					Čia įrašykite registruoto juridinio asmens pavadinimą							
Dokumento numeris: PII15					Dokumento pavadinimas: **PII incidentų ir pažeidimų valdymo politika**							
Versija: 1.0		Įsigaliojimo data: 01.01.2025			Dokumento savininkas:							
X	Politika		Standartas		Procedūra		Forma		Registras		Kita	

Peržiūrų istorija				
Peržiūros numeris	**Peržiūros data**	**Pakeitimai**	**Peržiūrėjo**	**Proceso savininkas**

Patvirtinimai			
Vardas	**Pareigos**	**Data**	**Parašas**

Suderinta su standartais ir reglamentais

Standartas / reglamentas	Nuostata / kontrolės priemonė / straipsnis	Taikymas	Aprėpties tipas	Komentaras
ISO/IEC 27701:2025	Clause 7.4; Clause 7.5	Both	Supporting	PIMS komunikacija ir dokumentuoti pažeidimų įrodymai
ISO/IEC 27701:2025	Clause 8.1; Clause 8.2; Clause 8.3	Both	Supporting	Operacinė kontrolė, privatumo rizikos vertinimas ir sąsaja su rizikos tvarkymu
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Stebėsena, vertinimas, neatitiktis, korekciniai veiksmai ir tobulinimas
ISO/IEC 27701:2025	Annex A.3.11	Both	Primary	Incidentų valdymo planavimas ir pasirengimas PII tvarkymui
ISO/IEC 27701:2025	Annex A.3.12	Both	Primary	Reagavimas į informacijos saugumo incidentus, susijusius su PII
ISO/IEC 27701:2025	Annex A.3.13; Annex A.3.14	Both	Supporting	Teisiniai, įstatyminiai, reglamentavimo ir sutartiniai reikalavimai bei įrašų apsauga
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.6	Processor	Supporting	Duomenų tvarkytojo kliento susitarimas ir pagalba vykdant kliento prievoles
GDPR	Article 5(2); Article 24	Controller	Supporting	Atskaitomybė ir duomenų valdytojo atsakomybė
GDPR	Article 26	Joint Controller	Supporting	Bendrų duomenų valdytojų atsakomybių dėl pažeidimų koordinavimas

GDPR	Article 28	Both	Supporting	Duomenų tvarkytojo pagalba ir sutartinės duomenų tvarkytojo prievolės
GDPR	Article 32	Both	Supporting	Tvarkymo saugumas ir pažeidimų aptikimo pajėgumas
GDPR	Article 33	Both	Primary	Pranešimas apie asmens duomenų saugumo pažeidimą ir pažeidimo dokumentavimas
GDPR	Article 34	Controller	Primary	Pranešimas apie asmens duomenų saugumo pažeidimus paveiktiems duomenų subjektams
GDPR	Article 39	Conditional	Supporting	DPO konsultacijos, stebėsena, bendradarbiavimas ir kontaktinio punkto palaikymas
ISO/IEC 29100:2020	Clause 5.11; Clause 5.12	Both	Supporting	Informacijos saugumo ir privatumo atitikties principai
ISO/IEC 29151:2022	Clause 16.1.2; Clause 16.1.3	Both	Supporting	PII incidentų reagavimo atsakomybės ir įvykių pranešimas
ISO/IEC 27002:2022	Control 5.24; Control 5.25; Control 5.26; Control 5.27; Control 5.28	Both	Supporting	Incidentų planavimas, vertinimas, reagavimas, įgyta patirtis ir įrodymų rinkimas
ISO/IEC 27035-1:2023	Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Both	Supporting	Incidentų valdymo proceso gyvavimo ciklas
ISO/IEC 27035-2:2023	Clause 4; Clause 6; Clause 10; Clause 11; Clause 12	Both	Supporting	Incidentų politika, planas, informuotumas,

				testavimas ir įgyta patirtis
ISO/IEC 27035-3:2020	Clause 7; Clause 8; Clause 9; Clause 10; Clause 11; Clause 12	Both	Supporting	Aptikimo, pranešimo, triažo, analizės, reagavimo ir ataskaitų teikimo operacijos
ISO/IEC 27018:2020	Annex A.10.1	Conditional	Supporting	Debesijos duomenų tvarkytojo pranešimo ir pažeidimų įrašų lūkesčiai
NIS2 Directive (EU) 2022/2555	Article 23	Conditional	Supporting	Pranešimas apie reikšmingus incidentus, kai taikoma
DORA Regulation (EU) 2022/2554	Article 17; Article 18; Article 19	Conditional	Supporting	IRT incidentų valdymas, klasifikavimas ir pranešimas, kai taikoma

1. Taikymo sritis

1.1 Ši politika nustato reikalavimus PIMS taikymo srityje identifikuoti PII incidentus ir PII pažeidimus, apie juos pranešti, atlikti jų triažą, juos vertinti, lokalizuoti, teikti pranešimus, dokumentuoti, uždaryti ir tobulinti veiklą po jų.

1.2 Ši politika taikoma:

1.2.1 organizacijai, veikiančiai kaip PII duomenų valdytojas;

1.2.2 organizacijai, veikiančiai kaip bendras duomenų valdytojas, kai reikia koordinuoti atsakomybę dėl pažeidimo;

1.2.3 organizacijai, veikiančiai kaip PII duomenų tvarkytojas;

1.2.4 organizacijai, veikiančiai kaip subtvarkytojas;

1.2.5 sistemoms, taikomosioms programoms, paslaugoms, procesams, tiekėjams, duomenų tvarkytojams, subtvarkytojams ir trečiosioms šalims, kurios tvarko, saugo, perduoda, palaiko, pasiekia arba kitaip veikia PII PIMS taikymo srityje.

1.3 Ši politika naudoja REG10 - PII incidentų ir pažeidimų registrą kaip pagrindinį įrodymų objektą PII incidentų ir pažeidimų valdymui.

1.4 Ši politika naudoja pagalbinius įrodymų objektus taip:

1.4.1 REG01 - PIMS taikymo sričiai, taikomam suinteresuotųjų šalių, teisiniam, sutartiniam, sektoriniam ir klientų pranešimų kontekstui.

1.4.2 REG02 - paveiktoms tvarkymo veikloms, PII kategorijoms, duomenų subjektų kategorijoms, tikslams ir sistemoms.

1.4.3 REG03 - Taikomumo pareiškimui ir kontrolės priemonių taikymo atnaujinimams.

1.4.4 REG04 - privatumo rizikos, DPIA ir liekamosios rizikos sąsajai.

1.4.5 REG08 - duomenų tvarkytojų, subtvarkytojų, klientų, tiekėjų ir trečiųjų šalių incidentų sąsajos įrodymams.

1.4.6 REG09 - tarptautinių perdavimų sąsajai, kai incidentas paveikia tarpvalstybinį tvarkymą.

1.4.7 REG11 - mokymų, informuotumo ir reagavimo į incidentus kompetencijos įrodymams.

1.4.8 REG12 - audito, neatitikties, korekcinių veiksmų ir tobulinimo įrodymams.

1.5 Ši politika remiasi susijusiomis PIMS politikomis specializuotoms kontrolės priemonėms:

1.5.1 PII03 reglamentuoja tvarkymo veiklos apskaitą ir teisinio pagrindo įrašus.

1.5.2 PII04 reglamentuoja privatumo pranešimo ir skaidrumo kontrolės priemones, kurios nėra konkrečiai susijusios su pažeidimo komunikacija.

1.5.3 PII06 reglamentuoja duomenų subjektų teisių prašymus, kurie kyla prieš incidentą, jo metu arba po jo.

1.5.4 PII07 reglamentuoja privatumo rizikos vertinimo ir DPIA metodiką.

1.5.5 PII08 reglamentuoja privatumo pagal projektavimą ir privatumo pagal numatytuosius nustatymus kontrolės priemones.

1.5.6 PII10 reglamentuoja saugojimo, ištrynimo ir sunaikinimo kontrolės priemones.

1.5.7 PII12 reglamentuoja duomenų tvarkytojų, subtvarkytojų, tiekėjų ir trečiųjų šalių privatumo santykių kontrolės priemones.

1.5.8 PII13 reglamentuoja tarptautinio PII perdavimo mechanizmus ir perdavimo rizikos įrašus.

1.5.9 PII14 reglamentuoja prevencines ir nustatomąsias PII saugumo ir prieigos kontrolės priemones.

1.5.10 PII16 reglamentuoja privatumo mokymus, informuotumą ir kompetenciją.

1.5.11 PII17 reglamentuoja dokumentuotos informacijos ir įrodymų valdymą.

1.5.12 PII18 reglamentuoja stebėseną, vidaus auditą, vadovybės peržiūrą, neatitiktį, korekcinius veiksmus ir nuolatinį tobulinimą.

1.6 Šioje politikoje:

1.6.1 „PII incidentas“ reiškia įtariamą arba patvirtintą įvykį, kuris paveikė, galėjo paveikti arba pagrįstai galėtų paveikti PII konfidencialumą, vientisumą, prieinamumą, teisėtą tvarkymą arba autorizuotą tvarkymą.

1.6.2 „PII pažeidimas“ reiškia patvirtintą PII incidentą, susijusį su neautorizuotu, neteisėtu, atsitiktiniu arba nenumatytu PII sunaikinimu, praradimu, pakeitimu, atskleidimu, prieiga prie PII, neprieinamumu arba kompromitavimu.

1.6.3 „Pažeidimo vertinimas“ reiškia dokumentuotą vertinimą, ar PII incidentas yra PII pažeidimas, kokia PII ir kurie duomenų subjektai yra paveikti, kokios rizikos gali kilti, kokių pranešimų arba komunikacijos reikia ir kokių taisomųjų veiksmų reikia imtis.

1.6.4 „Sužinojimas“ reiškia momentą, kai organizacija turi pagrįstą tikrumo laipsnį, kad įvyko saugumo arba privatumo incidentas ir PII buvo arba galėjo būti kompromituota.

1.6.5 „Didelio poveikio PII incidentas“ reiškia PII incidentą, susijusį su didelės rizikos tvarkymu, specialių kategorijų arba itin jautria PII, didelio masto PII, pažeidžiamais asmenimis, reglamentuojamais klientais, poveikiu keliose jurisdikcijose, reikšmingu poveikiu klientams, privilegijuotos prieigos kompromitavimu, viešu atskleidimu, išpirkos reikalaujančia programine įranga, paslaugos neprieinamumu arba reikšmingu operaciniu ar reputaciniu poveikiu.

1.6.6 „Esminis incidento pakeitimas“ reiškia naują arba pasikeitusią informaciją, kuri daro įtaką incidento apimčiai, sunkumui, PII kategorijoms, poveikiui duomenų subjektams, sprendimui dėl pranešimo, poveikiui klientams, pagrindinei priežasčiai, lokalizavimui, atkūrimui, korekciniams veiksmams arba išorinio pranešimo prievolėms.

2. Tikslas

2.1 Šios politikos tikslas – užtikrinti, kad PII incidentai ir pažeidimai būtų tvarkomi nuosekliai, laiku, teisėtai, saugiai ir su auditui tinkamais įrodymais.

2.2 Ši politika palaiko atskaitomybę reikalaudama, kad PII incidentai ir pažeidimai būtų registruojami REG10 ir, kai taikoma, susiejami su paveiktais tvarkymo įrašais, privatumo rizikomis, santykiais su duomenų tvarkytojais ir subtvarkytojais, perdavimo įrašais, korekciniais veiksmais ir mokymų įrašais.

2.3 Ši politika užtikrina, kad duomenų valdytojo, bendro duomenų valdytojo, duomenų tvarkytojo ir subtvarkytojo prievolės būtų tvarkomos pagal atskiras taikymo taisykles, išlaikant vieną integruotą incidentų ir pažeidimų įrodymų modelį.

3. Tikslai

3.1 Šios politikos tikslai yra:

3.1.1 užtikrinti, kad įtariami PII incidentai būtų pranešami ir registruojami nedelsiant;

3.1.2 užtikrinti, kad PII incidentams būtų atliekamas triažas ir jie būtų klasifikuojami pagal nuoseklius kriterijus;

3.1.3 užtikrinti, kad pažeidimo vertinimuose būtų atsižvelgiama į paveiktą PII, duomenų subjektus, sistemas, tvarkymo veiklas, duomenų tvarkytojus, subtvarkytojus, perdavimus, rizikas ir taisomuosius veiksmus;

3.1.4 užtikrinti, kad duomenų valdytojo sprendimai dėl pranešimo ir komunikacijos su duomenų subjektais būtų dokumentuojami;

3.1.5 užtikrinti, kad duomenų tvarkytojų ir subtvarkytojų pranešimai apie pažeidimus klientams arba aukštesnės grandies šalims būtų pateikiami nepagrįstai nedelsiant ir pagal taikomus susitarimus;

3.1.6 užtikrinti, kad incidentų valdymo metu įrodymai būtų išsaugomi ir apsaugomi;

3.1.7 užtikrinti, kad lokalizavimas, pašalinimas, atkūrimas ir patvirtinimas būtų sekami per REG10;

3.1.8 užtikrinti, kad, kai taikoma, būtų įvertinti reglamentuojami, sutartiniai, klientų ir sektoriniai pranešimo aktyvikliai;

3.1.9 užtikrinti, kad po incidentų įgyta patirtis lemtų korekcinius veiksmus ir nuolatinį tobulinimą;

3.1.10 užtikrinti, kad incidentų ir pažeidimų įrašai būtų prieinami auditui, vadovybės peržiūrai, klientų patikinimui ir reglamentavimo institucijų peržiūrai, kai taikoma.

4. Politikos nuostatos

4.1 Pasirengimas incidentams ir jų priėmimas

4.1.1 [Both] Privacy Lead / PIMS Manager PRIVALO prižiūrėti PII incidentų ir pažeidimų tvarkymo kriterijus REG10 ne rečiau kaip kartą per metus ir po bet kokio esminio PIMS taikymo srities, teisinio konteksto, sutartinių prievolių arba didelės rizikos tvarkymo pakeitimo.

4.1.2 [All] Incident Response Coordinator PRIVALO užregistruoti kiekvieną praneštą arba aptiktą įtariamą PII incidentą REG10 per vieną darbo dieną nuo gavimo arba anksčiau, kai gali būti aktyvuotas taikomas pranešimo arba kliento informavimo terminas.

4.1.3 [Both] System Owner / Application Owner PRIVALO išsaugoti atitinkamus sistemų žurnalus, įspėjimus, prieigos įrašus, konfigūracijos įrodymus ir atkūrimo įrodymus, susietus su REG10, kai įtariamas incidentas paveikia sistemą arba taikomąją programą, tvarkančią PII.

4.1.4 [Both] Information Security Lead PRIVALO atlikti pradinį techninį bet kokio saugumo įvykio, susijusio su PII, triažą per 24 valandas nuo aptikimo ir REG10 įrašyti pradinį sunkumo lygį, paveiktus išteklius ir lokalizavimo būseną.

4.2 Klasifikavimas ir pažeidimo vertinimas

4.2.1 [Both] Incident Response Coordinator PRIVALO kiekvieną REG10 įrašą per 24 valandas nuo priėmimo klasifikuoti kaip ne PII įvykį, įtariamą PII incidentą, patvirtintą PII incidentą arba patvirtintą PII pažeidimą, arba atnaujinti REG10 įrašą nurodydamas priežastį, dėl kurios klasifikavimas tebėra nebaigtas.

4.2.2 [Both] Privacy Lead / PIMS Manager PRIVALO nustatyti paveiktą tvarkymo veiklą, PII kategorijas, duomenų subjektų kategorijas, sistemas, duomenų tvarkytojus, subtvarkytojus, perdavimo vietas ir privatumo rizikas REG02, REG04, REG08, REG09 ir REG10 prieš galutinai priimant sprendimą dėl pranešimo apie pažeidimą.

4.2.3 [Controller] Data Protection Officer / Privacy Advisor PRIVALO įvertinti riziką paveiktiems duomenų subjektams dėl kiekvieno patvirtinto arba pagrįstai įtariamo PII pažeidimo ir REG10 įrašyti pranešimo rekomendaciją, rizikos pagrindimą ir konsultaciją prieš priimant sprendimą dėl išorinio pranešimo.

4.2.4 [Processor] Privacy Lead / PIMS Manager PRIVALO nustatyti paveiktą duomenų valdytoją arba klientą ir taikomus sutartinius pranešimo reikalavimus, kai tik organizacija sužino apie PII pažeidimą, paveikiantį kliento PII, ir PRIVALO įrašyti rezultatą REG08 ir REG10.

4.2.5 [Joint Controller] Privacy Lead / PIMS Manager PRIVALO patikrinti sutartą atsakomybę dėl pažeidimo, pagrindinę komunikacijos atsakomybę ir koordinavimo tvarką prieš bet kokį bendro duomenų valdytojo išorinį pranešimą ar komunikaciją ir PRIVALO įrašyti sprendimą REG08 ir REG10.

4.2.6 [Conditional] Privacy Lead / PIMS Manager PRIVALO įvertinti taikomus teisinius, sektorinius, finansų sektoriaus, kibernetinio saugumo, sutartinius, klientų ir paslaugų gavėjų pranešimo aktyviklius kiekvienam didelio poveikio PII incidentui ir REG01, REG08 bei REG10 įrašyti taikymo rezultatą.

[... 4.3–8 skyriai nėra įtraukti į šią peržiūrą. Įsigykite visą dokumentą, kad pasiektumėte visą turinį. ...]

9. Išimtys

9.1.1 [Both] Privacy Lead / PIMS Manager PRIVALO REG12 įrašyti bet kokią šios politikos išimtį prieš įgyvendinimą arba per 24 valandas po avarinio veiksmo, kai išankstinis patvirtinimas nebuvo įmanomas.

9.1.2 [Both] Top Management PRIVALO prieš uždarant incidentą patvirtinti bet kokią išimtį, kuri reikšmingai paveikia pranešimo apie pažeidimą laiką, viešąją komunikaciją, įsipareigojimą klientui, įrodymų išsaugojimą arba riziką duomenų subjektui, o patvirtinimo įrodymai turi būti saugomi REG10 ir REG12.

9.1.3 [Conditional] Data Protection Officer / Privacy Advisor PRIVALO prieš incidento uždarymą dokumentuoti konsultaciją dėl bet kokio pavėluoto pranešimo, sprendimo nepranešti arba išimtinio komunikacijos būdo, o konsultacija turi būti saugoma REG10.

9.1.4 [Both] Vendor / Procurement Owner PRIVALO per penkias darbo dienas nuo išimties nustatymo REG08 ir REG12 įrašyti tiekėjo, duomenų tvarkytojo, subtvarkytojo arba kliento inicijuotas išimtis, darančias įtaką reagavimui į incidentą.

10. Politikos laikymosi užtikrinimas

10.1.1 [All] Process Owner / Business Owner PRIVALO per dvi darbo dienas nuo nustatymo eskaluoti nepranešimą apie įtariamą PII incidentą, įrodymų neišsaugojimą, priskirtų veiksmų nesilaikymą arba nebendradarbiavimą atliekant pažeidimo vertinimą Privacy Lead / PIMS Manager, o įrodymai turi būti saugomi REG12.

10.1.2 [Both] Privacy Lead / PIMS Manager PRIVALO registruoti REG12 neatitiktį, kai šios politikos pažeidimas paveikia incidento priėmimą, triažą, lokalizavimą, pranešimą, įrodymų vientisumą, komunikaciją arba korekcinį veiksmą.

10.1.3 [Both] Vendor / Procurement Owner PRIVALO per penkias darbo dienas inicijuoti tiekėjo arba duomenų tvarkytojo taisomuosius veiksmus per REG08 ir REG12, kai duomenų tvarkytojas, subtvarkytojas, tiekėjas arba kita trečioji šalis neįvykdo sutartų incidentų arba pažeidimų prievolių.

10.1.4 [Both] Top Management PRIVALO kitos suplanuotos vadovybės peržiūros metu peržiūrėti esmines arba pasikartojančias incidentų valdymo neatitiktis, o sprendimai ir privalomi veiksmai turi būti saugomi REG12.

11. Peržiūra ir priežiūra

11.1.1 [Both] Privacy Lead / PIMS Manager PRIVALO peržiūrėti šią politiką ne rečiau kaip kartą per metus ir REG12 įrašyti peržiūros rezultatą, reikiamus pakeitimus ir patvirtinimo būseną.

11.1.2 [Both] Incident Response Coordinator PRIVALO inicijuoti šios politikos peržiūrą po incidento per 30 kalendorinių dienų po bet kurio didelio poveikio PII incidento arba patvirtinto PII pažeidimo uždarymo, o peržiūros įrodymai turi būti saugomi REG10 ir REG12.

11.1.3 [Conditional] Privacy Lead / PIMS Manager PRIVALO peržiūrėti šią politiką per 30 kalendorinių dienų nuo sužinojimo apie esminį taikomų teisinių, sektorinių, klientų, sutartinių, duomenų tvarkytojo, subtvarkytojo arba su perdavimu susijusių incidentų pranešimo reikalavimų pakeitimą, o peržiūros įrodymai turi būti saugomi REG01, REG08, REG09 ir REG12.

11.1.4 [Both] Internal Audit / Compliance Reviewer PRIVALO ne rečiau kaip kartą per metus per PIMS vidaus audito programą peržiūrėti šios politikos įgyvendinimą, o audito išvados ir korekciniai veiksmai turi būti saugomi REG12.

11.1.5 [Both] Top Management PRIVALO suplanuotos vadovybės peržiūros metu peržiūrėti incidentų tendencijas, reikšmingus pažeidimus, pranešimų veiksmingumą, vėluojančius korekcinius veiksmus ir politikos veiksmingumą, o rezultatai turi būti saugomi REG12.

12. Susijusios politikos

12.1 Ši politika turėtų būti skaitoma kartu su:

12.2 PII01 - Privatumo informacijos valdymo sistemos politika

12.3 PII02 - Privatumo vaidmenų, atsakomybių ir atskaitomybės politika

12.4 PII03 - PII tvarkymo veiklos apskaitos ir teisinio pagrindo politika

12.5 PII04 - Privatumo pranešimo ir skaidrumo politika

12.6 PII06 - Duomenų subjektų teisių valdymo politika

12.7 PII07 - Privatumo rizikos vertinimo ir DPIA politika

12.8 PII08 - Privatumo pagal projektavimą ir numatytuosius nustatymus politika

12.9 PII10 - PII saugojimo, ištrynimo ir sunaikinimo politika

12.10 PII12 - Duomenų tvarkytojų, subtvarkytojų ir trečiųjų šalių privatumo valdymo politika

12.11 PII13 - Tarptautinio PII perdavimo politika

12.12 PII14 - PII saugumo ir prieigos kontrolės politika

12.13 PII16 - Privatumo mokymų, informuotumo ir kompetencijos politika

12.14 PII17 - PIMS dokumentuotos informacijos ir įrodymų valdymo politika

12.15 PII18 - PIMS stebėsenos, audito ir tobulinimo politika

13. Pamatiniai standartai ir sistemos

13.1 ISO/IEC 27701:2025 - Clause 7.4; Clause 7.5. Addressed by clauses [4.4.7; 4.5.1; 4.5.3; 4.5.4; 5.2.2; 6.2.2; 7.1.1; 7.1.7; 11.1.3].

13.2 ISO/IEC 27701:2025 - Clause 8.1; Clause 8.2; Clause 8.3. Addressed by clauses [4.2.2; 4.3.4; 4.6.3; 6.3.1; 7.1.4; 11.1.2].

13.3 ISO/IEC 27701:2025 - Clause 9.1; Clause 10.2. Addressed by clauses [4.6.1; 4.6.2; 4.6.3; 4.6.4; 6.4.1; 6.5.1; 8.1.1; 8.1.4; 10.1.2; 11.1.4; 11.1.5].

13.4 ISO/IEC 27701:2025 - Annex A.3.11. Addressed by clauses [4.1.1; 4.1.2; 4.2.6; 4.4.1; 5.1.1; 5.4.1; 7.1.1; 7.1.2; 7.1.6].

13.5 ISO/IEC 27701:2025 - Annex A.3.12. Addressed by clauses [4.1.3; 4.1.4; 4.2.1; 4.2.3; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.4.1; 4.4.3; 4.4.4; 4.5.1; 4.5.4; 6.3.1].

13.6 ISO/IEC 27701:2025 - Annex A.3.13; Annex A.3.14. Addressed by clauses [4.2.6; 4.4.6; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.6.4; 6.2.2; 9.1.2; 11.1.3].

13.7 ISO/IEC 27701:2025 - Annex A.2.2.2; Annex A.2.2.6. Addressed by clauses [4.2.4; 4.4.4; 4.4.5; 4.5.5; 5.8.1; 7.1.5; 8.1.5; 10.1.3].

13.8 GDPR - Article 5(2); Article 24. Addressed by clauses [4.1.2; 4.2.2; 4.4.1; 4.5.1; 4.5.3; 4.5.4; 4.6.2; 5.2.1; 6.3.1; 8.1.3; 11.1.5].

13.9 GDPR - Article 26. Addressed by clauses [4.2.5; 4.4.1; 4.4.3; 5.3.1; 6.2.2; 11.1.3].

13.10 GDPR - Article 28. Addressed by clauses [4.2.4; 4.3.5; 4.4.4; 4.4.5; 4.5.5; 5.8.1; 7.1.5; 8.1.5; 10.1.3].

13.11 GDPR - Article 32. Addressed by clauses [4.1.3; 4.1.4; 4.3.2; 4.3.3; 4.5.2; 4.6.3; 5.5.1; 7.1.4; 8.1.2; 11.1.2].

13.12 GDPR - Article 33. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.4.1; 4.4.2; 4.4.4; 4.4.5; 4.5.1; 4.5.4; 8.1.3; 9.1.3].

13.13 GDPR - Article 34. Addressed by clauses [4.2.3; 4.2.5; 4.4.2; 4.4.3; 4.4.7; 4.5.4; 8.1.3; 9.1.3].

13.14 GDPR - Article 39. Addressed by clauses [4.2.3; 4.4.2; 5.3.1; 6.2.2; 9.1.3; 11.1.3].

13.15 ISO/IEC 29100:2020 - Clause 5.11; Clause 5.12. Addressed by clauses [4.2.2; 4.3.2; 4.3.3; 4.5.3; 4.6.2; 4.6.3; 5.2.2; 6.4.1; 8.1.4; 11.1.4].

13.16 ISO/IEC 29151:2022 - Clause 16.1.2; Clause 16.1.3. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.2.1; 4.2.3; 4.4.1; 4.4.3; 4.6.5; 7.1.3; 7.1.6].

13.17 ISO/IEC 27002:2022 - Control 5.24; Control 5.25; Control 5.26; Control 5.27; Control 5.28. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.4; 4.2.1; 4.3.1; 4.3.2; 4.3.3; 4.5.1; 4.5.2; 4.6.1; 4.6.2; 7.1.2; 7.1.6].

13.18 ISO/IEC 27035-1:2023 - Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.2.1; 4.3.1; 4.3.2; 4.4.7; 4.5.2; 4.6.1; 5.4.1; 7.1.6; 11.1.2].

13.19 ISO/IEC 27035-2:2023 - Clause 4; Clause 6; Clause 10; Clause 11; Clause 12. Addressed by clauses [4.1.1; 4.6.1; 4.6.5; 5.1.1; 7.1.1; 7.1.3; 7.1.6; 8.1.6; 11.1.1; 11.1.2].

13.20 ISO/IEC 27035-3:2020 - Clause 7; Clause 8; Clause 9; Clause 10; Clause 11; Clause 12. Addressed by clauses [4.1.2; 4.1.4; 4.2.1; 4.3.1; 4.3.2; 4.4.1; 4.4.4; 4.5.1; 5.4.2; 6.1.2; 8.1.2].

13.21 ISO/IEC 27018:2020 - Annex A.10.1. Addressed by clauses [4.2.4; 4.3.5; 4.4.4; 4.4.5; 4.5.5; 5.8.1; 7.1.5; 8.1.5].

13.22 NIS2 Directive (EU) 2022/2555 - Article 23. Addressed by clauses [4.2.6; 4.4.6; 4.4.7; 5.3.1; 6.2.2; 8.1.3; 11.1.3].

13.23 DORA Regulation (EU) 2022/2554 - Article 17; Article 18; Article 19. Addressed by clauses [4.2.1; 4.2.6; 4.4.6; 4.4.7; 5.1.2; 6.2.1; 8.1.3; 11.1.3; 11.1.5].