					Šeit ievadiet reģistrētās juridiskās personas nosaukumu							
Dokumenta numurs: PII22					Dokumenta nosaukums: **Mārketinga privātuma un sīkdatņu politika**							
Versija: 1.0		Spēkā stāšanās datums: 01.01.2025			Dokumenta īpašnieks:							
X	Politika		Standarts		Procedūra		Veidlapa		Reģistrs		Cits	

Pārskatījumu vēsture				
Pārskatījuma numurs	**Pārskatījuma datums**	**Izmaiņas**	**Pārskatīja**	**Procesa īpašnieks**

Apstiprinājumi			
Vārds	**Amats**	**Datums**	**Paraksts**

Saskaņots ar piemērojamiem standartiem un regulējumu

Standarts/regulējums	Punkts/kontrole/pants	Piemērojamība	Pārklājuma veids	Piezīme
ISO/IEC 27701:2025	Clause 7.5; Clause 8.1	Both	Primary	Dokumentēti mārketinga privātuma pierādījumi un darbības kontroles pasākumi
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Uzraudzība, neatbilstības un korektīvās darbības
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	Mārketinga nolūki, sasaiste ar tiesisko pamatu, piekrišana un apstrādes ieraksti
ISO/IEC 27701:2025	Annex A.1.2.7; Annex A.1.2.8	Controller	Supporting	Mārketinga apstrādātāji un kopīgu pārziņu atbildība
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	Mārketinga paziņojumi, sīkdatņu paziņojumi un informācija par piekrišanas atsaukšanu
ISO/IEC 27701:2025	Annex A.1.3.6; Annex A.1.3.10	Controller	Supporting	Iebildumu un pieprasījumu apstrādes novirzīšana tiešajam mārketingam
ISO/IEC 27701:2025	Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5	Controller	Primary	Vākšana, apstrāde un minimizēšana mārketingam un izsekošanai
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	Nosūtīšanas un izpaušanas novirzīšana adtech un analītikas vajadzībām
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	Apstrādātāja vienošanās, norādījumi, klienta atbalsts un apstrādātāja ieraksti
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	Apstrādātāja atbalsts pienākumiem, nosūtīšanas un izpaušanas novirzīšanai
ISO/IEC 27701:2025	Annex A.3.14; Annex A.3.25	Both	Supporting	Ierakstu aizsardzība un žurnālfiksēšanas pierādījumi izsekošanas izmaiņām
GDPR	Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(2)	Controller	Primary	Godprātība, pārredzamība, nolūka ierobežojums, minimizēšana un pārskatatbildība

GDPR	Article 6; Article 7	Controller	Primary	Likumīgums un piekrišanas nosacījumi
GDPR	Article 12; Article 13; Article 14	Controller	Primary	Pārredzama informācija un paziņojumi
GDPR	Article 21	Controller	Primary	Iebildumi pret tiešo mārketingu un atteikšanās novirzīšana
GDPR	Article 24; Article 25; Article 26; Article 28; Article 30; Article 32	Both	Supporting	Pārskatatbildība, projektēšana/noklusējums, kopīgi pārziņi, apstrādātāji, ieraksti un drošības atbalsts
GDPR	Article 44	Conditional	Referenced	Starptautiskas nosūtīšanas novirzīšana mārketinga piegādātājiem
ISO/IEC 29100:2020	Clause 5.1; Clause 5.8; Clause 5.9	Both	Primary	Piekrišana un izvēle, pārredzamība un līdzdalība
ISO/IEC 29100:2020	Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Both	Primary	Nolūks, vākšana, minimizēšana, izmantošanas un izpaušanas ierobežojums
ISO/IEC 29100:2020	Clause 5.10; Clause 5.11; Clause 5.12	Both	Supporting	Pārskatatbildība, informācijas drošība un atbilstība
ISO/IEC 29151:2022	Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.10	Both	Supporting	Piekrišanas, nolūka, vākšanas, minimizēšanas, izmantošanas/izpaušanas un līdzdalības kontroles pasākumi
ISO/IEC TS 27560:2023	Clause 5.2; Clause 5.3; Clause 6.2; Clause 6.4	Controller	Supporting	Piekrišanas ieraksta un kvīts struktūra, ja tiek izmantota

1. Piemērošanas joma

1.1 Šī politika nosaka obligātās privātuma prasības mārketingam, sīkdatnēm, izsekošanas tehnoloģijām, analītikai, reklāmas tehnoloģijām, auditorijas segmentācijai, tiešajam mārketingam, preferenču pārvaldībai, apspiešanai, trešo pušu tagiem, kampaņu pārskatīšanai un saistītai PII apstrādei.

1.2 Šī politika attiecas uz pārziņa, kopīga pārziņa, apstrādātāja un apakšapstrādātāja kontekstiem. Pārziņa pienākumi ir piemērojami, ja organizācija nosaka mārketinga nolūkus un līdzekļus. Apstrādātāja un apakšapstrādātāja pienākumi ir piemērojami tikai tad, ja organizācija apstrādā mārketinga, analītikas, izsekošanas vai ar kampaņām saistītu PII saskaņā ar dokumentētiem klienta vai augšupējā apstrādātāja norādījumiem.

1.3 Šī politika aptver:

1.3.1 mārketinga apstrādes uzskaiti un nolūku sasaisti;

1.3.2 piekrišanas un preferenču pierādījumus mārketingam un izsekošanai;

1.3.3 sīkdatņu, izsekošanas tehnoloģiju un tagu pārvaldību;

1.3.4 mārketinga privātuma paziņojuma un sīkdatņu paziņojuma ierakstus;

1.3.5 apspiešanas, atsaukšanas un atteikšanās novirzīšanu;

1.3.6 mārketinga piegādātāju, analītikas pakalpojumu sniedzēju un adtech attiecību pārvaldību;

1.3.7 starptautiskas nosūtīšanas novirzīšanu mārketinga piegādātājiem un platformām;

1.3.8 kampaņu pārskatīšanas un uzraudzības pierādījumus.

1.4 Šī politika neizveido atsevišķu sīkdatņu reģistru, tagu reģistru, apspiešanas reģistru, mārketinga kampaņu reģistru, analītikas reģistru, juridisko konsultāciju darbplūsmu, komiteju, informācijas paneli, veidlapu vai nekanonisku lomu.

1.5 Šī politika neaizstāj:

1.5.1 PII03 apstrādes uzskaitei un atbildībai par tiesisko pamatu;

1.5.2 PII04 vispārējai privātuma paziņojumu pārvaldībai;

1.5.3 PII05 piekrišanas un preferenču pārvaldībai;

1.5.4 PII06 datu subjekta tiesību īstenošanas pieprasījumu darbplūsmai;

1.5.5 PII07 privātuma risku izvērtēšanas un DPIA metodoloģijai;

1.5.6 PII08 datu aizsardzības pēc projektēšanas un pēc noklusējuma vārtiem;

1.5.7 PII09 vispārējiem vākšanas, izmantošanas, izpaušanas un koplietošanas kontroles pasākumiem;

1.5.8 PII10 glabāšanas, dzēšanas un likvidēšanas izpildei;

1.5.9 PII11 precizitātes un kvalitātes pārvaldībai;

1.5.10 PII12 apstrādātāju, apakšapstrādātāju un trešo pušu dzīves cikla pārvaldībai;

1.5.11 PII13 starptautiskas nosūtīšanas mehānisma izvērtēšanai;

1.5.12 PII14 PII drošības un piekļuves kontroles arhitektūrai;

1.5.13 PII15 PII incidentu un pārkāpumu apstrādei;

1.5.14 PII18 PIMS uzraudzības, audita un uzlabojumu pārvaldībai;

1.5.15 PII20 bērniem specifiskiem mārketinga vai izsekošanas aizsardzības pasākumiem;

1.5.16 PII21 AI, profilēšanas un automatizētas lēmumu pieņemšanas privātuma kontroles pasākumiem;

1.5.17 PII23 mākoņa PII apstrādātāja kontroles pasākumiem, ja piemērojams.

2. Mērķis

2.1 Šīs politikas mērķis ir nodrošināt, ka mārketinga, sīkdatņu, analītikas, izsekošanas un adtech apstrāde tiek pārvaldīta, izmantojot skaidrus nolūku ierakstus, pārredzamu paziņojumu, atbilstošus piekrišanas vai preferenču kontroles pasākumus, apspiešanas un atsaukšanas apstrādi, trešo pušu pārraudzību un auditam gatavus pierādījumus.

2.2 Šī politika atbalsta privātuma pārskatatbildību B2C, intensīvas analītikas, adtech iespējotās un piekrišanas pārvaldībā intensīvās vidēs, neieviešot nekanoniskus reģistrus, lomas vai dublējošas darbplūsmas.

3. Mērķi

3.1 Šīs politikas mērķi ir:

3.1.1 Nodrošināt, ka mārketinga un izsekošanas nolūki tiek reģistrēti pirms apstrādes sākšanas.

3.1.2 Nodrošināt, ka piekrišanas, preferenču, apspiešanas un atsaukšanas pierādījumi tiek uzturēti kanoniskajos pierādījumu objektos.

3.1.3 Nodrošināt, ka sīkdatņu paziņojumi un mārketinga paziņojumi ir aktuāli, pārvaldīti ar versiju kontroli un sasaistīti ar apstrādes ierakstiem.

3.1.4 Nodrošināt, ka izsekošanas tehnoloģijas, tagi, pikseļi, SDKs, analītikas rīki un adtech integrācijas tiek apstiprinātas pirms izmantošanas ražošanas vidē.

3.1.5 Nodrošināt, ka mārketinga piegādātāji, analītikas pakalpojumu sniedzēji un reklāmas partneri tiek klasificēti un pārvaldīti, izmantojot kanoniskus attiecību pierādījumus.

3.1.6 Nodrošināt, ka atteikšanās, iebildumi, atsaukumi un tiešā mārketinga sūdzības tiek novirzītas konsekventi.

3.1.7 Nodrošināt, ka starptautiskas nosūtīšanas novirzīšana tiek veikta mārketinga piegādātājiem un analītikas pakalpojumu sniedzējiem, ja piemērojams.

3.1.8 Nodrošināt, ka kampaņu un izsekošanas kontroles pasākumi tiek uzraudzīti, pārskatīti un uzlaboti, izmantojot PIMS pierādījumus.

4. Politikas nostādnes

4.1 Mārketinga un izsekošanas apstrādes uzskaite

4.1.1 [Controller] Process Owner / Business Owner jāreģistrē katra mārketinga kampaņa, kanāls, apstrādes nolūks, PII kategorija, auditorijas avots, sasaiste ar tiesisko pamatu, izsekošanas tehnoloģijas kategorija, piegādātāja vai taga atkarība, paziņojuma sasaiste, piekrišanas vai preferenču atkarība, glabāšanas sasaiste un nosūtīšanas pazīme REG02 pirms kampaņas vai izsekošanas darbības sākšanas.

4.1.2 [Controller] Privacy Lead / PIMS Manager jāapstiprina, ka katram mārketinga nolūkam REG02 ir aktuāla REG07 paziņojuma sasaiste un REG05 piekrišanas vai preferenču sasaiste pirms kampaņas sākšanas.

4.1.3 [Processor] Process Owner / Business Owner jādokumentē klienta apstiprinātie mārketinga nolūki un klienta norādījumi REG02 vai REG08 pirms mārketinga PII apstrādes pārziņa vārdā.

4.1.4 [Joint Controller] Privacy Lead / PIMS Manager jāreģistrē kopīgu pārziņu atbildības sadalījums REG08 pirms kopīga mārketinga, koplietotas auditorijas, kopzīmola kampaņas vai koplietotas izsekošanas darbības sākšanas.

4.1.5 [Conditional] Privacy Lead / PIMS Manager jānovirza mārketinga darbības, kurās iesaistīts starptautisks piegādātājs, tags, analītikas pakalpojumu sniedzējs, reklāmas platforma, auditorijas nosūtīšana vai datu koplietošanas nosūtīšana, uz REG09 pirms nodošanas ražošanas vidē.

4.1.6 [Controller] Process Owner / Business Owner jāreģistrē apspiešanas, izslēgšanas vai nesazināšanās prasības, kas saistītas ar katru mārketinga nolūku, REG05 pirms aktivizēšanas.

4.2 Piekrišanas, preferenču un sīkdatņu kontroles pasākumi

4.2.1 [Controller] Process Owner / Business Owner jānosaka, vai katram mārketinga kanālam ir nepieciešama piekrišana, preference, iebildums, līgumisks norādījums vai cits apstiprināts pamats, un jāreģistrē lēmums REG02 un REG05 pirms vākšanas vai izmantošanas kampaņā.

4.2.2 [Controller] System Owner / Application Owner jākonfigurē nebūtiskas sīkdatnes, tagi, pikseļi, SDKs un līdzīgas izsekošanas tehnoloģijas tā, lai tās paliktu neaktīvas, līdz REG05 ir pieejams nepieciešamais piekrišanas vai preferenču statuss, pirms izvietošanas.

4.2.3 [Controller] System Owner / Application Owner jāvalidē, ka piekrišanas vai preferenču signāli netiek pārrakstīti, apieti vai ignorēti tīmekļvietnes, lietotnes, kampaņas vai tagu pārvaldnieka izmaiņu laikā, un validācijas pierādījumi jāreģistrē REG05 vai REG12 pirms laidiena.

4.2.4 [Controller] Process Owner / Business Owner jāreģistrē piekrišanas, preferenču, atsaukšanas, apspiešanas un versijas pierādījumi REG05 vienas darbdienas laikā pēc fiksēšanas, izmaiņas vai atsaukšanas.

4.2.5 [Processor] System Owner / Application Owner jāpiemēro klienta nodrošinātie piekrišanas, preferenču, apspiešanas vai norādījumu dati apstrādātāja pārvaldītajiem mārketinga rīkiem klienta saskaņotajā termiņā un jāreģistrē pabeigšana REG05 vai REG08.

4.2.6 [Conditional] Privacy Lead / PIMS Manager jāuztur piekrišanas kvīts lauku kartēšana REG05 pirms piekrišanas kvīšu izsniegšanas mārketinga, sīkdatņu vai izsekošanas nolūkiem.

[... Sadaļas 4.3–8 nav iekļautas šajā priekšskatījumā. Iegādājieties pilnu dokumentu, lai piekļūtu pilnam saturam. ...]

9. Izņēmumi

9.1 [All] Process Owner / Business Owner jāpieprasa izņēmums REG12 pirms jebkura nestandarta mārketinga kanāla, taga, analītikas konfigurācijas, preferenču mehānisma vai piegādātāja izmantošanas, ja nepieciešamos pierādījumus nav iespējams pabeigt pirms sākšanas.

9.2 [Conditional] Data Protection Officer / Privacy Advisor jāpārskata mārketinga privātuma izņēmuma pieprasījums REG12 pirms apstiprināšanas, ja izņēmums skar piekrišanu, bērnus, darbiniekus, sensitīvas auditorijas, pārrobežu nosūtīšanu, profilēšanu vai būtisku izsekošanas paplašināšanu.

9.3 [All] Top Management jāapstiprina augsta riska vai būtiski mārketinga privātuma izņēmumi REG12 pirms izņēmuma stāšanās spēkā.

9.4 [All] Privacy Lead / PIMS Manager katram apstiprinātam mārketinga privātuma izņēmumam REG12 jānosaka termiņa beigu datums, trūkumu novēršanas īpašnieks un pārskatīšanas datums pirms apstiprināšanas.

10. Piemērošana

10.1 [All] Privacy Lead / PIMS Manager jāaptur vai jābloķē mārketinga darbība REG12, ja pirms sākšanas vai turpmākas izmantošanas trūkst nepieciešamo REG02, REG05, REG07, REG08 vai REG09 pierādījumu.

10.2 [All] System Owner / Application Owner jāatspējo neapstiprināti tagi, izsekotāji, pikseļi, SDKs vai kampaņu datu plūsmas vienas darbdienas laikā pēc piemērošanas lēmuma un pabeigšana jāreģistrē REG08 vai REG12.

10.3 [All] Vendor / Procurement Owner jābloķē mārketinga piegādātāja, analītikas pakalpojumu sniedzēja vai reklāmas platformas sākotnējā piesaiste, atjaunošana vai paplašināšana, ja pirms apstrādes sākšanas vai turpināšanas trūkst nepieciešamo REG08 vai REG09 pierādījumu.

10.4 [All] Process Owner / Business Owner jāaptur ietekmētās PII izmantošana kampaņā vienas darbdienas laikā pēc apstiprinātas preferenču, apspiešanas, paziņojuma vai piegādātāja kontroles kļūmes un pabeigšana jāreģistrē REG05 vai REG12.

10.5 [All] Internal Audit / Compliance Reviewer jāpārbauda korektīvās darbības efektivitāte būtisku vai atkārtotu mārketinga privātuma neatbilstību gadījumā REG12 60 dienu laikā pēc korektīvās darbības slēgšanas.

11. Pārskatīšana un uzturēšana

11.1 [All] Privacy Lead / PIMS Manager jāpārskata šī politika REG12 reizi gadā un 30 dienu laikā pēc būtiskas izmaiņas mārketinga, sīkdatņu, izsekošanas, analītikas, adtech vai piekrišanas pārvaldības prasībās.

11.2 [Controller] Process Owner / Business Owner jāpārskata REG02 mārketinga apstrādes ieraksti un REG05 preferenču atkarības vismaz reizi ceturksnī un 30 dienu laikā pēc būtiskas kampaņas izmaiņas.

11.3 [Controller] Privacy Lead / PIMS Manager jāpārskata REG07 mārketinga paziņojuma un sīkdatņu paziņojuma ieraksti vismaz reizi gadā un 30 dienu laikā pēc būtiskas paziņojuma, izsekošanas vai preferenču izmaiņas.

11.4 [All] Vendor / Procurement Owner jāpārskata REG08 mārketinga piegādātāju, tagu, analītikas un reklāmas platformu ieraksti vismaz reizi gadā un pirms atjaunošanas.

11.5 [Conditional] Privacy Lead / PIMS Manager jāatjaunina REG09 nosūtīšanas novirzīšana 15 darbdienu laikā pēc identificētas mārketinga piegādātāja, analītikas pakalpojumu sniedzēja vai mitināšanas vietas izmaiņas.

11.6 [All] Top Management jāapstiprina būtiski šīs politikas grozījumi REG12 pirms publicēšanas.

12. Saistītās politikas

12.1 Šo politiku atbalsta šādas saistītās politikas:

12.2 PII01 - Privātuma informācijas pārvaldības sistēmas politika

12.3 PII02 - Privātuma lomu, pienākumu un pārskatatbildības politika

12.4 PII03 - PII apstrādes uzskaites un tiesiskā pamata politika

12.5 PII04 - Privātuma paziņojumu un pārredzamības politika

12.6 PII05 - Piekrišanas un preferenču pārvaldības politika

12.7 PII06 - Datu subjektu tiesību pārvaldības politika

12.8 PII07 - Privātuma risku izvērtēšanas un DPIA politika

12.9 PII08 - Datu aizsardzības pēc projektēšanas un pēc noklusējuma politika

12.10 PII09 - PII vākšanas, izmantošanas, izpaušanas un koplietošanas politika

12.11 PII10 - PII glabāšanas, dzēšanas un likvidēšanas politika

12.12 PII11 - PII precizitātes un kvalitātes politika

12.13 PII12 - Apstrādātāju, apakšapstrādātāju un trešo pušu privātuma pārvaldības politika

12.14 PII13 - Starptautiskas PII nosūtīšanas politika

12.15 PII14 - PII drošības un piekļuves kontroles politika

12.16 PII15 - PII incidentu un pārkāpumu pārvaldības politika

12.17 PII17 - PIMS dokumentētas informācijas un pierādījumu pārvaldības politika

12.18 PII18 - PIMS uzraudzības, audita un uzlabošanas politika

12.19 PII19 - Darbinieku privātuma politika

12.20 PII20 - Bērnu privātuma politika

12.21 PII21 - AI un automatizētas lēmumu pieņemšanas privātuma politika

12.22 PII23 - Mākoņa PII apstrādātāja politika

13. Atsauces standarti un ietvari

13.1 Šī politika ir kartēta uz turpmāk norādītajiem standartiem un regulējumiem. Kartējums izskaidro, kā politika atbalsta citētās prasības, un identificē iekšējos punktus, kas tās ievieš vai atbalsta.

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].