

				Voer hier de naam van de geregistreerde rechtspersoon in							
Documentnummer: PII05				Documenttitel: Beleid inzake toestemming en voorkeurenbeheer							
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

Afgestemd op normen en regelgeving

Norm/regelgeving	Clausule/beheersmaatregel/artikel	Toepasselijkheid	Dekkingsoort	Opmerking
ISO/IEC 27701:2025	Clause 7.5; Clause 8.1	Both	Primary	Gedocumenteerde informatie en operationele beheersing voor bewijs van toestemming
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Monitoring, non-conformiteit, corrigerende maatregelen en verbetering
ISO/IEC 27701:2025	Annex A.1.2.3	Controller	Supporting	Koppeling met de rechtsgrondslag
ISO/IEC 27701:2025	Annex A.1.2.4; Annex A.1.2.5	Controller	Primary	Vaststelling, verkrijging en registratie van toestemming
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Primary	Verwerkingsregistraties van de verwerkingsverantwoordelijke
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.7	Processor	Supporting	Verwerkersovereenkomsten, klantdoeleinden en verwerkersregistraties
ISO/IEC 27701:2025	Annex A.2.3.2	Processor	Supporting	Ondersteuning door de verwerker voor verplichtingen van de verwerkingsverantwoordelijke jegens betrokkenen
ISO/IEC 27701:2025	Annex A.3.14	Both	Supporting	Bescherming van registraties van PII-verwerking
GDPR	Article 4(11)	Controller	Supporting	Criteria voor toestemming
GDPR	Article 5(1)(a); Article 5(2)	Controller	Supporting	Rechtmatigheid, behoorlijkheid, transparantie en verantwoordingsplicht
GDPR	Article 6(1)(a); Article 6(4)	Controller	Primary	Toestemming als rechtsgrondslag en koppeling bij gewijzigd doel

GDPR	Article 7	Controller	Primary	Voorwaarden voor toestemming en intrekking
GDPR	Article 8	Conditional	Supporting	Escalatie voor toestemming van kinderen
GDPR	Article 9(2)(a)	Conditional	Supporting	Uitdrukkelijke toestemming voor verwerking van bijzondere categorieën
GDPR	Article 24	Controller	Supporting	Verantwoordelijkheid en maatregelen van de verwerkingsverantwoordelijke
GDPR	Article 28	Both	Supporting	Koppeling met verwerkersinstructies en bijstand
GDPR	Article 30	Both	Supporting	Koppeling met verwerkingsregistraties
ISO/IEC 29100:2020	Clause 5.2; Clause 5.8; Clause 5.12	Both	Supporting	Beginnelsen voor toestemming en keuze, transparantie en naleving
ISO/IEC 29151:2022	Annex A.3	Both	Supporting	Beheersmaatregelen voor toestemming en keuze
ISO/IEC TS 27560:2023	Clause 5.2; Clause 6.2; Clause 6.3; Clause 6.4	Conditional	Supporting	Structuur voor toestemmingsregistratie en toestemmingsbewijs waar gebruikt

1. Reikwijdte

- 1.1 Dit beleid definieert verplichte vereisten voor het bepalen wanneer toestemming vereist is, het vragen van toestemming, het vastleggen van bewijs van toestemming, het beheren van voorkeuren, het verwerken van intrekkingen, het onderhouden van toestemmingsregistraties en het beoordelen van toestemmingsmechanismen.
- 1.2 Dit beleid is van toepassing op PII-verwerking waarbij toestemming als rechtsgrondslag wordt gekozen of vereist is, waarbij uitdrukkelijke toestemming vereist is, waarbij toestemmingsvoorkeuren worden vastgelegd, of waarbij de organisatie toestemmingsregistraties namens een verwerkingsverantwoordelijke beheert.
- 1.3 Dit beleid is van toepassing in contexten van verwerkingsverantwoordelijke, gezamenlijke verwerkingsverantwoordelijke, verwerker en subverwerker. Verplichtingen van verwerkers en subverwerkers zijn alleen van toepassing wanneer toestemmingsregistraties, voorkeursstatussen of instructies tot intrekking worden beheerd op basis van gedocumenteerde instructies van de verwerkingsverantwoordelijke of klant.
- 1.4 Dit beleid maakt toestemming niet tot de standaardrechtsgrondslag voor PII-verwerking. De vaststelling van de rechtsgrondslag blijft beheerst door PII03 - Beleid inzake PII-verwerkingsinventaris en rechtsgrondslag.

2. Doel

- 2.1 Het doel van dit beleid is te waarborgen dat toestemming en voorkeurenbeheer rechtmatig, transparant, aantoonbaar, herroepbaar, technisch afdwingbaar en ondersteund door beheerst bewijsmateriaal zijn.
- 2.2 Dit beleid waarborgt dat toestemming alleen wordt gevraagd waar dit passend is, dat toestemmingsregistraties volledig en traceerbaar zijn, dat intrekkingen worden nageleefd, en dat bewijs van toestemming beschikbaar blijft voor audits, onderzoeken en verantwoordingsdoeleinden.

3. Doelstellingen

3.1 De doelstellingen van dit beleid zijn om:

- 3.1.1 Te waarborgen dat toestemming alleen wordt gebruikt wanneer deze de passende rechtsgrondslag is of wanneer toestemming voor de verwerkingsactiviteit vereist is.
- 3.1.2 Te waarborgen dat toestemmingsverzoeken specifiek, geïnformeerd en onderscheidbaar zijn en aan de toepasselijke privacyverklaring zijn gekoppeld.
- 3.1.3 Te waarborgen dat toestemmings- en voorkeursregistraties in REG05 worden vastgelegd en onderhouden.
- 3.1.4 Te waarborgen dat intrekkingen en voorkeurswijzigingen binnen gedefinieerde operationele termijnen worden uitgevoerd.
- 3.1.5 Te waarborgen dat toestemmingsregistraties worden gekoppeld aan verwerkingsdoeleinden in REG02 en versies van privacyverklaringen in REG07.
- 3.1.6 Te waarborgen dat activiteiten van verwerkers en subverwerkers ter ondersteuning van toestemming gedocumenteerde instructies van de verwerkingsverantwoordelijke of klant volgen.
- 3.1.7 Te waarborgen dat toestemmingsmechanismen worden gemonitord, beoordeeld, gecorrigeerd en auditeerbaar zijn.

4. Beleidsverklaringen

4.1 Toepasselijkheid van toestemming en rechtsgrondslag

- 4.1.1 [Controller] De Process Owner / Business Owner moet in REG02 vastleggen of toestemming vereist of gekozen is voordat een nieuwe of wezenlijk gewijzigde PII-verwerkingsactiviteit die op toestemming berust, begint.
- 4.1.2 [Controller] De Privacy Lead / PIMS Manager moet in REG02 en REG05 verifiëren dat toestemming niet als standaardrechtsgrondslag is gekozen voordat een nieuwe of wezenlijk gewijzigde verwerkingsactiviteit op basis van toestemming wordt goedgekeurd.
- 4.1.3 [Controller] De Data Protection Officer / Privacy Advisor moet de toestemmingsgrondslag vóór ingebruikname in REG04 beoordelen wanneer de verwerking bijzondere categorieën PII, op kinderen gerichte diensten, verwerking met een hoog risico, of een onevenwicht tussen de organisatie en de betrokkene omvat.
- 4.1.4 [Joint Controller] De Privacy Lead / PIMS Manager moet in REG02 en REG05 documenteren welke partij verantwoordelijk is voor het verkrijgen, registreren, vernieuwen en naleven van toestemming voordat verwerking door gezamenlijke verwerkingsverantwoordelijken begint.
- 4.1.5 [Processor] De Privacy Lead / PIMS Manager moet klantinstructies voor het vastleggen van toestemming, voorkeurenbeheer of ondersteuning bij intrekking in REG08 en REG05 vastleggen voordat een toestemmingsmechanisme namens een verwerkingsverantwoordelijke wordt geïmplementeerd.
- 4.1.6 [Subprocessor] De Vendor / Procurement Owner moet toestemmingsgerelateerde verplichtingen van subverwerkers in REG08 vastleggen voordat een subverwerker toestemmingsregistraties, voorkeursstatussen of instructies tot intrekking mag behandelen.

4.2 Verzoek om en vastlegging van toestemming

- 4.2.1 [Controller] De Process Owner / Business Owner moet waarborgen dat elk toestemmingsverzoek doelspecifiek is en aan de toepasselijke REG07-versie van de privacyverklaring is gekoppeld voordat het toestemmingsverzoek aan een betrokkene wordt voorgelegd.
- 4.2.2 [Controller] De System Owner / Application Owner moet toestemmingsmechanismen zo configureren dat een bevestigende handeling vereist is voordat de verwerking begint, wanneer uitdrukkelijke toestemming of opt-in-toestemming vereist is.
- 4.2.3 [Controller] De Process Owner / Business Owner moet de referentie van de betrokkene, het doel, de PII-categorie, de toestemmingsformulering of -versie, de versie van de privacyverklaring, het vastleggingskanaal, het tijdstempel, de methode, de status en de toepasselijke geldigheidsduur in REG05 vastleggen wanneer toestemming wordt vastgelegd.
- 4.2.4 [Conditional] De Privacy Lead / PIMS Manager moet logica voor leeftijdsverificatie of autorisatie in REG05 vastleggen en een REG04-beoordeling vóór ingebruikname activeren wanneer toestemming betrekking heeft op verwerking gericht op kinderen.
- 4.2.5 [Conditional] De Privacy Lead / PIMS Manager moet toestemming in REG05 als uitdrukkelijk markeren voordat de verwerking begint wanneer uitdrukkelijke toestemming voor het gekozen doel vereist is.
- 4.2.6 [Both] De System Owner / Application Owner moet voorkomen dat verwerking die op toestemming berust, doorgaat voordat REG05 een actieve toestemmingsstatus voor het betreffende doel toont.

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

9. Uitzonderingen

- 9.1.1 [All] De Process Owner / Business Owner moet een uitzondering in REG12 aanvragen voordat wordt afgeweken van een goedgekeurde vereiste voor het vastleggen van toestemming, voorkeurenbeheer, intrekking of bewijs.
- 9.1.2 [All] De Privacy Lead / PIMS Manager moet elke toestemmingsgerelateerde uitzondering in REG12 goedkeuren of afwijzen vóór implementatie en voor elke goedgekeurde uitzondering een vervaldatum en compenserende beheersmaatregel toewijzen.
- 9.1.3 [Conditional] De Data Protection Officer / Privacy Advisor moet de uitzondering in REG04 of REG12 beoordelen vóór goedkeuring wanneer de uitzondering uitdrukkelijke toestemming, verwerking gericht op kinderen, verwerking met een hoog risico of een intrekkingmechanisme betreft.
- 9.1.4 [Both] De System Owner / Application Owner moet de productierelease blokkeren of het betrokken toestemmingsmechanisme uitschakelen wanneer een door dit beleid vereiste uitzondering vóór livegang niet in REG12 is goedgekeurd.

10. Handhaving

- 10.1.1 [All] De Privacy Lead / PIMS Manager moet binnen vijf werkdagen na identificatie van ontbrekend, ongeldig, niet-gekoppeld of onbetrouwbaar bewijs van toestemming een toestemmingsgerelateerde non-conformiteit in REG12 vastleggen.
- 10.1.2 [Controller] De Process Owner / Business Owner moet verwerking voor het betrokken doel opschorten of remediëren voordat verdere verwerking op basis van toestemming wordt voortgezet wanneer toestemming vereist is maar niet in REG05 kan worden aangetoond.
- 10.1.3 [Both] De System Owner / Application Owner moet een niet-conform mechanisme voor het vastleggen van toestemming, voorkeuren of intrekking uitschakelen of corrigeren binnen de in REG12 toegewezen termijn.
- 10.1.4 [Processor] De Vendor / Procurement Owner moet tekortkomingen in klantinstructies met betrekking tot toestemmingsregistraties, voorkeursstatussen of ondersteuning bij intrekking binnen vijf werkdagen na identificatie in REG08 en REG12 escaleren.
- 10.1.5 [All] De Internal Audit / Compliance Reviewer moet uiterlijk op de toegewezen vervaldatum het afsluitingsbewijs voor toestemmingsgerelateerde corrigerende maatregelen in REG12 verifiëren.

11. Beoordeling en onderhoud

- 11.1.1 [All] De Privacy Lead / PIMS Manager moet dit beleid jaarlijks beoordelen en de uitkomst van de beoordeling in REG12 vastleggen.
- 11.1.2 [All] De Privacy Lead / PIMS Manager moet dit beleid binnen 30 dagen beoordelen na een wezenlijke wijziging in wetgeving over toestemming, toestemmingstechnologie, tooling voor voorkeurenbeheer, de structuur van privacyverklaringen of PIMS-certificeringsvereisten.
- 11.1.3 [All] De Data Protection Officer / Privacy Advisor moet privacy-significante wijzigingen in dit beleid in REG12 beoordelen vóór goedkeuring.
- 11.1.4 [All] Top Management moet wezenlijke wijzigingen in dit beleid in REG12 goedkeuren vóór publicatie.
- 11.1.5 [All] De Privacy Lead / PIMS Manager moet de communicatie van goedgekeurde beleidswijzigingen binnen 30 dagen na publicatie in REG11 vastleggen.

12. Gerelateerde beleidslijnen

- 12.1 Dit beleid wordt ondersteund door de volgende gerelateerde beleidslijnen:
- 12.2 PII01 - Beleid voor het privacy-informatiemanagementsysteem
- 12.3 PII02 - Beleid inzake privacyrollen, verantwoordelijkheden en verantwoordingsplicht
- 12.4 PII03 - Beleid inzake PII-verwerkingsinventaris en rechtsgrondslag

- 12.5 PII04 - Beleid inzake privacyverklaring en transparantie
- 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 deling van PII
- 12.10 PII10 - Beleid inzake bewaring, verwijdering en vernietiging van PII
- 12.11 PII11 - Beleid inzake nauwkeurigheid en kwaliteit van PII
- 12.12 PII12 - Beleid inzake privacybeheer van verwerkers, subverwerkers en derden
- 12.13 PII14 - Beleid inzake PII-beveiliging en toegangscontrole
- 12.14 PII16 - Beleid inzake privacytraining, bewustwording en bekwaamheid
- 12.15 PII17 - Beleid inzake PIMS-gedocumenteerde informatie en bewijsbeheer
- 12.16 PII18 - Beleid inzake PIMS-monitoring, audit en verbetering

13. Referentienormen en -raamwerken

- 13.1 Dit beleid is gekoppeld aan de volgende normen en regelgeving. De mapping licht toe hoe het beleid de aangehaalde vereisten ondersteunt en identificeert de interne clausules die deze implementeren of ondersteunen.

13.2 ISO/IEC 27701:2025

- 13.2.1 **Clause 7.5; Clause 8.1** - Gekoppeld aan gedocumenteerde informatie en operationele beheersing voor het bepalen van de toepasselijkheid van toestemming, het vastleggen van bewijs van toestemming, het beheren van intrekking, versiebeheer van toestemmingsregistraties, het testen van mechanismen en het onderhouden van 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** - Gekoppeld aan monitoring van toestemming, metrieken, auditsteekproeven, registratie van non-conformiteiten, corrigerende maatregelen en verificatie van doeltreffendheid. 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** - Gekoppeld aan het bevestigen wanneer toestemming een passende rechtsgrondslag is en aan het koppelen van toestemmingsregistraties aan REG02-registraties van rechtsgrondslagen. 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** - Gekoppeld aan het bepalen wanneer en hoe toestemming wordt verkregen, het vastleggen van toestemming, het registreren van bewijs, het beheren van uitdrukkelijke toestemming, intrekking, vernieuwing en toestemmingsstatus. 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** - Gekoppeld aan registraties van de verwerkingsverantwoordelijke voor verwerking op basis van toestemming, toestemmingshistorie, koppeling met privacyverklaringen, bewaring van bewijs en toestemmingsregistraties die gereed zijn voor audits. 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** - Gekoppeld aan klantovereenkomsten van verwerkers, afstemming op klantdoeleinden en -instructies, en verwerkersregistraties wanneer diensten ter ondersteuning van toestemming voor een verwerkingsverantwoordelijke worden uitgevoerd. 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** - Gekoppeld aan ondersteuning door de verwerker voor verplichtingen van de verwerkingsverantwoordelijke jegens betrokkenen wanneer intrekking van toestemming,

voorkeurswijzigingen of bewijs van toestemming op basis van klantinstructies worden behandeld. 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** - Gekoppeld aan bescherming van toestemmings- en voorkeursregistraties tegen ongeautoriseerde wijziging en aan behoud van audittrailbewijs. Addressed by clauses [4.5.2; 5.1.6; 7.1.2; 10.1.5].

13.3 **GDPR**

13.3.1 **Article 4(11)** - Gekoppeld aan toestemmingscriteria die vereisen dat toestemming specifiek en geïnformeerd is, waar vereist bevestigend wordt gegeven, en aan het relevante doel en de toepasselijke versie van de privacyverklaring is gekoppeld. 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)** - Gekoppeld aan rechtmatigheid, behoorlijkheid, transparantie, verantwoordingsbewijs, auditsteekproeven, corrigerende maatregelen en bewijs van verwerking op basis van toestemming. 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)** - Gekoppeld aan toestemming als rechtsgrondslag voor specifieke doeleinden en aan herbeoordeling of vernieuwde toestemming wanneer het doel of de verwerkingsvoorwaarden wezenlijk wijzigen. Addressed by clauses [4.1.1; 4.1.2; 4.4.1; 4.4.2; 4.5.3].

13.3.4 **Article 7** - Gekoppeld aan aantoonbaarheid, onderscheidbare toestemmingsverzoeken, intrekking, gemak van intrekking, geldigheid van toestemming en bewaarde toestemmingshistorie. 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** - Gekoppeld aan escalatie voor toestemming bij op kinderen gerichte diensten, logica voor leeftijdsverificatie of autorisatie, en privacyrisicobeoordeling vóór ingebruikname. Addressed by clauses [4.1.3; 4.2.4; 9.1.3].

13.3.6 **Article 9(2)(a)** - Gekoppeld aan de behandeling van uitdrukkelijke toestemming wanneer uitdrukkelijke toestemming is gekozen voor verwerking van bijzondere categorieën. Addressed by clauses [4.1.3; 4.2.5; 9.1.3].

13.3.7 **Article 24** - Gekoppeld aan governancemaatregelen van de verwerkingsverantwoordelijke, beoordeling, goedkeuring, uitzonderingen, corrigerende maatregelen en managementtoezicht op toestemmingsbeheersmaatregelen. 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** - Gekoppeld aan behandeling van verwerkersinstructies, bewijs voor ondersteuning van toestemming, ondersteuning bij intrekking, verplichtingen van subverwerkers en escalatie van klantinstructies. 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** - Gekoppeld aan het koppelen van toestemmingsregistraties aan verwerkingsdoeleinden, registraties van de verwerkingsverantwoordelijke, ondersteunende registraties van verwerkers en traceerbaarheid tussen REG02 en REG05. 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** - Gekoppeld aan toestemming en keuze, transparantie en koppeling met privacyverklaringen, intrekking, verantwoordingsplicht en bewijs voor privacy naleving. 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** - Gekoppeld aan beheersmaatregelen voor toestemming en keuze die betekenisvolle, geïnformeerde en ondubbelzinnige toestemming, wijziging van voorkeuren en tijdige verwerkingswijzigingen na wijziging of intrekking van toestemming vereisen. 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** - Gekoppeld aan concepten voor toestemmingsregistraties en toestemmingsbewijzen, het bijhouden van toestemmingsregistraties, structuur van toestemmingsregistraties, toestemmingsstatus, koppeling met versie van de privacyverklaring, structuur van toestemmingsbewijzen en interpretatie van toestemmingsbewijzen waar dergelijke registraties of bewijzen worden gebruikt. 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 Interne vereiste - Clausules die REG05 definiëren als het gezaghebbende bewijsobject, goedkeuring van niet-standaard bewijs, blokkering van operationele vrijgave, training, beleidsonderhoud en communicatie ondersteunen consistentie in de implementatie, maar zijn niet rechtstreeks aan één externe clausule gekoppeld. Addressed by clauses [4.5.1; 5.1.2; 7.1.5; 9.1.4; 11.1.2; 11.1.3; 11.1.5].