

				Insérez ici la dénomination de l'entité juridique enregistrée							
Numéro du document : PII22				Titre du document : Politique de confidentialité marketing et relative aux cookies							
Version : 1.0		Date d'entrée en vigueur : 01.01.2025		Propriétaire du document :							
X	Politique		Norme		Procédure		Formulaire		Registre		Autre

Historique des révisions				
Numéro de révision	Date de révision	Modifications	Revu par	Propriétaire du processus

Approbations			
Nom	Fonction	Date	Signature

Mentions légales (droits d'auteur et restrictions d'utilisation)
(C) 2025 Clarysec LLC. All rights reserved.

Le présent document est la propriété intellectuelle de Clarysec LLC. Aucune partie de ce document ne peut être copiée, réutilisée, distribuée ou modifiée à des fins commerciales ou de mise en œuvre sans autorisation écrite expresse préalable.

Toute utilisation non autorisée est strictement interdite et peut entraîner des poursuites judiciaires.

Pour toute demande de licence, contactez : info@clarysec.com

Alignement sur les normes et réglementations

Standard / Regulation	Clause / Control / Article	Applicability	Coverage Type	Comment
ISO/IEC 27701:2025	Clause 7.5; Clause 8.1	Both	Primary	Éléments de preuve documentés en matière de confidentialité marketing et contrôle opérationnel
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Surveillance, non-conformité et action corrective
ISO/IEC 27701:2025	Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.4; Annex A.1.2.5; Annex A.1.2.9	Controller	Primary	Finalités marketing, articulation avec la base légale, consentement et registres de traitement
ISO/IEC 27701:2025	Annex A.1.2.7; Annex A.1.2.8	Controller	Supporting	Sous-traitants marketing et responsabilités des responsables conjoints du traitement
ISO/IEC 27701:2025	Annex A.1.3.2; Annex A.1.3.3; Annex A.1.3.4; Annex A.1.3.5	Controller	Primary	Mentions d'information marketing, mentions relatives aux cookies et informations sur le retrait du consentement
ISO/IEC 27701:2025	Annex A.1.3.6; Annex A.1.3.10	Controller	Supporting	Circuit de traitement des objections et des demandes relatives au marketing direct
ISO/IEC 27701:2025	Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5	Controller	Primary	Collecte, traitement et minimisation pour le marketing et le suivi
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	Circuit de transfert et de divulgation pour l'adtech et l'analytique
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	Supporting	Accord avec le sous-traitant, instruction, support client et registres du sous-traitant

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	Appui du sous-traitant aux obligations, aux transferts et aux circuits de divulgation
ISO/IEC 27701:2025	Annex A.3.14; Annex A.3.25	Both	Supporting	Protection des enregistrements et éléments de preuve de journalisation pour le suivi des modifications
GDPR	Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(2)	Controller	Primary	Loyauté, transparence, limitation des finalités, minimisation et responsabilité
GDPR	Article 6; Article 7	Controller	Primary	Licéité et conditions du consentement
GDPR	Article 12; Article 13; Article 14	Controller	Primary	Informations et mentions transparentes
GDPR	Article 21	Controller	Primary	Circuit d'objection au marketing direct et d'opposition
GDPR	Article 24; Article 25; Article 26; Article 28; Article 30; Article 32	Both	Supporting	Responsabilité, conception/par défaut, responsables conjoints du traitement, sous-traitants, registres et appui à la sécurité
GDPR	Article 44	Conditional	Referenced	Circuit des transferts internationaux pour les prestataires marketing
ISO/IEC 29100:2020	Clause 5.1; Clause 5.8; Clause 5.9	Both	Primary	Consentement et choix, transparence et participation
ISO/IEC 29100:2020	Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Both	Primary	Finalité, collecte, minimisation, utilisation et limitation de la divulgation
ISO/IEC 29100:2020	Clause 5.10; Clause 5.11; Clause 5.12	Both	Supporting	Responsabilité, sécurité de l'information et conformité

ISO/IEC 29151:2022	Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.10	Both	Supporting	Contrôles relatifs au consentement, à la finalité, à la collecte, à la minimisation, à l'utilisation/divulgation et à la participation
ISO/IEC TS 27560:2023	Clause 5.2; Clause 5.3; Clause 6.2; Clause 6.4	Controller	Supporting	Structure des enregistrements et reçus de consentement lorsqu'ils sont utilisés

1. Champ d'application

1.1 La présente politique définit les exigences obligatoires de confidentialité applicables au marketing, aux cookies, aux technologies de suivi, à l'analytique, aux technologies publicitaires, à la segmentation d'audience, au marketing direct, à la gestion des préférences, à la suppression, aux balises de tiers, à la revue des campagnes et aux traitements de PII associés.

1.2 La présente politique s'applique aux contextes de responsable du traitement, de responsable conjoint du traitement, de sous-traitant et de sous-traitant ultérieur. Les obligations du responsable du traitement s'appliquent lorsque l'organisation détermine les finalités et les moyens du marketing. Les obligations du sous-traitant et du sous-traitant ultérieur s'appliquent uniquement lorsque l'organisation traite des PII relatives au marketing, à l'analytique, au suivi ou aux campagnes sur la base d'instructions documentées du client ou du sous-traitant en amont.

1.3 La présente politique couvre :

1.3.1 l'inventaire des traitements marketing et l'articulation avec les finalités ;

1.3.2 les éléments de preuve du consentement et des préférences pour le marketing et le suivi ;

1.3.3 la gouvernance des cookies, des technologies de suivi et des balises ;

1.3.4 les enregistrements des mentions d'information marketing et des mentions relatives aux cookies ;

1.3.5 les circuits de suppression, de retrait et d'opposition ;

1.3.6 la gouvernance des relations avec les prestataires marketing, les fournisseurs d'analytique et l'adtech ;

1.3.7 le circuit des transferts internationaux pour les prestataires et plateformes marketing ;

1.3.8 les éléments de preuve relatifs à la revue et à la surveillance des campagnes.

1.4 La présente politique ne crée pas de registre distinct des cookies, registre des balises, registre de suppression, registre des campagnes marketing, registre analytique, workflow de conseil juridique, comité, tableau de bord, formulaire ou rôle non canonique.

1.5 La présente politique ne remplace pas :

1.5.1 PII03 pour l'inventaire des traitements et la responsabilité relative aux bases légales ;

1.5.2 PII04 pour la gouvernance générale des mentions d'information ;

1.5.3 PII05 pour la gestion du consentement et des préférences ;

1.5.4 PII06 pour le workflow des demandes d'exercice des droits des personnes concernées ;

1.5.5 PII07 pour l'appréciation des risques relatifs à la vie privée et la méthodologie de DPIA ;

1.5.6 PII08 pour les points de contrôle de protection de la vie privée dès la conception et par défaut ;

1.5.7 PII09 pour les contrôles généraux relatifs à la collecte, à l'utilisation, à la divulgation et au partage ;

1.5.8 PII10 pour l'exécution de la conservation, de la suppression et de l'élimination ;

1.5.9 PII11 pour la gouvernance de l'exactitude et de la qualité ;

1.5.10 PII12 pour la gouvernance du cycle de vie des sous-traitants, sous-traitants ultérieurs et tiers ;

1.5.11 PII13 pour l'évaluation des outils de transfert international ;

1.5.12 PII14 pour l'architecture de sécurité des PII et de contrôle d'accès ;

1.5.13 PII15 pour la gestion des incidents et violations relatifs aux PII ;

1.5.14 PII18 pour la gouvernance de la surveillance, de l'audit et de l'amélioration du PIMS ;

- 1.5.15 PII20 pour les mesures de protection propres au marketing ou au suivi visant les enfants ;
- 1.5.16 PII21 pour les contrôles de confidentialité relatifs à l'AI, au profilage et à la prise de décision individuelle automatisée ;
- 1.5.17 PII23 pour les contrôles des sous-traitants PII cloud, le cas échéant.

2. Objet

- 2.1 La présente politique a pour objet de veiller à ce que les traitements liés au marketing, aux cookies, à l'analytique, au suivi et à l'adtech soient encadrés par des enregistrements clairs des finalités, des mentions transparentes, des contrôles appropriés du consentement ou des préférences, la gestion de la suppression et du retrait, la supervision des tiers et des éléments de preuve compatibles avec les exigences d'audit.
- 2.2 La présente politique soutient la responsabilité en matière de vie privée dans les environnements B2C, fortement axés sur l'analytique, activés par l'adtech et fortement dépendants de la gestion du consentement, sans introduire de registres, de rôles ou de workflows redondants ou non canoniques.

3. Objectifs

3.1 Les objectifs de la présente politique sont les suivants :

- 3.1.1 Veiller à ce que les finalités de marketing et de suivi soient enregistrées avant le début du traitement.
- 3.1.2 Veiller à ce que les éléments de preuve relatifs au consentement, aux préférences, à la suppression et au retrait soient conservés dans des éléments de preuve canoniques.
- 3.1.3 Veiller à ce que les mentions relatives aux cookies et les mentions d'information marketing soient à jour, soumises à gestion des versions et reliées aux enregistrements de traitement.
- 3.1.4 Veiller à ce que les technologies de suivi, balises, pixels, SDKs, outils d'analytique et intégrations adtech soient approuvés avant leur utilisation en production.
- 3.1.5 Veiller à ce que les prestataires marketing, fournisseurs d'analytique et partenaires publicitaires soient classifiés et encadrés au moyen d'éléments de preuve canoniques relatifs aux relations.
- 3.1.6 Veiller à ce que les oppositions, objections, retraits et réclamations relatives au marketing direct soient routés de manière cohérente.
- 3.1.7 Veiller à ce que le circuit des transferts internationaux soit appliqué aux prestataires marketing et fournisseurs d'analytique, le cas échéant.
- 3.1.8 Veiller à ce que les contrôles relatifs aux campagnes et au suivi soient surveillés, revus et améliorés au moyen des éléments de preuve du PIMS.

4. Énoncés de politique

4.1 Inventaire des traitements marketing et de suivi

- 4.1.1 [Controller] Le Process Owner / Business Owner DOIT enregistrer dans REG02 chaque campagne marketing, canal, finalité de traitement, catégorie de PII, source d'audience, articulation avec la base légale, catégorie de technologie de suivi, dépendance à un prestataire ou à une balise, lien avec la mention d'information, dépendance au consentement ou aux préférences, lien avec la conservation et indicateur de transfert avant le début de la campagne ou de l'activité de suivi.
- 4.1.2 [Controller] Le Privacy Lead / PIMS Manager DOIT confirmer que chaque finalité marketing dans REG02 dispose d'un lien à jour avec la mention REG07 et d'un lien avec le consentement ou les préférences REG05 avant le lancement de la campagne.

- 4.1.3 [Processor] Le Process Owner / Business Owner DOIT documenter les finalités marketing approuvées par le client et les instructions du client dans REG02 ou REG08 avant de traiter des PII marketing pour le compte d'un responsable du traitement.
- 4.1.4 [Joint Controller] Le Privacy Lead / PIMS Manager DOIT enregistrer la répartition des responsabilités entre responsables conjoints du traitement dans REG08 avant de lancer une activité de marketing conjoint, d'audience partagée, de campagne comarquée ou de suivi partagé.
- 4.1.5 [Conditional] Le Privacy Lead / PIMS Manager DOIT router vers REG09 les activités marketing impliquant un prestataire international, une balise, un fournisseur d'analytique, une plateforme publicitaire, un transfert d'audience ou un transfert par partage de données avant la mise en production.
- 4.1.6 [Controller] Le Process Owner / Business Owner DOIT enregistrer dans REG05 les exigences de suppression, d'exclusion ou de non-contact associées à chaque finalité marketing avant l'activation.

4.2 Contrôles du consentement, des préférences et des cookies

- 4.2.1 [Controller] Le Process Owner / Business Owner DOIT déterminer si le consentement, une préférence, une objection, une instruction contractuelle ou une autre base approuvée est requis pour chaque canal marketing et enregistrer la décision dans REG02 et REG05 avant la collecte ou l'utilisation de la campagne.
- 4.2.2 [Controller] Le System Owner / Application Owner DOIT configurer les cookies non essentiels, balises, pixels, SDKs et technologies de suivi similaires afin qu'ils restent inactifs jusqu'à ce que l'état requis du consentement ou des préférences soit disponible dans REG05 avant le déploiement.
- 4.2.3 [Controller] Le System Owner / Application Owner DOIT valider que les signaux de consentement ou de préférence ne sont pas écrasés, contournés ou ignorés lors de modifications du site web, de l'application, de la campagne ou du gestionnaire de balises, et enregistrer les éléments de preuve de validation dans REG05 ou REG12 avant la mise en production.
- 4.2.4 [Controller] Le Process Owner / Business Owner DOIT enregistrer les éléments de preuve relatifs au consentement, aux préférences, au retrait, à la suppression et aux versions dans REG05 dans un délai d'un jour ouvré après la capture, la modification ou le retrait.
- 4.2.5 [Processor] Le System Owner / Application Owner DOIT appliquer les données de consentement, de préférence, de suppression ou d'instruction fournies par le client aux outils marketing gérés par le sous-traitant dans le délai convenu avec le client et enregistrer l'achèvement dans REG05 ou REG08.
- 4.2.6 [Conditional] Le Privacy Lead / PIMS Manager DOIT maintenir la correspondance des champs des reçus de consentement dans REG05 avant d'émettre des reçus de consentement à des fins de marketing, de cookies ou de suivi.

[... Les sections 4.3–8 ne sont pas incluses dans cet aperçu. Achetez le document complet pour accéder à l'intégralité du contenu. ...]

9. Exceptions

- 9.1 [All] Le Process Owner / Business Owner DOIT demander une exception dans REG12 avant d'utiliser tout canal marketing, balise, configuration analytique, mécanisme de préférence ou prestataire non standard lorsque les éléments de preuve requis ne peuvent pas être complétés avant le lancement.
- 9.2 [Conditional] Le Data Protection Officer / Privacy Advisor DOIT revoir une demande d'exception relative à la confidentialité marketing dans REG12 avant approbation lorsque l'exception concerne

le consentement, les enfants, les employés, les audiences sensibles, les transferts transfrontaliers, le profilage ou l'extension substantielle du suivi.

9.3 [All] Top Management DOIT approuver les exceptions à haut risque ou substantielles relatives à la confidentialité marketing dans REG12 avant leur prise d'effet.

9.4 [All] Le Privacy Lead / PIMS Manager DOIT définir dans REG12 une date d'expiration, un responsable de la remédiation et une date de revue pour chaque exception approuvée relative à la confidentialité marketing avant approbation.

10. Application de la politique

10.1 [All] Le Privacy Lead / PIMS Manager DOIT suspendre ou bloquer une activité marketing dans REG12 lorsque les éléments de preuve REG02, REG05, REG07, REG08 ou REG09 requis sont manquants avant le lancement ou la poursuite de l'utilisation.

10.2 [All] Le System Owner / Application Owner DOIT désactiver les balises, traceurs, pixels, SDKs ou flux de données de campagne non approuvés dans un délai d'un jour ouvré après une décision d'application de la politique et enregistrer l'achèvement dans REG08 ou REG12.

10.3 [All] Le Vendor / Procurement Owner DOIT bloquer l'intégration, le renouvellement ou l'extension d'un prestataire marketing, fournisseur d'analytique ou plateforme publicitaire lorsque les éléments de preuve REG08 ou REG09 requis sont manquants avant le début ou la poursuite du traitement.

10.4 [All] Le Process Owner / Business Owner DOIT arrêter l'utilisation des PII concernées dans une campagne dans un délai d'un jour ouvré après une défaillance confirmée d'un contrôle relatif aux préférences, à la suppression, aux mentions d'information ou aux prestataires, et enregistrer l'achèvement dans REG05 ou REG12.

10.5 [All] L'Internal Audit / Compliance Reviewer DOIT vérifier l'efficacité des actions correctives relatives aux non-conformités majeures ou répétées en matière de confidentialité marketing dans REG12 dans un délai de 60 jours après la clôture de l'action corrective.

11. Revue et maintenance

11.1 [All] Le Privacy Lead / PIMS Manager DOIT revoir la présente politique dans REG12 chaque année et dans un délai de 30 jours après toute modification substantielle des exigences relatives au marketing, aux cookies, au suivi, à l'analytique, à l'adtech ou à la gestion du consentement.

11.2 [Controller] Le Process Owner / Business Owner DOIT revoir les enregistrements REG02 des traitements marketing et les dépendances de préférences REG05 au moins une fois par trimestre et dans un délai de 30 jours après toute modification substantielle de campagne.

11.3 [Controller] Le Privacy Lead / PIMS Manager DOIT revoir les enregistrements REG07 des mentions d'information marketing et des mentions relatives aux cookies au moins une fois par an et dans un délai de 30 jours après toute modification substantielle de mention d'information, de suivi ou de préférence.

11.4 [All] Le Vendor / Procurement Owner DOIT revoir les enregistrements REG08 relatifs aux prestataires marketing, balises, fournisseurs d'analytique et plateformes publicitaires au moins une fois par an et avant renouvellement.

11.5 [Conditional] Le Privacy Lead / PIMS Manager DOIT mettre à jour le circuit de transfert REG09 dans un délai de 15 jours ouvrés après l'identification d'un changement de prestataire marketing, de fournisseur d'analytique ou d'emplacement d'hébergement.

11.6 [All] Top Management DOIT approuver les révisions substantielles de la présente politique dans REG12 avant publication.

12. Politiques associées

- 12.1 La présente politique est soutenue par les politiques associées suivantes :
- 12.2 PII01 - Politique du système de management des informations relatives à la vie privée
- 12.3 PII02 - Politique relative aux rôles, responsabilités et à la responsabilité en matière de vie privée
- 12.4 PII03 - Politique relative à l'inventaire des traitements de PII et aux bases légales
- 12.5 PII04 - Politique relative aux mentions d'information et à la transparence
- 12.6 PII05 - Politique de gestion du consentement et des préférences
- 12.7 PII06 - Politique de gestion des droits des personnes concernées
- 12.8 PII07 - Politique relative à l'appréciation des risques relatifs à la vie privée et à la DPIA
- 12.9 PII08 - Politique de protection de la vie privée dès la conception et par défaut
- 12.10 PII09 - Politique relative à la collecte, à l'utilisation, à la divulgation et au partage des PII
- 12.11 PII10 - Politique relative à la conservation, à la suppression et à l'élimination des PII
- 12.12 PII11 - Politique relative à l'exactitude et à la qualité des PII
- 12.13 PII12 - Politique de gestion de la protection des données pour les sous-traitants, sous-traitants ultérieurs et tiers
- 12.14 PII13 - Politique de transfert international de PII
- 12.15 PII14 - Politique de sécurité des PII et de contrôle d'accès
- 12.16 PII15 - Politique de gestion des incidents et violations relatifs aux PII
- 12.17 PII17 - Politique de gestion des informations documentées et des éléments de preuve du PIMS
- 12.18 PII18 - Politique de surveillance, d'audit et d'amélioration du PIMS
- 12.19 PII19 - Politique de confidentialité des employés
- 12.20 PII20 - Politique de confidentialité des enfants
- 12.21 PII21 - Politique de confidentialité relative à l'AI et à la prise de décision automatisée
- 12.22 PII23 - Politique relative aux sous-traitants PII cloud

13. Normes et référentiels de référence

- 13.1 La présente politique est mappée aux normes et réglementations suivantes. Le mapping explique comment la politique soutient les exigences citées et identifie les clauses internes qui les mettent en œuvre ou les soutiennent.
- 13.2 ISO/IEC 27701:2025 - Clause 7.5; Clause 8.1. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.2.4; 4.3.1; 4.4.1; 4.5.1; 4.7.1; 7.1; 7.2; 7.6; 11.1].
- 13.3 ISO/IEC 27701:2025 - Clause 9.1; Clause 10.2. Addressed by clauses [4.3.6; 4.5.5; 4.6.5; 4.7.4; 6.1; 6.5; 8.1; 8.2; 8.3; 8.4; 8.5; 10.5; 11.1].
- 13.4 ISO/IEC 27701:2025 - Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.4; Annex A.1.2.5; Annex A.1.2.9. Addressed by clauses [4.1.1; 4.1.2; 4.1.6; 4.2.1; 4.2.4; 4.2.6; 4.5.1; 4.7.2; 7.1; 11.2].
- 13.5 ISO/IEC 27701:2025 - Annex A.1.2.7; Annex A.1.2.8. Addressed by clauses [4.1.4; 4.4.2; 4.4.3; 4.4.5; 5.6; 6.4; 7.5; 11.4].
- 13.6 ISO/IEC 27701:2025 - Annex A.1.3.2; Annex A.1.3.3; Annex A.1.3.4; Annex A.1.3.5. Addressed by clauses [4.2.2; 4.2.3; 4.2.4; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 7.3; 11.3].
- 13.7 ISO/IEC 27701:2025 - Annex A.1.3.6; Annex A.1.3.10. Addressed by clauses [4.5.2; 4.5.3; 4.6.1; 4.6.2; 4.6.3; 4.6.4; 4.6.5; 7.2].
- 13.8 ISO/IEC 27701:2025 - Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5. Addressed by clauses [4.1.1; 4.2.2; 4.4.4; 4.5.1; 4.5.2; 4.5.4; 4.5.5; 4.7.2; 7.2].

- 13.9 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 [4.1.5; 4.4.3; 4.4.6; 7.5; 11.5].
- 13.10 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 [4.1.3; 4.2.5; 4.3.4; 4.4.5; 7.4].
- 13.11 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 [4.2.5; 4.3.4; 4.4.6; 4.6.3; 7.4; 7.5].
- 13.12 ISO/IEC 27701:2025 - Annex A.3.14; Annex A.3.25. Addressed by clauses [4.2.3; 4.4.4; 4.7.1; 4.7.3; 5.7; 7.2; 10.2].
- 13.13 GDPR - Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(2). Addressed by clauses [4.1.1; 4.1.2; 4.1.6; 4.5.1; 4.5.2; 4.7.2; 8.1].
- 13.14 GDPR - Article 6; Article 7. Addressed by clauses [4.2.1; 4.2.2; 4.2.4; 4.2.6; 4.6.2; 7.2].
- 13.15 GDPR - Article 12; Article 13; Article 14. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.3.5; 11.3].
- 13.16 GDPR - Article 21. Addressed by clauses [4.5.2; 4.6.1; 4.6.2; 4.6.4; 8.3].
- 13.17 GDPR - Article 24; Article 25; Article 26; Article 28; Article 30; Article 32. Addressed by clauses [4.1.3; 4.1.4; 4.4.2; 4.4.3; 4.4.5; 4.5.5; 4.7.3; 5.6; 5.7; 6.2; 6.4; 8.4; 10.3].
- 13.18 GDPR - Article 44. Addressed by clauses [4.1.5; 4.4.6; 7.5; 11.5].
- 13.19 ISO/IEC 29100:2020 - Clause 5.1; Clause 5.8; Clause 5.9. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.3.1; 4.3.3; 4.6.1; 4.6.2].
- 13.20 ISO/IEC 29100:2020 - Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6. Addressed by clauses [4.1.1; 4.1.2; 4.5.1; 4.5.2; 4.5.4; 4.7.2].
- 13.21 ISO/IEC 29100:2020 - Clause 5.10; Clause 5.11; Clause 5.12. Addressed by clauses [4.3.6; 4.5.5; 4.6.5; 4.7.1; 4.7.3; 4.7.4; 6.1; 8.5; 10.5].
- 13.22 ISO/IEC 29151:2022 - Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.10. Addressed by clauses [4.2.1; 4.2.2; 4.2.4; 4.5.1; 4.5.2; 4.6.1; 4.6.2; 7.2].
- 13.23 ISO/IEC TS 27560:2023 - Clause 5.2; Clause 5.3; Clause 6.2; Clause 6.4. Addressed by clauses [4.2.4; 4.2.6; 7.1; 7.2].