					Sisestage siia registreeritud juriidilise isiku nimi						
Dokumendi number: PII21					Dokumendi pealkiri: **Tehisintellekti ja automatiseeritud otsuste tegemise privaatsuspoliitika**						
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 / Regulation	Clause / Control / Article	Applicability	Coverage Type	Comment
ISO/IEC 27701:2025	Clause 7.5; Clause 8.1	Both	Primary	Dokumenteeritud teave ja tegevuslik ohje tehisintellekti, profiilianalüüsi ning automatiseeritud otsuste tegemisega seotud töötlemise tõendusmaterjali jaoks
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Tehisintellektiga seotud privaatsuskontrollide seire, mittevastavused ja parandusmeetmed
ISO/IEC 27701:2025	Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.9	Controller	Primary	Eesmärk, õiguslik alus, privaatsuse mõjuhindamine ja vastutava töötleja kirjed
ISO/IEC 27701:2025	Annex A.1.2.7; Annex A.1.2.8	Controller	Supporting	Volitatud töötleja lepingud ja kaasvastutavate töötlejate kohustused tehisintellektiga seotud PII töötlemisel
ISO/IEC 27701:2025	Annex A.1.3.2; Annex A.1.3.3; Annex A.1.3.4	Controller	Primary	Kohustused isikuandmesubjektide ees ja läbipaistvus tehisintellektiga seotud töötlemisel
ISO/IEC 27701:2025	Annex A.1.3.6; Annex A.1.3.7; Annex A.1.3.10; Annex A.1.3.11	Controller	Primary	Vastuväited, juurdepääs, parandamine, kustutamine, taotluste käsitlemine ja automatiseeritud otsuste tegemise kohustused
ISO/IEC 27701:2025	Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5	Controller	Primary	Kogumise, töötlemise ja minimaalsuse piirangud tehisintellekti sisendite, väljundite ja tuletatud andmete jaoks

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	Rahvusvahelise edastamise, avalikustamise ja avalikustamistaotluste suunamine tehisintellektiga seotud PII puhul
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	Primary	Volitatud töötleja leping, dokumenteeritud juhised, kliendi kohustuste toetamine ja kirjed
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	Volitatud töötleja tugi isikuandmesubjekti puudutavatele kohustustele, edastamise suunamisele ja avalikustamise käsitlemisele
ISO/IEC 27701:2025	Annex A.3.14; Annex A.3.25	Both	Supporting	Tehisintellektiga seotud PII töötlemise kirjete ja logimise kaitse
GDPR	Article 4(4); Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(1)(d); Article 5(2)	Controller	Primary	Profiilianalüüs, õiglus, läbipaistvus, eesmärgi piirang, minimaalsus, täpsus ja vastutus
GDPR	Article 6; Article 9; Article 10	Controller	Primary	Seaduslikkus, eriliiki andmed ning süüdimõistvate kohtuotsuste või süütegudega seotud andmete kaitsemeetmed
GDPR	Article 12; Article 13; Article 14; Article 15	Controller	Primary	Läbipaistev teave, juurdepääs ja sisuline teave automatiseeritud otsuste tegemise kohta
GDPR	Article 16; Article 17; Article 18; Article 21; Article 22	Controller	Primary	Parandamise, kustutamise, piiramise, vastuväite esitamise ja automatiseeritud

				otsuste tegemisega seotud õigused
GDPR	Article 24; Article 25; Article 26; Article 28; Article 30; Article 32; Article 35; Article 39	Both	Supporting	Vastutava töötleja vastutus, lõimitud ja vaikimisi andmekaitse, kaasvastutavad töötlejad, volitatud töötlejad, kirjed, turvalisus, DPIA ja DPO ülesanded
GDPR	Article 44	Conditional	Referenced	Rahvusvahelise edastamise suunamine tehisintellektiga seotud PII töötlemisel
ISO/IEC 29100:2020	Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6; Clause 5.7	Both	Primary	Eesmärgi, kogumise, minimaalsuse, kasutamise, säilitamise, avalikustamise, täpsuse ja kvaliteedi põhimõtted
ISO/IEC 29100:2020	Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.11; Clause 5.12	Both	Supporting	Läbipaistvus, isiku osalemine, vastutus, infoturve ja privaatsusnõuete järgimine
ISO/IEC 29134:2020	Clause 5.1; Clause 6.2; Clause 6.3	Both	Supporting	PIA kasu, künnise määramine ja ettevalmistus tehisintellektiga seotud privaatsusriskide hindamiseks
ISO/IEC 29151:2022	Annex A.4; Annex A.5; Annex A.7; Annex A.8; Annex A.10	Both	Supporting	Eesmärgi, kogumise, minimaalsuse, kasutamise, säilitamise, avalikustamise, täpsuse ja isiku osalemise kontrollimeetmed

1. Kohaldamisala

1.1 Käesolev poliitika määrab kohustuslikud privaatsusnõuded tehisintellekti, profiilianalüüsi, skoorimise, soovituste, otsustustoe ja automatiseeritud otsuste tegemisega seotud töötlemistoimingutele, mis kasutavad, tuletavad, genereerivad, avalikustavad või muul viisil töötlevad PII-d PIMS-i kohaldamisalas.

1.2 Käesolevat poliitikat kohaldatakse järgmisele:

1.2.1 tehisintellekti kasutavad süsteemid, rakendused, mudelid, teenused, töövood, otsustusmootorid, skoorimisvahendid, soovitussüsteemid, analüütilised mudelid ja automatiseeritud otsuste tegemise protsessid, mis töötlevad PII-d;

1.2.2 profiilianalüüs, segmenteerimine, klassifitseerimine, prognoosimine, järeldamine, personaliseerimine, järjestamine, sobivuse hindamine, pettuste tuvastamine, riskiskoorimine, juurdepääsuotsused, tööga seotud hindamine, lastega seotud profiilianalüüs, turunduse personaliseerimine ja sarnane töötlemine, kui see hõlmab PII-d;

1.2.3 tehisintellektiga seotud PII, mida kasutatakse koolitamiseks, testimiseks, valideerimiseks, häälestamiseks, seireks, tootmiskeskkonnas järeldamiseks, väljundi läbivaatamiseks, toimivuse mõõtmiseks, intsidendi uurimiseks või mudeli kasutuselt kõrvaldamiseks;

1.2.4 vastutava töötleja, kaasvastutava töötleja, volitatud töötleja ja alltöötleja kontekstid;

1.2.5 tehisintellektiga seotud tarnijad, volitatud töötlejad, alltöötlejad, andmete jagamise saajad ja rahvusvahelise edastamise marsruudid, mis töötlevad PII-d.

1.3 Käesolev poliitika ei loo terviklikku tehisintellekti juhtimisraamistikku, tehisintellekti haldussüsteemi, tehisintellekti registrit, mudelite registrit, mudeliriskide registrit, õigluse registrit, algoritmide registrit, tehisintellekti intsidentide registrit, tehisintellekti komiteed, mudeli omaniku rolli, tehisintellektisüsteemi omaniku rolli, õigusnõustamise töövoogu ega eraldi tehisintellekti heakskiiduvormi.

1.4 Käesolev poliitika ei asenda järgmisi dokumente:

1.4.1 PII03 töötlemise registri, õigusliku aluse ja ROPA omamise kohta;

1.4.2 PII04 privaatsusteate juhtimise kohta;

1.4.3 PII05 nõusoleku ja eelistuste haldamise kohta;

1.4.4 PII06 isikuandmesubjekti õiguste töövoo kohta;

1.4.5 PII07 privaatsusriskide hindamise ja DPIA metoodika kohta;

1.4.6 PII08 lõimitud ja vaikimisi andmekaitse kontrollväravate kohta;

1.4.7 PII09 kogumise, kasutamise, avalikustamise ja jagamise kontrollimeetmete kohta;

1.4.8 PII10 säilitamise, kustutamise ja kõrvaldamise teostamise kohta;

1.4.9 PII11 täpsuse ja kvaliteedi kontrollimeetmete kohta;

1.4.10 PII12 volitatud töötleja, alltöötleja ja kolmanda osapoole elutsükli juhtimise kohta;

1.4.11 PII13 rahvusvahelise edastamise kontrollimeetmete kohta;

1.4.12 PII14 turvalisuse ja juurdepääsukontrolli kohta;

1.4.13 PII15 intsidendi ja rikkumise käsitlemise kohta;

1.4.14 PII18 seire, auditi ja täiustamise kohta;

1.4.15 PII19 töötajate privaatsuse kohta;

1.4.16 PII20 laste privaatsuse kohta;

1.4.17 PII22 turunduse privaatsuse ja küpsiste kohta.

2. Eesmärk

2.1 Käesoleva poliitika eesmärk on tagada, et PII-d hõlmavad tehisintellekti, profiilianalüüsi ja automatiseeritud otsuste tegemise toimingud on tuvastatud, dokumenteeritud, riskihinnatud, läbipaistvad, vaidlustatavad, seiratavad ja PIMS-i kaudu ohjatud, ilma et loodaks dubleerivaid tehisintellektispetsiifilisi juhtimise artefakte.

2.2 Käesolev poliitika tagab, et tehisintellektiga seotud PII töötlemise privaatsuskohustuste täitmist tõendatakse REG02, REG04, REG06, REG07, REG08, REG09, REG10 ja REG12 kaudu.

3. Eesmärgid

3.1 Käesoleva poliitika eesmärgid on:

3.1.1 tuvastada REG02-s tehisintellekti, profiilianalüüsi ja automatiseeritud otsuste tegemisega seotud PII töötlemine;

3.1.2 dokumenteerida REG02-s tehisintellektiga seotud eesmärgid, õiguslik alus, PII kategooriad, andmeallikad, järeldatud andmed, väljundid, saajad ja otsuste mõjud;

3.1.3 käivitada privaatsusriskide eelhindamine ja DPIA suunamine REG04 kaudu;

3.1.4 tagada, et tehisintellektiga seotud privaatsusteated ja sisuline teave registreeritakse REG07-s;

3.1.5 suunata õiguste, vastuväidete, inimese tehtava läbivaatamise ja vaidlustatavuse taotlused REG06 kaudu;

3.1.6 ohjata tehisintellektiga seotud volitatud töötlejaid, alltöötlejaid, tarnijaid ja andmete jagamise kokkuleppeid REG08 kaudu;

3.1.7 suunata tehisintellektiga seotud rahvusvahelised edastamised REG09 kaudu;

3.1.8 eskaleerida kahtlustatavad tehisintellektiga seotud PII intsidendid, väärkasutus, loata avalikustamine ja kahjulikud privaatsustulemused REG10 ja REG12 kaudu;

3.1.9 registreerida seire, erandid, mittevastavused, parandusmeetmed ja täiustused REG12-s.

4. Poliitika põhimõtted

4.1 Tehisintellekti, profiilianalüüsi ja automatiseeritud otsuste tegemise tuvastamine

4.1.1 [Controller] Kui kavandatakse uut või oluliselt muudetud süsteemi, rakendust, mudelit, töövoogu, teenust või äriprotsessi, peab Process Owner / Business Owner kindlaks tegema, kas see kasutab PII-d hõlmavat tehisintellekti, profiilianalüüsi, skoorimist, soovitusi, otsustustuge või automatiseeritud otsuste tegemist, ning registreerima otsuse REG02-s.

4.1.2 [Controller] Enne tehisintellektiga seotud PII töötlemise alustamist peab Process Owner / Business Owner dokumenteerima REG02-s töötlemise eesmärgi, PII kategooriad, isikuandmesubjektide kategooriad, andmeallikad, järeldatud või tuletatud andmete kategooriad, väljundite kategooriad, saajate kategooriad, õigusliku aluse ja seose säilitamisega.

4.1.3 [Controller] Enne profiilianalüüsi, skoorimise, soovituste, otsustustoe või automatiseeritud otsuste tegemise kasutamist tootmiskeskkonnas peab Process Owner / Business Owner dokumenteerima REG02-s ja REG04-s otsuse konteksti, eeldatava mõju isikuandmesubjektidele, inimese osaluse ja õiguste kasutamise tee.

4.1.4 [Joint Controller] Enne tehisintellektiga seotud PII töötlemist koos kaasvastutava töötlejaga peab Privacy Lead / PIMS Manager dokumenteerima REG08-s vastutuse eesmärgi määratlemise, teavitamise, õiguste käsitlemise, DPIA toe, volitatud töötleja juhtimise ja intsidendi eskaleerimise eest.

4.1.5 [Processor] Enne PII töötlemist kliendi jaoks tehisintellektiga seotud teenuse kaudu peab Process Owner / Business Owner kinnitama, et kliendi juhised, lubatud eesmärgid, keelatud kasutused, väljundite käitlemine ja abistamiskohustused on dokumenteeritud REG08-s.

4.1.6 [Both] Enne tehisintellektiga seotud PII töötlemise aktiveerimist peab Privacy Lead / PIMS Manager kinnitama, et töötlemine on seotud kohaldatavate kanooniliste tõendusmaterjali objektidega ning et väljaspool REG02, REG04, REG06, REG07, REG08, REG09, REG10 või REG12 ei looda eraldi tehisintellektispetsiifilist registrit.

4.2 Privaatsusriskide hindamine ja DPIA suunamine

4.2.1 [Controller] Enne tehisintellektiga seotud PII töötlemise käivitamist või olulist muutmist peab Privacy Lead / PIMS Manager tegema privaatsusriskide eelhindamise ja registreerima DPIA otsuse REG04-s.

4.2.2 [Conditional] Kui tehisintellektiga seotud töötlemine hõlmab profiilianalüüsi, automatiseeritud otsuseid, ulatuslikku hindamist, eriliiki andmeid, süüteoandmeid, haavatavaid isikuandmesubjekte, töötajate hindamist, lapsi, käitumise jälgimist, asukohaandmeid, biomeetrilisi andmeid, suure mõjuga skoorimist või olulisi mõjusid, peab Data Protection Officer / Privacy Advisor privaatsusriski läbi vaatama ja registreerima nõuande REG04-s.

4.2.3 [Controller] Enne tehisintellektiga seotud PII töötlemise tootmiskeskkonda kasutuselevõttu peab Process Owner / Business Owner dokumenteerima riskikäsitluse tegevused, jääkriski staatuse ja kasutuselevõtu valmisoleku tõendusmaterjali REG04-s või REG12-s.

4.2.4 [Controller] Enne PII taaskasutamist tehisintellekti koolitamiseks, testimiseks, valideerimiseks, häälestamiseks, seireks või mudeli täiustamiseks uuel või oluliselt muudetud eesmärgil peab Process Owner / Business Owner tegema privaatsuse läbivaatamise ja registreerima otsuse REG02-s ja REG04-s.

4.2.5 [Conditional] Kui privaatsuse jääkrisk jääb pärast kavandatud käsitlemist kõrgeks, peab Top Management enne tootmiskeskkonnas kasutamist selle heaks kiitma, tagasi lükkama või nõudma täiendavat käsitlemist ning registreerima otsuse REG04-s ja REG12-s.

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

9. Erandid

9.1 [All] Enne käesolevas poliitikas sätestatud tehisintellektiga seotud privaatsusnõudest kõrvalekaldumist peab taotluse esitanud Process Owner / Business Owner esitama REG12-s erandi põhjenduse ja kompenseeriva kontrollimeetme tõendusmaterjali.

9.2 [Conditional] Kui erand mõjutab profiilianalüüsi, automatiseeritud otsuste tegemist, inimese tehtavat läbivaatamist, vaidlustatavust, läbipaistvust, DPIA tulemust, suure mõjuga skoorimist, lastega seotud töötlemist, töötajatega seotud töötlemist, volitatud töötleja piiranguid või rahvusvahelisi edastamisi, peab Data Protection Officer / Privacy Advisor erandi läbi vaatama ja registreerima nõuande REG04-s või REG12-s.

9.3 [Conditional] Kui erand loob või säilitab kõrge privaatsuse jääkriski, peab Top Management erandi heaks kiitma või tagasi lükkama ning registreerima otsuse REG04-s ja REG12-s.

9.4 [All] Enne heakskiidetud tehisintellektiga seotud privaatsuserandi aegumist peab Privacy Lead / PIMS Manager läbi vaatama sulgemise, uuendamise või parandusmeetme staatuse ning registreerima tulemuse REG12-s.

10. Järgimise tagamine

10.1 [All] Kui tuvastatakse käesoleva poliitika mittejärgimine, peab Privacy Lead / PIMS Manager registreerima mittevastavuse ja parandusmeetme REG12-s.

10.2 [Both] Kui kahtlustatakse tehisintellektiga seotud PII loata töötlemist, avalikustamist, juurdepääsu, mudeli väärkasutust, õiguste täitmise tõrget või kahjulikku privaatsustulemust, peab Incident Response Coordinator algatama intsidendi eskaleerimise ning registreerima tõendusmaterjali REG10-s ja REG12-s.

10.3 [Both] Kui volitatud töötleja, alltöötleja, tarnija või andmete jagamise saaja ei täida tehisintellektiga seotud privaatsuskohustusi, peab Vendor / Procurement Owner registreerima parandus-, eskaleerimis- või lõpetamistegevuse REG08-s ja REG12-s.

10.4 [All] Kui tekivad korduvad või süsteemsed tehisintellektiga seotud privaatsuse mittevastavused, peab Top Management probleemi läbi vaatama ja registreerima juhtimismeetme REG12-s.

11. Läbivaatamine ja hooldus

11.1 [All] Vähemalt kord aastas peab Privacy Lead / PIMS Manager käesoleva poliitika jätkuva sobivuse läbi vaatama ja registreerima läbivaatamise tulemuse REG12-s.

11.2 [Conditional] Kui õigusaktid, teenused, mudelid, andmeallikad, profiilianalüüsi praktikad, automatiseeritud otsuste tegemise loogika, tarnijakokkulepped, edastamisteed või privaatsusriskid oluliselt muutuvad, peab Privacy Lead / PIMS Manager mõjutatud tehisintellektiga seotud privaatsuskontrollid läbi vaatama ja registreerima tulemuse REG02-s, REG04-s või REG12-s.

11.3 [Controller] Vähemalt kord aastas ja pärast olulisi tehisintellektiga seotud kasutajateekonna muudatusi peab Process Owner / Business Owner läbi vaatama läbipaistvuse, sisulise teabe, inimese tehtava läbivaatamise ja õiguste kasutamise tee tõendusmaterjali ning registreerima läbivaatamise REG06-s ja REG07-s.

11.4 [All] Pärast tehisintellektiga seotud privaatsuse parandusmeetmete sulgemist peab Internal Audit / Compliance Reviewer kontrollima tõhusust ja registreerima kontrollimise tõendusmaterjali REG12-s.

12. Seotud poliitikad

12.1 PII01 - Privaatsusteabe haldussüsteemi poliitika

12.2 PII02 - Privaatsuse rollide, vastutuste ja vastutuse poliitika

12.3 PII03 - PII töötlemisregistri ja õigusliku aluse poliitika

12.4 PII04 - Privaatsusteate ja läbipaistvuse poliitika

12.5 PII05 - Nõusoleku ja eelistuste haldamise poliitika

12.6 PII06 - Isikuandmesubjekti õiguste haldamise poliitika

12.7 PII07 - Privaatsusriskide hindamise ja DPIA poliitika

12.8 PII08 - Lõimitud ja vaikimisi andmekaitse poliitika

12.9 PII09 - PII kogumise, kasutamise, avalikustamise ja jagamise poliitika

12.10 PII10 - PII säilitamise, kustutamise ja kõrvaldamise poliitika

12.11 PII11 - PII täpsuse ja kvaliteedi poliitika

12.12 PII12 - Volitatud töötleja, alltöötleja ja kolmanda osapoole privaatsuse juhtimise poliitika

12.13 PII13 - Rahvusvahelise PII edastamise poliitika

12.14 PII14 - PII turvalisuse ja juurdepääsukontrolli poliitika

12.15 PII15 - PII intsidendi ja rikkumise haldamise poliitika

12.16 PII17 - PIMS-i dokumenteeritud teabe ja tõendusmaterjali haldamise poliitika

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

12.18 PII19 - Töötajate privaatsuspoliitika

12.19 PII20 - Laste privaatsuspoliitika

12.20 PII22 - Turunduse privaatsuse ja küpsiste poliitika

13. Viitestandardid ja raamistikud

13.1 ISO/IEC 27701:2025 - Clause 7.5; Clause 8.1. Addressed by clauses [4.1.6; 4.8.1; 6.1; 7.1; 7.5; 11.1].

13.2 ISO/IEC 27701:2025 - Clause 9.1; Clause 10.2. Addressed by clauses [4.6.2; 4.6.5; 4.8.2; 6.5; 8.1; 8.2; 8.3; 8.4; 8.5; 10.1; 11.4].

13.3 ISO/IEC 27701:2025 - Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.9. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.2.1; 4.2.3; 4.2.4; 4.8.1; 7.1; 7.2].

13.4 ISO/IEC 27701:2025 - Annex A.1.2.7; Annex A.1.2.8. Addressed by clauses [4.1.4; 4.7.1; 4.7.2; 4.7.3; 5.7; 6.3; 7.6].

13.5 ISO/IEC 27701:2025 - Annex A.1.3.2; Annex A.1.3.3; Annex A.1.3.4. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 7.3; 11.3].

13.6 ISO/IEC 27701:2025 - Annex A.1.3.6; Annex A.1.3.7; Annex A.1.3.10; Annex A.1.3.11. Addressed by clauses [4.1.3; 4.3.2; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 7.4; 11.3].

13.7 ISO/IEC 27701:2025 - Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5. Addressed by clauses [4.2.4; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 7.1; 7.5].

13.8 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 [4.7.3; 4.7.4; 4.7.5; 7.7].

13.9 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 [4.1.5; 4.3.5; 4.5.5; 4.7.1; 4.7.2; 5.7; 6.3; 7.6].

13.10 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 [4.3.5; 4.5.5; 4.7.1; 4.7.2; 4.7.4; 4.7.5; 7.6; 7.7].

13.11 ISO/IEC 27701:2025 - Annex A.3.14; Annex A.3.25. Addressed by clauses [4.4.4; 4.6.1; 4.6.3; 4.8.1; 5.4; 7.5; 7.8; 10.2].

13.12 GDPR - Article 4(4); Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(1)(d); Article 5(2). Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.3.1; 4.4.1; 4.4.2; 4.4.5; 4.8.1; 8.1].

13.13 GDPR - Article 6; Article 9; Article 10. Addressed by clauses [4.1.2; 4.2.4; 4.4.3; 4.7.3; 7.1].

13.14 GDPR - Article 12; Article 13; Article 14; Article 15. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.5.2; 4.5.3; 7.3; 11.3].

13.15 GDPR - Article 16; Article 17; Article 18; Article 21; Article 22. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 7.4].

13.16 GDPR - Article 24; Article 25; Article 26; Article 28; Article 30; Article 32; Article 35; Article 39. Addressed by clauses [4.1.4; 4.1.5; 4.2.1; 4.2.2; 4.2.5; 4.4.4; 4.7.1; 4.8.2; 5.3; 6.2; 6.4; 7.2].

13.17 GDPR - Article 44. Addressed by clauses [4.7.4; 7.7; 8.4].

13.18 ISO/IEC 29100:2020 - Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6; Clause 5.7. Addressed by clauses [4.1.2; 4.2.4; 4.4.1; 4.4.2; 4.4.4; 4.4.5; 4.7.5].

13.19 ISO/IEC 29100:2020 - Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.11; Clause 5.12. Addressed by clauses [4.3.1; 4.3.2; 4.5.1; 4.5.2; 4.6.3; 4.8.1; 4.8.2; 8.5; 10.1].

13.20 ISO/IEC 29134:2020 - Clause 5.1; Clause 6.2; Clause 6.3. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.5; 4.6.4; 6.4; 7.2; 9.2].

13.21 ISO/IEC 29151:2022 - Annex A.4; Annex A.5; Annex A.7; Annex A.8; Annex A.10. Addressed by clauses [4.3.1; 4.3.2; 4.4.1; 4.4.2; 4.4.4; 4.4.5; 4.5.2; 4.5.4; 4.7.5].