					Sisestage siia registreeritud juriidilise isiku nimi							
Dokumendi number: PII15					Dokumendi pealkiri: **PII intsidentide ja rikkumiste haldamise poliitika**							
Versioon: 1.0		Jõustumiskuupäev: 01.01.2025			Dokumendi omanik:							
X	Poliitika		Standard		Protseduur		Vorm		Register		Muu	

Muudatuste ajalugu				
Muudatuse number	**Muudatuse kuupäev**	**Muudatused**	**Läbi vaadanud**	**Protsessi omanik**

Kinnitused			
Nimi	**Ametikoht**	**Kuupäev**	**Allkiri**

Kooskõla standardite ja regulatsioonidega

Standard/õigusnorm	Punkt/kontrollimeede/artikkel	Applicability	Coverage Type	Kommentaar
ISO/IEC 27701:2025	Clause 7.4; Clause 7.5	Both	Supporting	PIMS-i kommunikatsioon ja dokumenteeritud rikkumise tõendusmaterjal
ISO/IEC 27701:2025	Clause 8.1; Clause 8.2; Clause 8.3	Both	Supporting	Tegevuslik ohje, privaatsusriskide hindamine ning seos riski käsitlemisega
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Seire, hindamine, mittevastavus, parandusmeetmed ja täiustamine
ISO/IEC 27701:2025	Annex A.3.11	Both	Primary	Intsidendihalduse planeerimine ja ettevalmistus PII töötlemiseks
ISO/IEC 27701:2025	Annex A.3.12	Both	Primary	Reageerimine infoturbeintsidentidele, mis hõlmavad PII-d
ISO/IEC 27701:2025	Annex A.3.13; Annex A.3.14	Both	Supporting	Õiguslikud, seadusest tulenevad, regulatiivsed ja lepingulised nõuded ning kirjete kaitse
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.6	Processor	Supporting	Volitatud töötleja kliendileping ja kliendi kohustuste toetamine
GDPR	Article 5(2); Article 24	Controller	Supporting	Vastutus ja vastutava töötleja vastutusala
GDPR	Article 26	Joint Controller	Supporting	Kaasvastutavate töötlejate rikkumisega seotud vastutuse koordineerimine
GDPR	Article 28	Both	Supporting	Volitatud töötleja abi ja volitatud töötleja lepingulised kohustused
GDPR	Article 32	Both	Supporting	Töötlemise turvalisus ja rikkumise tuvastamise võimekus
GDPR	Article 33	Both	Primary	Isikuandmete rikkumisest teatamine

				ja rikkumise dokumenteerimine
GDPR	Article 34	Controller	Primary	Isikuandmete rikkumistest teavitamine mõjutatud isikuandmesubjektidele
GDPR	Article 39	Conditional	Supporting	Andmekaitseametniku nõustamine, seire, koostöö ja kontaktpunkti tugi
ISO/IEC 29100:2020	Clause 5.11; Clause 5.12	Both	Supporting	Infoturbe ja privaatsuse vastavuse põhimõtted
ISO/IEC 29151:2022	Clause 16.1.2; Clause 16.1.3	Both	Supporting	PII intsidentidele reageerimise vastutusalad ja sündmustest teatamine
ISO/IEC 27002:2022	Control 5.24; Control 5.25; Control 5.26; Control 5.27; Control 5.28	Both	Supporting	Intsidendi planeerimine, hindamine, reageerimine, õppetunnid ja tõendite kogumine
ISO/IEC 27035-1:2023	Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Both	Supporting	Intsidendihalduse protsessi elutsükkel
ISO/IEC 27035-2:2023	Clause 4; Clause 6; Clause 10; Clause 11; Clause 12	Both	Supporting	Intsidendipoliitika, plaan, teadlikkus, testimine ja õppetunnid
ISO/IEC 27035-3:2020	Clause 7; Clause 8; Clause 9; Clause 10; Clause 11; Clause 12	Both	Supporting	Tuvastamise, teavitamise, triaaži, analüüsi, reageerimise ja aruandluse toimingud
ISO/IEC 27018:2020	Annex A.10.1	Conditional	Supporting	Pilvekeskkonna volitatud töötleja teavitamise ja rikkumiskirjete ootused
NIS2 Directive (EU) 2022/2555	Article 23	Conditional	Supporting	Olulistest intsidentidest teatamine, kui kohaldatav
DORA Regulation (EU) 2022/2554	Article 17; Article 18; Article 19	Conditional	Supporting	IKT intsidentide haldus, klassifitseerimine ja aruandlus, kui kohaldatav

1. Kohaldamisala

1.1 Käesolev poliitika määrab nõuded PII intsidentide ja PII rikkumiste tuvastamiseks, neist teatamiseks, triaažiks, hindamiseks, ohjeldamiseks, teavitamiseks, dokumenteerimiseks, sulgemiseks ja nende põhjal täiustamiseks PIMS-i kohaldamisalas.

1.2 Käesolev poliitika kohaldub järgmistele juhtudele:

1.2.1 organisatsioon tegutseb PII vastutava töötlejana;

1.2.2 organisatsioon tegutseb kaasvastutava töötlejana, kui on vaja koordineerida rikkumisega seotud vastutust;

1.2.3 organisatsioon tegutseb PII volitatud töötlejana;

1.2.4 organisatsioon tegutseb alltöötlejana;

1.2.5 süsteemid, rakendused, teenused, protsessid, tarnijad, volitatud töötlejad, alltöötlejad ja kolmandad osapooled, kes töötlevad, säilitavad, edastavad, toetavad, pääsevad juurde või muul viisil mõjutavad PII-d PIMS-i kohaldamisalas.

1.3 Käesolev poliitika kasutab REG10 - PII intsidentide ja rikkumiste registrit PII intsidentide ja rikkumiste haldamise peamise tõendusobjektina.

1.4 Käesolev poliitika kasutab toetavaid tõendusobjekte järgmiselt:

1.4.1 REG01 PIMS-i kohaldamisala ning kohaldatava huvitatud osapoole, õigusliku, lepingulise, valdkondliku ja kliendiaruandluse konteksti jaoks.

1.4.2 REG02 mõjutatud töötlemistoimingute, PII kategooriate, isikuandmesubjektide kategooriate, eesmärkide ja süsteemide jaoks.

1.4.3 REG03 kohaldatavusavalduse ja kontrollimeetmete kohaldatavuse uuenduste jaoks.

1.4.4 REG04 privaatsusriski, DPIA ja jääkriski seoste jaoks.

1.4.5 REG08 volitatud töötleja, alltöötleja, kliendi, tarnija ja kolmanda osapoole intsidendiliidese tõendusmaterjali jaoks.

1.4.6 REG09 rahvusvahelise edastuse seose jaoks, kui intsident mõjutab piiriülest töötlemist.

1.4.7 REG11 koolituse, teadlikkuse ja intsidentidele reageerimise pädevuse tõendusmaterjali jaoks.

1.4.8 REG12 auditi, mittevastavuse, parandusmeetmete ja täiustamise tõendusmaterjali jaoks.

1.5 Käesolev poliitika tugineb seotud PIMS-i poliitikatele erikontrollide osas:

1.5.1 PII03 reguleerib töötlemisregistrit ja õigusliku aluse kirjeid.

1.5.2 PII04 reguleerib privaatsusteate ja läbipaistvuse kontrollimeetmeid väljaspool rikkumisspetsiifilist kommunikatsiooni.

1.5.3 PII06 reguleerib isikuandmesubjekti õiguste taotlusi, mis tekivad enne intsidenti, intsidendi ajal või pärast intsidenti.

1.5.4 PII07 reguleerib privaatsusriskide hindamise ja DPIA metoodikat.

1.5.5 PII08 reguleerib lõimitud andmekaitse ja vaikimisi andmekaitse kontrollimeetmeid.

1.5.6 PII10 reguleerib säilitamise, kustutamise ja kõrvaldamise kontrollimeetmeid.

1.5.7 PII12 reguleerib volitatud töötlejate, alltöötlejate, tarnijate ja kolmandate osapoolte privaatsussuhete kontrollimeetmeid.

1.5.8 PII13 reguleerib PII rahvusvahelise edastuse mehhanisme ja edastusriski kirjeid.

1.5.9 PII14 reguleerib ennetavaid ja tuvastavaid PII turbe- ja juurdepääsukontrolle.

1.5.10 PII16 reguleerib privaatsuskoolitust, teadlikkust ja pädevust.

1.5.11 PII17 reguleerib dokumenteeritud teabe ja tõendusmaterjali haldust.

1.5.12 PII18 reguleerib seiret, siseauditit, juhtkonna läbivaatamist, mittevastavust, parandusmeetmeid ja pidevat täiustamist.

1.6 Käesolevas poliitikas:

1.6.1 „PII intsident“ tähendab kahtlustatavat või kinnitatud sündmust, mis on mõjutanud, võib olla mõjutanud või võib mõistlikult mõjutada PII konfidentsiaalsust, terviklust, käideldavust, seaduslikku töötlemist või lubatud käitlemist.

1.6.2 „PII rikkumine“ tähendab kinnitatud PII intsidenti, mis hõlmab PII volitamata, õigusvastast, juhuslikku või ettekavatsematut hävitamist, kaotsiminekut, muutmist, avalikustamist, sellele juurdepääsu, selle kättesaamatust või kompromiteerimist.

1.6.3 „Rikkumise hindamine“ tähendab dokumenteeritud hindamist selle kohta, kas PII intsident on PII rikkumine, milline PII ja millised isikuandmesubjektid on mõjutatud, millised riskid võivad tekkida, millised teavitused või kommunikatsioonid on nõutavad ning millised parandusmeetmed on vajalikud.

1.6.4 „Teadlikuks saamine“ tähendab hetke, mil organisatsioonil on mõistlik kindlus, et turbe- või privaatsusintsident on toimunud ning PII on või võib olla kompromiteeritud.

1.6.5 „Suure mõjuga PII intsident“ tähendab PII intsidenti, mis hõlmab kõrge riskiga töötlemist, eriliiki või väga tundlikku PII-d, suuremahulist PII-d, haavatavaid isikuid, reguleeritud kliente, mitme jurisdiktsiooni mõju, olulist mõju kliendile, privilegeeritud juurdepääsu kompromiteerimist, avalikku kokkupuudet, lunavara, teenuse kättesaamatust või olulist tegevuslikku või mainealast mõju.

1.6.6 „Oluline intsidendi muudatus“ tähendab uut või muutunud teavet, mis mõjutab intsidendi ulatust, raskusastet, PII kategooriaid, mõju isikuandmesubjektidele, teavitamisotsust, mõju kliendile, algpõhjust, ohjeldamist, taastet, parandusmeedet või väliseid aruandluskohustusi.

2. Eesmärk

2.1 Käesoleva poliitika eesmärk on tagada, et PII intsidente ja rikkumisi käsitletakse järjepidevalt, viivitamata, õiguspäraselt, turvaliselt ja auditiks valmis tõendusmaterjaliga.

2.2 Käesolev poliitika toetab vastutust, nõudes PII intsidentide ja rikkumiste registreerimist REG10-s ning nende sidumist mõjutatud töötlemiskirjete, privaatsusriskide, volitatud töötlejate ja alltöötlejate suhete, edastuskirjete, parandusmeetmete ja koolituskirjetega, kui need on asjakohased.

2.3 Käesolev poliitika tagab, et vastutava töötleja, kaasvastutava töötleja, volitatud töötleja ja alltöötleja kohustusi käsitletakse eraldi kohaldatavusreeglite kaudu, säilitades samal ajal ühe integreeritud intsidendi- ja rikkumistõendite mudeli.

3. Eesmärgid

3.1 Käesoleva poliitika eesmärgid on:

3.1.1 tagada, et kahtlustatavatest PII intsidentidest teatatakse ja need registreeritakse viivitamata;

3.1.2 tagada, et PII intsidente triaažitakse ja klassifitseeritakse järjepidevate kriteeriumide alusel;

3.1.3 tagada, et rikkumise hindamisel võetakse arvesse mõjutatud PII-d, isikuandmesubjekte, süsteeme, töötlemistoiminguid, volitatud töötlejaid, alltöötlejaid, edastusi, riske ja parandusmeetmeid;

3.1.4 tagada, et vastutava töötleja teavitamisotsused ja isikuandmesubjektidele suunatud kommunikatsiooni otsused dokumenteeritakse;

3.1.5 tagada, et volitatud töötleja ja alltöötleja rikkumisteated klientidele või ülesvoolu osapooltele tehakse põhjendamatu viivituseta ja kooskõlas kohaldatavate lepingutega;

3.1.6 tagada, et tõendusmaterjal säilitatakse ja kaitstakse intsidendi käsitlemise ajal;

3.1.7 tagada, et ohjeldamist, kõrvaldamist, taastet ja valideerimist jälgitakse REG10 kaudu;

3.1.8 tagada, et reguleeritud, lepingulisi, kliendi- ja valdkondlikke aruandluse käivitajaid hinnatakse, kui kohaldatav;

3.1.9 tagada, et intsidendi õppetunnid toovad kaasa parandusmeetmed ja pideva täiustamise;

3.1.10 tagada, et intsidendi- ja rikkumiskirjed on kättesaadavad auditiks, juhtkonna läbivaatamiseks, kliendile kindluse andmiseks ja regulatiivseks läbivaatamiseks, kui kohaldatav.

4. Poliitika seisukohad

4.1 Intsidendivalmidus ja vastuvõtt

4.1.1 [Both] Privacy Lead / PIMS Manager peab vähemalt kord aastas ja pärast iga olulist muudatust PIMS-i kohaldamisalas, õiguslikus kontekstis, lepingulistes kohustustes või kõrge riskiga töötlemises hoidma REG10-s ajakohasena PII intsidentide ja rikkumiste käsitlemise kriteeriume.

4.1.2 [All] Incident Response Coordinator peab registreerima iga teatatud või tuvastatud kahtlustatava PII intsidendi REG10-s ühe tööpäeva jooksul alates selle kättesaamisest või varem, kui võib käivituda kohaldatav teavitamise või kliendiaruandluse tähtaeg.

4.1.3 [Both] System Owner / Application Owner peab säilitama asjakohased süsteemilogid, teavitused, juurdepääsukirjed, konfiguratsiooni tõendusmaterjali ja taastetõendid ning siduma need REG10-ga, kui kahtlustatav intsident mõjutab PII-d töötlevat süsteemi või rakendust.

4.1.4 [Both] Information Security Lead peab viima PII-d hõlmava turbesündmuse esmase tehnilise triaaži lõpule 24 tunni jooksul alates tuvastamisest ning registreerima esialgse raskusastme, mõjutatud varad ja ohjeldamise seisu REG10-s.

4.2 Klassifitseerimine ja rikkumise hindamine

4.2.1 [Both] Incident Response Coordinator peab klassifitseerima iga REG10 kande mitte-PII sündmuseks, kahtlustatavaks PII intsidendiks, kinnitatud PII intsidendiks või kinnitatud PII rikkumiseks 24 tunni jooksul alates vastuvõtust või ajakohastama REG10 kirjet põhjusega, miks klassifitseerimine on jätkuvalt pooleli.

4.2.2 [Both] Privacy Lead / PIMS Manager peab enne rikkumisest teavitamise otsuse lõplikku tegemist tuvastama mõjutatud töötlemistoimingu, PII kategooriad, isikuandmesubjektide kategooriad, süsteemid, volitatud töötlejad, alltöötlejad, edastuse asukohad ja privaatsusriskid REG02-s, REG04-s, REG08-s, REG09-s ja REG10-s.

4.2.3 [Controller] Data Protection Officer / Privacy Advisor peab hindama riski mõjutatud isikuandmesubjektidele iga kinnitatud või mõistlikult kahtlustatava PII rikkumise puhul ning registreerima teavitamissoovituse, riskipõhjenduse ja nõuande REG10-s enne välise teavitamise otsuse tegemist.

4.2.4 [Processor] Privacy Lead / PIMS Manager peab tuvastama mõjutatud vastutava töötleja või kliendi ja kohaldatavad lepingulised teavitamisnõuded niipea, kui organisatsioon saab teadlikuks kliendi PII-d mõjutavast PII rikkumisest, ning peab tulemuse registreerima REG08-s ja REG10-s.

4.2.5 [Joint Controller] Privacy Lead / PIMS Manager peab enne kaasvastutava töötleja mis tahes välist teavitust või kommunikatsiooni kontrollima kokkulepitud rikkumisega seotud vastutust, juhtiva kommunikatsioonivastutaja rolli ja koordineerimiskorda ning peab otsuse registreerima REG08-s ja REG10-s.

4.2.6 [Conditional] Privacy Lead / PIMS Manager peab iga suure mõjuga PII intsidendi puhul hindama kohaldatavaid õiguslikke, valdkondlikke, finantssektori, küberturbe, lepingulisi, kliendi- ja teenusesaaja aruandluse käivitajaid ning registreerima kohaldatavuse tulemuse REG01-s, REG08-s ja REG10-s.

[... Jaotised 4.3–8 ei ole selles eelvaates. Täieliku sisu saamiseks ostke täisdokument. ...]

9. Erandid

9.1.1 [Both] Privacy Lead / PIMS Manager peab registreerima mis tahes erandi käesolevast poliitikast REG12-s enne rakendamist või 24 tunni jooksul pärast erakorralist tegevust, kui eelnev heakskiit ei olnud teostatav.

9.1.2 [Both] Top Management peab enne intsidendi sulgemist heaks kiitma mis tahes erandi, mis oluliselt mõjutab rikkumisest teavitamise ajastust, avalikku kommunikatsiooni, kliendikohustust, tõendusmaterjali säilitamist või isikuandmesubjekti riski, kusjuures heakskiidu tõendusmaterjal säilitatakse REG10-s ja REG12-s.

9.1.3 [Conditional] Data Protection Officer / Privacy Advisor peab enne intsidendi sulgemist dokumenteerima nõuande mis tahes viivitatud teavituse, teavitamata jätmise otsuse või erandliku kommunikatsiooniviisi kohta, kusjuures nõuanne säilitatakse REG10-s.

9.1.4 [Both] Vendor / Procurement Owner peab registreerima tarnija, volitatud töötleja, alltöötleja või kliendi põhjustatud erandid, mis mõjutavad intsidendile reageerimist, REG08-s ja REG12-s viie tööpäeva jooksul pärast erandi tuvastamist.

10. Järgimise tagamine

10.1.1 [All] Process Owner / Business Owner peab eskaleerima kahtlustatavast PII intsidendist teatamata jätmise, tõendusmaterjali säilitamata jätmise, määratud tegevuste järgimata jätmise või rikkumise hindamisel koostööst keeldumise rollile Privacy Lead / PIMS Manager kahe tööpäeva jooksul pärast avastamist, kusjuures tõendusmaterjal säilitatakse REG12-s.

10.1.2 [Both] Privacy Lead / PIMS Manager peab registreerima REG12 mittevastavuse, kui käesoleva poliitika rikkumine mõjutab intsidendi vastuvõttu, triaaži, ohjeldamist, teavitamist, tõendusmaterjali terviklust, kommunikatsiooni või parandusmeedet.

10.1.3 [Both] Vendor / Procurement Owner peab REG08 ja REG12 kaudu algatama tarnija või volitatud töötleja parandusmeetmed viie tööpäeva jooksul, kui volitatud töötleja, alltöötleja, tarnija või muu kolmas osapool ei täida kokkulepitud intsidendi- või rikkumiskohustusi.

10.1.4 [Both] Top Management peab olulised või korduvad intsidendihalduse mittevastavused läbi vaatama järgmisel kavandatud juhtkonna läbivaatamisel, kusjuures otsused ja nõutavad tegevused säilitatakse REG12-s.

11. Läbivaatamine ja ajakohastamine

11.1.1 [Both] Privacy Lead / PIMS Manager peab käesoleva poliitika vähemalt kord aastas läbi vaatama ning registreerima läbivaatamise tulemuse, nõutavad muudatused ja heakskiidu staatuse REG12-s.

11.1.2 [Both] Incident Response Coordinator peab käivitama käesoleva poliitika intsidendijärgse läbivaatamise 30 kalendripäeva jooksul pärast mis tahes suure mõjuga PII intsidendi või kinnitatud PII rikkumise sulgemist, kusjuures läbivaatamise tõendusmaterjal säilitatakse REG10-s ja REG12-s.

11.1.3 [Conditional] Privacy Lead / PIMS Manager peab käesoleva poliitika läbi vaatama 30 kalendripäeva jooksul pärast teadlikuks saamist olulisest muudatusest kohaldatavates õiguslikes, valdkondlikes, kliendi-, lepingulistes, volitatud töötleja, alltöötleja või edastusega seotud intsidentidest teatamise nõuetes, kusjuures läbivaatamise tõendusmaterjal säilitatakse REG01-s, REG08-s, REG09-s ja REG12-s.

11.1.4 [Both] Internal Audit / Compliance Reviewer peab käesoleva poliitika rakendamist vähemalt kord aastas läbi vaatama PIMS-i siseauditi programmi kaudu, kusjuures auditi leiud ja parandusmeetmed säilitatakse REG12-s.

11.1.5 [Both] Top Management peab kavandatud juhtkonna läbivaatamisel läbi vaatama intsidenditrendid, olulised rikkumised, teavitamise tulemuslikkuse, tähtaja ületanud parandusmeetmed ja poliitika tõhususe, kusjuures väljundid säilitatakse REG12-s.

12. Seotud poliitikad

12.1 Käesolevat poliitikat tuleb lugeda koos järgmiste dokumentidega:

12.1.1 PII01 - privaatsusteabe haldussüsteemi poliitika

12.1.2 PII02 - privaatsusrollide, vastutuste ja aruandekohustuse poliitika

12.1.3 PII03 - PII töötlemisregistri ja õigusliku aluse poliitika

12.1.4 PII04 - privaatsusteate ja läbipaistvuse poliitika

12.1.5 PII06 - isikuandmesubjekti õiguste haldamise poliitika

12.1.6 PII07 - privaatsusriskide hindamise ja DPIA poliitika

12.1.7 PII08 - lõimitud andmekaitse ja vaikimisi andmekaitse poliitika

12.1.8 PII10 - PII säilitamise, kustutamise ja kõrvaldamise poliitika

12.1.9 PII12 - volitatud töötlejate, alltöötlejate ja kolmandate osapoolte privaatsushalduse poliitika

12.1.10 PII13 - rahvusvahelise PII edastuse poliitika

12.1.11 PII14 - PII turbe- ja juurdepääsukontrolli poliitika

12.1.12 PII16 - privaatsuskoolituse, teadlikkuse ja pädevuse poliitika

12.1.13 PII17 - PIMS-i dokumenteeritud teabe ja tõendusmaterjali halduse poliitika

12.1.14 PII18 - PIMS-i seire, auditi ja täiustamise poliitika

13. Viitestandardid ja raamistikud

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].