
GDPR	Article 6; Article 9; Article 10	Controller	Primary	Rechtmatigheid, bijzondere categorieën van gegevens en waarborgen voor gegevens over strafrechtelijke veroordelingen of strafbare feiten
GDPR	Article 12; Article 13; Article 14; Article 15	Controller	Primary	Transparante informatie, inzage en nuttige informatie over geautomatiseerde besluitvorming
GDPR	Article 16; Article 17; Article 18; Article 21; Article 22	Controller	Primary	Rechten op rectificatie, wissing, beperking, bezwaar en geautomatiseerde besluitvorming
GDPR	Article 24; Article 25; Article 26; Article 28; Article 30; Article 32; Article 35; Article 39	Both	Supporting	Verantwoordelijkheid van de verwerkingsverantwoordelijke, ontwerp/standaardinstellingen, gezamenlijke verwerkingsverantwoordel

				ijken, verwerkers, registraties, beveiliging, DPIA en DPO-taken
GDPR	Article 44	Conditional	Referenced	Routing van internationale doorgiften voor AI-gerelateerde verwerking van PII
ISO/IEC 29100:2020	Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6; Clause 5.7	Both	Primary	Beginselen inzake doel, verzameling, minimalisatie, gebruik, bewaring, verstrekking, juistheid en kwaliteit
ISO/IEC 29100:2020	Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.11; Clause 5.12	Both	Supporting	Transparantie, deelname van personen, verantwoordingsplicht, informatiebeveiliging en naleving van privacyvereisten
ISO/IEC 29134:2020	Clause 5.1; Clause 6.2; Clause 6.3	Both	Supporting	Voordeel van PIA, drempelbepaling en voorbereiding voor AI-gerelateerde beoordeling van privacyrisico's
ISO/IEC 29151:2022	Annex A.4; Annex A.5; Annex A.7; Annex A.8; Annex A.10	Both	Supporting	Beheersmaatregelen voor doel, verzameling, minimalisatie, gebruik, bewaring, verstrekking, juistheid en deelname van betrokkenen

## 1. Reikwijdte

1.1 Dit beleid definieert verplichte privacyvereisten voor verwerkingsactiviteiten met kunstmatige intelligentie, profilering, scoring, aanbevelingen, beslissingsondersteuning en geautomatiseerde besluitvorming die PII gebruiken, afleiden, genereren, verstrekken of anderszins verwerken binnen de PIMS-reikwijdte.

### 1.2 Dit beleid is van toepassing op:

1.2.1 AI-ondersteunde systemen, toepassingen, modellen, diensten, workflows, beslissingsengines, scoringtools, aanbevelingssystemen, analysemodellen en processen voor geautomatiseerde besluitvorming die PII verwerken;

1.2.2 profilering, segmentatie, classificatie, voorspelling, inferentie, personalisatie, rangschikking, geschiktheid, fraudedetectie, risicoscoring, toegangsbeslissingen, arbeidsgerelateerde beoordeling, kindgerelateerde profilering, marketingpersonalisatie en vergelijkbare verwerking waarbij PII betrokken is;

1.2.3 AI-gerelateerde PII die wordt gebruikt voor training, testen, validatie, tuning, monitoring, productie-inferentie, beoordeling van uitvoer, prestatiemeting, incidentonderzoek of uitfasering van modellen;

1.2.4 contexten van verwerkingsverantwoordelijke, gezamenlijke verwerkingsverantwoordelijke, verwerker en subverwerker;

1.2.5 AI-gerelateerde leveranciers, verwerkers, subverwerkers, ontvangers van gegevensdeling en internationale doorgiftroutes die PII verwerken.

1.3 Dit beleid creëert geen volledig AI-governancekader, AI-managementsysteem, AI-inventaris, modelinventaris, modelrisicoregister, fairness-register, algoritmeregister, AI-incidentregister, AI-comité, rol van modeleigenaar, rol van AI-systeemeigenaar, workflow voor juridisch advies of afzonderlijk AI-goedkeuringsformulier.

### 1.4 Dit beleid vervangt niet:

1.4.1 PII03 voor verwerkingsinventaris, rechtsgrondslag en ROPA-eigenaarschap;

1.4.2 PII04 voor governance van privacyverklaringen;

1.4.3 PII05 voor toestemming en voorkeurenbeheer;

1.4.4 PII06 voor de workflow voor rechten van betrokkenen;

1.4.5 PII07 voor privacyrisicobeoordeling en DPIA-methodologie;

1.4.6 PII08 voor privacy by design- en privacy-by-default-gates;

1.4.7 PII09 voor beheersmaatregelen voor verzameling, gebruik, verstrekking en delen;

1.4.8 PII10 voor uitvoering van bewaring, verwijdering en afvoer;

1.4.9 PII11 voor beheersmaatregelen voor juistheid en kwaliteit;

1.4.10 PII12 voor lifecycle-governance van verwerkers, subverwerkers en derde partijen;

1.4.11 PII13 voor beheersmaatregelen voor internationale doorgifte;

1.4.12 PII14 voor beveiliging en toegangscontrole;

1.4.13 PII15 voor incident- en inbreukafhandeling;

1.4.14 PII18 voor monitoring, audit en verbetering;

1.4.15 PII19 voor privacy van werknemers;

1.4.16 PII20 voor privacy van kinderen;

1.4.17 PII22 voor marketingprivacy en cookies.

## 2. Doel

- 2.1 Het doel van dit beleid is te waarborgen dat activiteiten met AI, profilering en geautomatiseerde besluitvorming waarbij PII betrokken is, worden geïdentificeerd, gedocumenteerd, op risico beoordeeld, transparant en aanvechtbaar zijn, worden gemonitord en via het PIMS worden beheerst zonder dubbele AI-specifieke governanceartefacten te creëren.
- 2.2 Dit beleid waarborgt dat privacyverplichtingen voor AI-gerelateerde verwerking van PII worden aangetoond via REG02, REG04, REG06, REG07, REG08, REG09, REG10 en REG12.

### **3. Doelstellingen**

#### **3.1 De doelstellingen van dit beleid zijn:**

- 3.1.1 AI, profilering en geautomatiseerde besluitvorming waarbij PII betrokken is in REG02 te identificeren;
- 3.1.2 AI-gerelateerde doelen, rechtsgrondslag, PII-categorieën, gegevensbronnen, afgeleide gegevens, uitvoer, ontvangers en besluitvormingseffecten in REG02 te documenteren;
- 3.1.3 privacyrisicoscreening en DPIA-routering via REG04 te activeren;
- 3.1.4 te waarborgen dat AI-gerelateerde privacyverklaringen en nuttige informatie in REG07 worden geregistreerd;
- 3.1.5 verzoeken inzake rechten, bezwaar, menselijke tussenkomst en aanvechtbaarheid via REG06 te routeren;
- 3.1.6 AI-gerelateerde verwerkers, subverwerkers, leveranciers en gegevensdelingsregelingen via REG08 te beheersen;
- 3.1.7 AI-gerelateerde internationale doorgiften via REG09 te routeren;
- 3.1.8 vermoedelijke AI-gerelateerde incidenten met PII, misbruik, ongeautoriseerde verstrekking en nadelige privacy-uitkomsten via REG10 en REG12 te escaleren;
- 3.1.9 monitoring, uitzonderingen, non-conformiteiten, corrigerende maatregelen en verbeteringen in REG12 vast te leggen.

### **4. Beleidsverklaringen**

#### **4.1 Identificatie van AI, profilering en geautomatiseerde besluitvorming**

- 4.1.1 [Controller] Wanneer een nieuw of wezenlijk gewijzigd systeem, toepassing, model, workflow, dienst of bedrijfsproces wordt voorgesteld, moet de Process Owner / Business Owner bepalen of dit AI, profilering, scoring, aanbeveling, beslissingsondersteuning of geautomatiseerde besluitvorming waarbij PII betrokken is gebruikt, en de bepaling in REG02 vastleggen.
- 4.1.2 [Controller] Voordat AI-gerelateerde verwerking van PII begint, moet de Process Owner / Business Owner het verwerkingsdoel, de PII-categorieën, categorieën betrokkenen, gegevensbronnen, categorieën geïnfereerde of afgeleide gegevens, uitvoercategorieën, ontvangerscategorieën, rechtsgrondslag en koppeling aan bewaartermijnen in REG02 documenteren.
- 4.1.3 [Controller] Voordat profilering, scoring, aanbeveling, beslissingsondersteuning of geautomatiseerde besluitvorming in productie wordt gebruikt, moet de Process Owner / Business Owner de beslissingscontext, het verwachte effect op betrokkenen, menselijke betrokkenheid en route voor rechten in REG02 en REG04 documenteren.
- 4.1.4 [Joint Controller] Voordat AI-gerelateerde verwerking van PII met een gezamenlijke verwerkingsverantwoordelijke wordt uitgevoerd, moet de Privacy Lead / PIMS Manager de verantwoordelijkheid voor doelbepaling, kennisgeving, afhandeling van rechten, DPIA-ondersteuning, verwerkersgovernance en incidentescalatie in REG08 documenteren.
- 4.1.5 [Processor] Voordat PII via een AI-gerelateerde dienst voor een klant wordt verwerkt, moet de Process Owner / Business Owner bevestigen dat klantinstructies, toegestane doelen,

verboden gebruik, behandeling van uitvoer en bijstandsverplichtingen in REG08 zijn gedocumenteerd.

- 4.1.6 [Both] Voordat AI-gerelateerde verwerking van PII wordt geactiveerd, moet de Privacy Lead / PIMS Manager bevestigen dat de verwerking is gekoppeld aan de toepasselijke canonieke bewijsobjecten en dat er geen afzonderlijk AI-specifiek register buiten REG02, REG04, REG06, REG07, REG08, REG09, REG10 of REG12 wordt aangemaakt.

## **4.2 Privacyrisicobeoordeling en DPIA-routering**

- 4.2.1 [Controller] Voordat AI-gerelateerde verwerking van PII wordt gelanceerd of wezenlijk wordt gewijzigd, moet de Privacy Lead / PIMS Manager een privacyrisicoscreening uitvoeren en het DPIA-besluit in REG04 vastleggen.
- 4.2.2 [Conditional] Wanneer AI-gerelateerde verwerking profilering, geautomatiseerde besluiten, grootschalige beoordeling, bijzondere categorieën van gegevens, gegevens over strafbare feiten, kwetsbare betrokkenen, werknemersbeoordeling, kinderen, gedragsmonitoring, locatiegegevens, biometrische gegevens, scoring met hoge impact of aanzienlijke effecten omvat, moet de Data Protection Officer / Privacy Advisor het privacyrisico beoordelen en advies in REG04 vastleggen.
- 4.2.3 [Controller] Vóór livegang in productie voor AI-gerelateerde verwerking van PII moet de Process Owner / Business Owner risicobehandelingsacties, de status van resterend risico en bewijsmateriaal voor liveganggereedheid in REG04 of REG12 documenteren.
- 4.2.4 [Controller] Voordat PII wordt hergebruikt voor AI-training, testen, validatie, tuning, monitoring of modelverbetering voor een nieuw of wezenlijk gewijzigd doel, moet de Process Owner / Business Owner een privacybeoordeling uitvoeren en het besluit in REG02 en REG04 vastleggen.
- 4.2.5 [Conditional] Wanneer het resterende privacyrisico na geplande behandeling hoog blijft, moet Top Management het gebruik in productie goedkeuren, afwijzen of verdere behandeling vereisen en het besluit in REG04 en REG12 vastleggen.

[ ... Secties 4.3–8 zijn niet opgenomen in dit voorbeeld. Koop het volledige document voor toegang tot de volledige inhoud. ... ]

## **9. Uitzonderingen**

- 9.1 [All] Voordat van een AI-gerelateerde privacyvereiste in dit beleid wordt afgeweken, moet de verzoekende Process Owner / Business Owner een motivering voor de uitzondering en bewijsmateriaal voor compenserende beheersmaatregelen in REG12 indienen.
- 9.2 [Conditional] Wanneer een uitzondering gevolgen heeft voor profilering, geautomatiseerde besluitvorming, menselijke tussenkomst, aanvechtbaarheid, transparantie, DPIA-uitkomst, scoring met hoge impact, kindgerelateerde verwerking, werknemersgerelateerde verwerking, verwerkersbeperkingen of internationale doorgiften, moet de Data Protection Officer / Privacy Advisor de uitzondering beoordelen en advies in REG04 of REG12 vastleggen.
- 9.3 [Conditional] Wanneer een uitzondering een hoog resterend privacyrisico creëert of in stand houdt, moet Top Management de uitzondering goedkeuren of afwijzen en het besluit in REG04 en REG12 vastleggen.
- 9.4 [All] Voordat een goedgekeurde AI-gerelateerde privacy-uitzondering verloopt, moet de Privacy Lead / PIMS Manager de status van afsluiting, verlenging of corrigerende maatregelen beoordelen en de uitkomst in REG12 vastleggen.

## **10. Handhaving**

- 10.1 [All] Wanneer niet-naleving van dit beleid wordt vastgesteld, moet de Privacy Lead / PIMS Manager de non-conformiteit en corrigerende maatregel in REG12 vastleggen.

- 10.2 [Both] Wanneer ongeautoriseerde AI-gerelateerde verwerking, verstrekking, toegang, modelmisbruik, falen van rechten of een nadelige privacy-uitkomst met betrekking tot PII wordt vermoed, moet de Incident Response Coordinator incidentescalatie initiëren en bewijsmateriaal in REG10 en REG12 vastleggen.
- 10.3 [Both] Wanneer een verwerker, subverwerker, leverancier of ontvanger van gegevensdeling niet voldoet aan AI-gerelateerde privacyverplichtingen, moet de Vendor / Procurement Owner herstel-, escalatie- of beëindigingsmaatregelen in REG08 en REG12 vastleggen.
- 10.4 [All] Wanneer herhaalde of systemische AI-gerelateerde privacy-non-conformiteiten optreden, moet Top Management de kwestie beoordelen en de managementmaatregel in REG12 vastleggen.

## 11. Beoordeling en onderhoud

- 11.1 [All] Ten minste jaarlijks moet de Privacy Lead / PIMS Manager dit beleid beoordelen op blijvende geschiktheid en de beoordelingsuitkomst in REG12 vastleggen.
- 11.2 [Conditional] Wanneer wetgeving, diensten, modellen, gegevensbronnen, profileringspraktijken, logica voor geautomatiseerde besluitvorming, leveranciersregelingen, doorgiftroutes of privacyrisico's wezenlijk veranderen, moet de Privacy Lead / PIMS Manager de getroffen AI-gerelateerde privacybeheersmaatregelen beoordelen en de uitkomst in REG02, REG04 of REG12 vastleggen.
- 11.3 [Controller] Ten minste jaarlijks en na wezenlijke wijzigingen in AI-gerelateerde gebruikersreizen moet de Process Owner / Business Owner bewijsmateriaal over transparantie, nuttige informatie, menselijke tussenkomst en routes voor rechten beoordelen en de beoordeling in REG06 en REG07 vastleggen.
- 11.4 [All] Nadat AI-gerelateerde corrigerende privacymaatregelen zijn afgesloten, moet de Internal Audit / Compliance Reviewer de doeltreffendheid verifiëren en verificatiebewijsmateriaal in REG12 vastleggen.

## 12. Gerelateerde beleidslijnen

- 12.1 PII01 - Beleid voor het privacy-informatiemanagementsysteem
- 12.2 PII02 - Beleid inzake privacyrollen, verantwoordelijkheden en verantwoordingsplicht
- 12.3 PII03 - Beleid inzake PII-verwerkingsinventaris en rechtsgrondslag
- 12.4 PII04 - Beleid inzake privacyverklaring en transparantie
- 12.5 PII05 - Beleid inzake toestemming en voorkeurenbeheer
- 12.6 PII06 - Beleid voor beheer van rechten van betrokkenen
- 12.7 PII07 - Beleid inzake privacyrisicobeoordeling en DPIA
- 12.8 PII08 - Beleid inzake privacy by design en privacy by default
- 12.9 PII09 - Beleid inzake verzameling, gebruik, verstrekking en delen van PII
- 12.10 PII10 - Beleid inzake bewaring, verwijdering en afvoer van PII
- 12.11 PII11 - Beleid inzake juistheid en kwaliteit van PII
- 12.12 PII12 - Beleid inzake privacybeheer van verwerkers, subverwerkers en derde partijen
- 12.13 PII13 - Beleid inzake internationale doorgifte van PII
- 12.14 PII14 - Beleid inzake PII-beveiliging en toegangscontrole
- 12.15 PII15 - Beleid inzake incident- en inbreukbeheer voor PII
- 12.16 PII17 - Beleid inzake gedocumenteerde informatie en bewijsbeheer voor PIMS
- 12.17 PII18 - Beleid inzake PIMS-monitoring, audit en verbetering
- 12.18 PII19 - Privacybeleid voor werknemers

- 12.19 PII20 - Privacybeleid voor kinderen
- 12.20 PII22 - Beleid inzake marketingprivacy en cookies

### 13. Referentienormen en -raamwerken

- 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].