

				Sem vnesite naziv registrirane pravne osebe							
Številka dokumenta: PII22				Naslov dokumenta: <b>Politika zasebnosti pri trženju in piškotkih</b>							
Različica: 1.0		Datum začetka veljavnosti: 01.01.2025		Lastnik dokumenta:							
X	Politika		Standard		Postopek		Obrazec		Register		Drugo

Zgodovina revizij				
Številka revizije	Datum revizije	Spremembe	Pregledal	Lastnik procesa

Odobritve			
Ime	Delovno mesto	Datum	Podpis

<p><b>Pravno obvestilo (avtorske pravice in omejitve uporabe)</b>  (C) 2025 Clarysec LLC. All rights reserved.</p> <p>Ta dokument je intelektualna lastnina družbe Clarysec LLC. Noben del tega dokumenta se ne sme kopirati, ponovno uporabiti, distribuirati ali spreminjati za komercialne ali implementacijske namene brez predhodnega izrecnega pisnega dovoljenja.</p> <p>Nepooblaščen uporaba je strogo prepovedana in lahko povzroči pravne ukrepe.</p> <p>Za licenciranje se obrnite na: <a href="mailto:info@clarysec.com">info@clarysec.com</a></p>
--

## Usklajenost s standardi in predpisi

Standard / Regulation	Clause / Control / Article	Applicability	Coverage Type	Comment
ISO/IEC 27701:2025	Clause 7.5; Clause 8.1	Both	Primary	Dokumentirana dokazila o zasebnosti pri trženju in operativna kontrola
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Spremljanje, neskladnosti in korektivni ukrepi
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	Nameni trženja, povezava s pravno podlago, privolitve in evidence dejavnosti obdelave
ISO/IEC 27701:2025	Annex A.1.2.7; Annex A.1.2.8	Controller	Supporting	Obdelovalci za trženje in odgovornosti skupnih upravljavcev
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	Obvestila za trženje, obvestila o piškotkih in informacije o preklicu privolitve
ISO/IEC 27701:2025	Annex A.1.3.6; Annex A.1.3.10	Controller	Supporting	Usmerjanje ugovorov in obravnave zahtev za neposredno trženje
ISO/IEC 27701:2025	Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5	Controller	Primary	Zbiranje, obdelava in minimizacija za trženje in sledenje
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	Usmerjanje prenosov in razkritij za oglaševalsko tehnologijo in analitiko
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	Pogodba z obdelovalcem, navodila, podpora naročniku in evidence obdelovalca

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	Podpora obdelovalca pri obveznostih ter usmerjanje prenosov in razkritij
ISO/IEC 27701:2025	Annex A.3.14; Annex A.3.25	Both	Supporting	Zaščita evidenc in dokazila o beleženju sprememb pri sledenju
GDPR	Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(2)	Controller	Primary	Poštenost, preglednost, omejitev namena, minimizacija in odgovornost
GDPR	Article 6; Article 7	Controller	Primary	Zakonitost in pogoji za privolitev
GDPR	Article 12; Article 13; Article 14	Controller	Primary	Pregledne informacije in obvestila
GDPR	Article 21	Controller	Primary	Ugovor neposrednemu trženju in usmerjanje odjav
GDPR	Article 24; Article 25; Article 26; Article 28; Article 30; Article 32	Both	Supporting	Odgovornost, vgrajeno in privzeto varstvo podatkov, skupni upravljavci, obdelovalci, evidence in varnostna podpora
GDPR	Article 44	Conditional	Referenced	Usmerjanje mednarodnih prenosov za dobavitelje na področju trženja
ISO/IEC 29100:2020	Clause 5.1; Clause 5.8; Clause 5.9	Both	Primary	Privolitev in izbira, preglednost in sodelovanje
ISO/IEC 29100:2020	Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Both	Primary	Omejitev namena, zbiranja, minimizacije, uporabe in razkritja
ISO/IEC 29100:2020	Clause 5.10; Clause 5.11; Clause 5.12	Both	Supporting	Odgovornost, informacijska varnost in skladnost

ISO/IEC 29151:2022	Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.10	Both	Supporting	Kontrole privolitve, namena, zbiranja, minimizacije, uporabe/razkritja in sodelovanja
ISO/IEC TS 27560:2023	Clause 5.2; Clause 5.3; Clause 6.2; Clause 6.4	Controller	Supporting	Struktura evidence in potrdila o privolitvi, kadar se uporablja

## 1. Področje uporabe

- 1.1 Ta politika določa obvezne zahteve glede zasebnosti za trženje, piškotke, sledilne tehnologije, analitiko, oglaševalsko tehnologijo, segmentacijo občinstva, neposredno trženje, upravljanje preferenc, izključitve, oznake tretjih oseb, pregled kampanj in povezavo obdelavo PII.
- 1.2 Ta politika se uporablja v kontekstih upravljavca, skupnega upravljavca, obdelovalca in podobdelovalca.
- 1.3 Obveznosti upravljavca veljajo, kadar organizacija določa namene in sredstva trženja.
- 1.4 Obveznosti obdelovalca in podobdelovalca veljajo samo, kadar organizacija obdeluje PII, povezane s trženjem, analitiko, sledenjem ali kampanjami, na podlagi dokumentiranih navodil naročnika ali nadrejenega obdelovalca.

### 1.5 Ta politika zajema:

- 1.5.1 popis dejavnosti obdelave za trženje in povezavo namenov;
  - 1.5.2 dokazila o privolitvi in preferencah za trženje in sledenje;
  - 1.5.3 upravljanje piškotkov, sledilnih tehnologij in oznak;
  - 1.5.4 evidence obvestil o zasebnosti pri trženju in obvestil o piškotkih;
  - 1.5.5 usmerjanje izključitev, preklicev in odjav;
  - 1.5.6 upravljanje razmerij z dobavitelji za trženje, ponudniki analitike in oglaševalsko tehnologijo;
  - 1.5.7 usmerjanje mednarodnih prenosov za dobavitelje in platforme za trženje;
  - 1.5.8 dokazila o pregledu kampanj in spremljanju.
- 1.6 Ta politika ne ustvarja ločenega registra piškotkov, registra oznak, registra izključitev, registra trženjskih kampanj, registra analitike, delovnega toka za pravno svetovanje, odbora, nadzorne plošče, obrazca ali nekanonične vloge.

### 1.7 Ta politika ne nadomešča:

- 1.7.1 PII03 za popis dejavnosti obdelave in lastništvo pravne podlage;
- 1.7.2 PII04 za splošno upravljanje obvestil o zasebnosti;
- 1.7.3 PII05 za upravljanje privolitev in preferenc;
- 1.7.4 PII06 za delovni tok zahtev PII principal za uveljavljanje pravic;
- 1.7.5 PII07 za metodologijo ocene tveganj za zasebnost in DPIA;
- 1.7.6 PII08 za kontrolne točke vgrajenega in privzetega varstva zasebnosti;
- 1.7.7 PII09 za splošne kontrole zbiranja, uporabe, razkritja in deljenja;
- 1.7.8 PII10 za izvajanje hrambe, izbrisa in odstranjevanja;
- 1.7.9 PII11 za upravljanje točnosti in kakovosti;
- 1.7.10 PII12 za upravljanje življenjskega cikla obdelovalcev, podobdelovalcev in tretjih oseb;
- 1.7.11 PII13 za presojo mehanizmov mednarodnega prenosa;
- 1.7.12 PII14 za varnostno arhitekturo in nadzor dostopa za PII;
- 1.7.13 PII15 za obravnavanje incidentov in kršitev v zvezi s PII;
- 1.7.14 PII18 za upravljanje spremljanja, presoje in izboljševanja PIMS;
- 1.7.15 PII20 za zaščitne ukrepe pri trženju ali sledenju, posebej namenjenem otrokom;
- 1.7.16 PII21 za kontrole zasebnosti pri AI, oblikovanju profilov in avtomatiziranem sprejemanju odločitev;
- 1.7.17 PII23 za kontrole obdelovalcev PII v oblaku, kadar je to primerno.

## 2. Namen

- 2.1 Namen te politike je zagotoviti, da se trženje, piškotki, analitika, sledenje in obdelava z oglaševalsko tehnologijo upravljajo prek jasnih evidenc namenov, preglednih obvestil, ustreznih kontrol privolitve ali preferenc, obravnave izključitev in preklicev, nadzora tretjih oseb ter dokazil, pripravljenih za presojo.
- 2.2 Ta politika podpira odgovornost za zasebnost v okoljih B2C, okoljih z intenzivno analitiko, okoljih z oglaševalsko tehnologijo in okoljih z intenzivnim upravljanjem privolitve, ne da bi uvajala nekanonične registre, vloge ali podvojene delovne tokove.

### 3. Cilji

#### 3.1 Cilji te politike so:

- 3.1.1 Zagotoviti, da so nameni trženja in sledenja evidentirani pred začetkom obdelave.
- 3.1.2 Zagotoviti, da se dokazila o privolitvi, preferencah, izključitvah in preklicih hranijo v kanoničnih dokaznih objektih.
- 3.1.3 Zagotoviti, da so obvestila o piškotkih in obvestila za trženje ažurna, upravljana z različicami in povezana z evidencami dejavnosti obdelave.
- 3.1.4 Zagotoviti, da so sledilne tehnologije, oznake, piksli, SDKs, analitična orodja in integracije oglaševalske tehnologije odobreni pred uporabo v produkciji.
- 3.1.5 Zagotoviti, da so dobavitelji za trženje, ponudniki analitike in oglaševalski partnerji razvrščeni in upravljani prek kanoničnih dokazil o razmerjih.
- 3.1.6 Zagotoviti dosledno usmerjanje odjav, ugovorov, preklicev in pritožb glede neposrednega trženja.
- 3.1.7 Zagotoviti usmerjanje mednarodnih prenosov za dobavitelje za trženje in ponudnike analitike, kadar je to primerno.
- 3.1.8 Zagotoviti, da se kontrole kampanj in sledenja spremljajo, pregledujejo in izboljšujejo z uporabo dokazil PIMS.

### 4. Izjave politike

#### 4.1 Popis dejavnosti obdelave za trženje in sledenje

- 4.1.1 [Controller] Process Owner / Business Owner mora pred začetkom kampanje ali dejavnosti sledenja v REG02 evidentirati vsako trženjsko kampanjo, kanal, namen obdelave, kategorijo PII, vir občinstva, povezavo s pravno podlago, kategorijo sledilne tehnologije, odvisnost od dobavitelja ali oznake, povezavo z obvestilom, odvisnost od privolitve ali preference, povezavo s hrambo in oznako prenosa.
- 4.1.2 [Controller] Privacy Lead / PIMS Manager mora pred začetkom kampanje potrditi, da ima vsak namen trženja v REG02 aktualno povezavo z obvestilom REG07 ter povezavo s privolitvijo ali preferenco REG05.
- 4.1.3 [Processor] Process Owner / Business Owner mora pred obdelavo PII za trženje v imenu upravljavca v REG02 ali REG08 dokumentirati namene trženja, ki jih je odobril naročnik, in navodila naročnika.
- 4.1.4 [Joint Controller] Privacy Lead / PIMS Manager mora pred začetkom skupnega trženja, dejavnosti s skupnim občinstvom, skupno označene kampanje ali skupne dejavnosti sledenja v REG08 evidentirati razdelitev odgovornosti skupnih upravljavcev.
- 4.1.5 [Conditional] Privacy Lead / PIMS Manager mora trženjske dejavnosti, ki vključujejo mednarodnega dobavitelja, oznako, ponudnika analitike, oglaševalsko platformo, prenos občinstva ali prenos z deljenjem podatkov, pred prehodom v produkcijo usmeriti v REG09.
- 4.1.6 [Controller] Process Owner / Business Owner mora pred aktivacijo v REG05 evidentirati zahteve glede izključitev, izvzetij ali prepovedi stika, povezane z vsakim namenom trženja.

#### 4.2 Kontrole privolitve, preferenc in piškotkov

- 4.2.1 [Controller] Process Owner / Business Owner mora pred zbiranjem ali uporabo v kampanji ugotoviti, ali je za vsak trženjski kanal potrebna privolitve, preferenca, ugovor, pogodbeno navodilo ali druga odobrena podlaga, ter odločitev evidentirati v REG02 in REG05.
- 4.2.2 [Controller] System Owner / Application Owner mora nebitvene piškotke, oznake, piksele, SDKs in podobne sledilne tehnologije konfigurirati tako, da ostanejo neaktivni, dokler pred uvedbo ni v REG05 na voljo zahtevano stanje privolitve ali preferenc.
- 4.2.3 [Controller] System Owner / Application Owner mora preveriti, da se signali privolitve ali preferenc med spremembami spletnega mesta, aplikacije, kampanje ali upravljalnika oznak ne prepišejo, zaobidejo ali prezrejo, ter pred izdajo evidentirati dokazila o validaciji v REG05 ali REG12.
- 4.2.4 [Controller] Process Owner / Business Owner mora dokazila o privolitvi, preferenci, preklicu, izključitvi in različici evidentirati v REG05 v enem delovnem dnevu po zajemu, spremembi ali preklicu.
- 4.2.5 [Processor] System Owner / Application Owner mora podatke o privolitvah, preferencah, izključitvah ali navodilih, ki jih zagotovi naročnik, uporabiti v trženjskih orodjih, ki jih upravlja obdelovalec, v roku, dogovorjenem z naročnikom, ter dokončanje evidentirati v REG05 ali REG08.
- 4.2.6 [Conditional] Privacy Lead / PIMS Manager mora pred izdajanjem potrdil o privolitvi za namene trženja, piškotkov ali sledenja v REG05 vzdrževati preslikavo polj potrdila o privolitvi.

[ ... Razdelki 4.3–8 niso vključeni v ta predogled. Kupite celoten dokument za dostop do celotne vsebine. ... ]

## 9. Izjeme

- 9.1 [All] Process Owner / Business Owner mora pred uporabo nestandardnega trženjskega kanala, oznake, konfiguracije analitike, mehanizma preferenc ali dobavitelja, kadar zahtevanih dokazil ni mogoče dokončati pred začetkom, zahtevati izjemo v REG12.
- 9.2 [Conditional] Data Protection Officer / Privacy Advisor mora pred odobritvijo v REG12 pregledati zahtevo za izjemo glede zasebnosti pri trženju, kadar izjema vpliva na privolitve, otroke, zaposlene, občutljiva občinstva, čezmejni prenos, oblikovanje profilov ali bistveno razširitev sledenja.
- 9.3 [All] Top Management mora visoko tvegane ali bistvene izjeme glede zasebnosti pri trženju odobriti v REG12, preden izjema začne učinkovati.
- 9.4 [All] Privacy Lead / PIMS Manager mora za vsako odobreno izjemo glede zasebnosti pri trženju pred odobritvijo v REG12 določiti datum poteka, nosilca odprave in datum pregleda.

## 10. Uveljavljanje

- 10.1 [All] Privacy Lead / PIMS Manager mora v REG12 začasno ustaviti ali blokirati trženjsko dejavnost, kadar pred začetkom ali nadaljnjo uporabo manjkajo zahtevana dokazila REG02, REG05, REG07, REG08 ali REG09.
- 10.2 [All] System Owner / Application Owner mora neodobrene oznake, sledilnike, piksele, SDKs ali tokove podatkov kampanj onemogočiti v enem delovnem dnevu po odločitvi o uveljavljanju ter dokončanje evidentirati v REG08 ali REG12.
- 10.3 [All] Vendor / Procurement Owner mora blokirati uvajanje, podaljšanje ali razširitev dobavitelja za trženje, ponudnika analitike ali oglaševalske platforme, kadar pred začetkom ali nadaljevanjem obdelave manjkajo zahtevana dokazila REG08 ali REG09.
- 10.4 [All] Process Owner / Business Owner mora uporabo prizadetih PII v kampanji ustaviti v enem delovnem dnevu po potrjeni odpovedi kontrole preferenc, izključitev, obvestil ali dobaviteljev ter dokončanje evidentirati v REG05 ali REG12.

- 10.5 [All] Internal Audit / Compliance Reviewer mora v 60 dneh po zaključku korektivnega ukrepa v REG12 preveriti učinkovitost korektivnih ukrepov za večje ali ponavljajoče se neskladnosti glede zasebnosti pri trženju.

## 11. Pregled in vzdrževanje

- 11.1 [All] Privacy Lead / PIMS Manager mora to politiko pregledati v REG12 enkrat letno in v 30 dneh po bistveni spremembi zahtev glede trženja, piškotkov, sledenja, analitike, oglaševalske tehnologije ali upravljanja privolitiev.
- 11.2 [Controller] Process Owner / Business Owner mora evidence obdelave za trženje v REG02 in odvisnosti preferenc v REG05 pregledati najmanj četrletno in v 30 dneh po bistveni spremembi kampanje.
- 11.3 [Controller] Privacy Lead / PIMS Manager mora evidence obvestil za trženje in obvestil o piškotkih v REG07 pregledati najmanj enkrat letno in v 30 dneh po bistveni spremembi obvestila, sledenja ali preferenc.
- 11.4 [All] Vendor / Procurement Owner mora evidence dobaviteljev za trženje, oznak, analitike in oglaševalskih platform v REG08 pregledati najmanj enkrat letno in pred podaljšanjem.
- 11.5 [Conditional] Privacy Lead / PIMS Manager mora usmerjanje prenosov v REG09 posodobiti v 15 delovnih dneh po ugotovljeni spremembi dobavitelja za trženje, ponudnika analitike ali lokacije gostovanja.
- 11.6 [All] Top Management mora pred objavo v REG12 odobriti bistvene revizije te politike.

## 12. Povezane politike

- 12.1 To politiko podpirajo naslednje povezane politike:
- 12.2 PII01 - Politika sistema upravljanja informacij o zasebnosti
- 12.3 PII02 - Politika vlog, odgovornosti in odgovornosti za ravnanje na področju zasebnosti
- 12.4 PII03 - Politika popisa dejavnosti obdelave PII in pravne podlage
- 12.5 PII04 - Politika obvestil o zasebnosti in preglednosti
- 12.6 PII05 - Politika upravljanja privolitiev in preferenc
- 12.7 PII06 - Politika upravljanja pravic PII principal
- 12.8 PII07 - Politika ocene tveganj za zasebnost in DPIA
- 12.9 PII08 - Politika vgrajenega in privzetega varstva zasebnosti
- 12.10 PII09 - Politika zbiranja, uporabe, razkritja in deljenja PII
- 12.11 PII10 - Politika hrambe, izbrisa in odstranjevanja PII
- 12.12 PII11 - Politika točnosti in kakovosti PII
- 12.13 PII12 - Politika upravljanja zasebnosti obdelovalcev, podobdelovalcev in tretjih oseb
- 12.14 PII13 - Politika mednarodnega prenosa PII
- 12.15 PII14 - Politika varnosti PII in nadzora dostopa
- 12.16 PII15 - Politika upravljanja incidentov in kršitev v zvezi s PII
- 12.17 PII17 - Politika dokumentiranih informacij in upravljanja dokazil PIMS
- 12.18 PII18 - Politika spremljanja, presoje in izboljševanja PIMS
- 12.19 PII19 - Politika zasebnosti zaposlenih
- 12.20 PII20 - Politika zasebnosti otrok
- 12.21 PII21 - Politika zasebnosti pri AI in avtomatiziranem sprejemanju odločitev
- 12.22 PII23 - Politika obdelovalcev PII v oblaku

## 13. Referenčni standardi in okviri

- 13.1 Ta politika je preslikana na naslednje standarde in predpise. Preslikava pojasnjuje, kako politika podpira navedene zahteve, in opredeljuje notranje določbe, ki jih izvajajo ali podpirajo.
- 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].