					Sisestage siia registreeritud juriidilise isiku nimi							
Dokumendi number: PII07					Dokumendi pealkiri: **Privaatsusriskide hindamise ja DPIA 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**

Õiguslik teatis (autoriõigus ja kasutuspiirangud)

(C) 2025 Clarysec LLC. All rights reserved.

Käesolev dokument on Clarysec LLC intellektuaalomand. Selle dokumendi ühtegi osa ei tohi ilma eelneva selgesõnalise kirjaliku loata kopeerida, taaskasutada, levitada ega muuta ärilistel või rakendamise eesmärkidel.

Loata kasutamine on rangelt keelatud ja võib kaasa tuua õiguslikke meetmeid.

Litsentsimise küsimustes võtke ühendust: info@clarysec.com

Kooskõla standardite ja regulatsioonidega

Standard/õigusnorm	Punkt/kontroll/artikkel	Kohaldatavus	Katvuse tüüp	Kommentaar
ISO/IEC 27701:2025	Clause 6.1.1	Both	Primary	PIMS-i riskid ja võimalused
ISO/IEC 27701:2025	Clause 6.1.2	Both	Primary	Privaatsusriskide hindamine
ISO/IEC 27701:2025	Clause 6.1.3	Both	Primary	Privaatsusriskide käsitlemine ja SoA seos
ISO/IEC 27701:2025	Clause 6.3	Both	Supporting	Kavandatud PIMS-i muudatused ja riski kordushindamine
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Privaatsusriski ja DPIA dokumenteeritud teave
ISO/IEC 27701:2025	Clause 8.1	Both	Supporting	Tegevuse planeerimine ja ohje
ISO/IEC 27701:2025	Clause 8.2	Both	Primary	Operatiivne privaatsusriskide hindamine
ISO/IEC 27701:2025	Clause 8.3	Both	Primary	Operatiivne privaatsusriskide käsitlemine
ISO/IEC 27701:2025	Clause 9.1	Both	Supporting	Privaatsusriskide seire ja mõõtmine
ISO/IEC 27701:2025	Clause 9.3	Both	Supporting	Juhtkonnapoolne privaatsusriskide läbivaatamine
ISO/IEC 27701:2025	Clause 10.2	Both	Supporting	Riskiga seotud mittevastavus ja parandusmeede
ISO/IEC 27701:2025	Annex A.1.2.6	Controller	Primary	Privaatsusmõju hindamine
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Supporting	Töötlemiskirjed, mis toetavad riskihindamist
ISO/IEC 27701:2025	Annex A.2.2.2	Processor	Supporting	Volitatud töötleja kliendileping ja DPIA-ga seotud abi
ISO/IEC 27701:2025	Annex A.2.2.6	Processor	Supporting	Volitatud töötleja teave kliendi

				vastavuse toetamiseks
GDPR	Article 5(2)	Controller	Supporting	Vastutuse tõendusmaterjal
GDPR	Article 24	Controller	Supporting	Vastutava töötleja vastutus ja meetmed
GDPR	Article 25	Controller	Supporting	Lõimitud andmekaitse ja vaikimisi andmekaitse
GDPR	Article 28	Both	Supporting	Volitatud töötleja abi ja juhised
GDPR	Article 30	Both	Supporting	DPIA-d toetavad töötlemiskirjed
GDPR	Article 32	Both	Supporting	Turvarisk ja kaitsemeetmed
GDPR	Article 35	Controller	Primary	Andmekaitsealane mõjuhindamine
GDPR	Article 36	Controller	Primary	Eelnev konsulteerimine
GDPR	Article 39	Conditional	Supporting	DPO nõustamine ja seire, kui see on kohaldatav
ISO/IEC 29100:2020	Clause 4.7; Clause 5.11; Clause 5.12	Both	Supporting	Privaatsuse kontrollimeetmed, infoturve ja privaatsusnõuete täitmine
ISO/IEC 29134:2020	Clause 1; Clause 5.1; Clause 6.2; Clause 6.3	Both	Primary	PIA kohaldamisala, kasu, käivitaja ja ettevalmistus
ISO/IEC 29151:2022	Clause 4.1; Clause 4.2	Both	Supporting	PII kaitse programm ja nõuete tuvastamine
ISO/IEC 27557:2022	Clause 4; Clause 5.2; Clause 5.3; Clause 6.4; Clause 6.5; Clause 6.6; Clause 6.7	Both	Supporting	Organisatsioonilise privaatsusriskide juhtimise integreerimine

1. Kohaldamisala

1.1 Käesolev poliitika määrab nõuded privaatsusriskide hindamisele, DPIA vajaduse hindamisele, täiemahulise DPIA tegemisele, riski käsitlemisele, jääkriski aktsepteerimisele, konsulteerimisele, läbivaatamisele ja tõendusmaterjali haldamisele PIMS-i kohaldamisalasse kuuluva PII töötlemise puhul.

1.2 Käesolev poliitika kohaldub järgmisele:

1.2.1 uued ja oluliselt muudetud PII töötlemistoimingud;

1.2.2 vastutava töötleja, kaasvastutava töötleja, volitatud töötleja ja alltöötleja töötlemiskontekstid;

1.2.3 süsteemid, rakendused, teenused, äriprotsessid, tarnijad, volitatud töötlejad, alltöötlejad, rahvusvahelised edastused ja andmejagamise kokkulepped, mis mõjutavad PII töötlemist;

1.2.4 privaatsusriski ja DPIA tõendusmaterjal, mida hoitakse REG04-s, ning toetav tõendusmaterjal, mida hoitakse REG02-s, REG03-s, REG08-s, REG09-s, REG10-s, REG11-s ja REG12-s.

1.3 Käesolev poliitika ei asenda töötlemisregistri kontrollimeetmeid, privaatsusteate kontrollimeetmeid, nõusoleku kontrollimeetmeid, isikuandmesubjektide õiguste kontrollimeetmeid, lõimitud andmekaitse kontrollimeetmeid, tarnijate kontrollimeetmeid, rahvusvahelise edastuse kontrollimeetmeid, PII turbekontrollimeetmeid, intsidendikontrollimeetmeid, dokumenteeritud teabe kontrollimeetmeid ega seire-, auditi- ja parenduskontrollimeetmeid. Need nõuded on määratletud seotud poliitikates, mis on loetletud jaotises 12.

1.4 Käesolevas poliitikas tähendab privaatsusriskide hindamine PII töötlemisest tulenevate võimalike kahjulike privaatsusmõjude dokumenteeritud tuvastamist, analüüsimist, hindamist, käsitlemist, läbivaatamist ja seiret.

1.5 Käesolevas poliitikas tähendab DPIA dokumenteeritud hindamist, mida kasutatakse vastutava töötleja töötlemise puhul, mis tõenäoliselt põhjustab isikuandmesubjektidele suurt riski, ning milles hinnatakse töötlemise vajalikkust, proportsionaalsust, riske, kaitsemeetmeid, jääkriski, konsulteerimisvajadust ja heakskiitmise tingimusi.

1.6 Käesolevas poliitikas tähendab kõrge privaatsuse jääkrisk privaatsusriski, mis jääb pärast kavandatud või rakendatud riskikäsitlust üle kinnitatud aktsepteerimislävendi.

1.7 Käesolevas poliitikas tähendab oluline muudatus mis tahes muudatust, mis mõjutab PIMS-i kohaldamisala, töötlemise eesmärki, õiguslikku alust, PII kategooriaid, isikuandmesubjektide kategooriaid, töötlemise ulatust, töötlemistehnoloogiat, seiret või profiilianalüüsi, automatiseeritud otsuste tegemist, haavatavaid isikuandmesubjekte, vastuvõtjaid, volitatud töötlejaid, alltöötlejaid, rahvusvahelisi edastusi, säilitamist, turbekontrolle, riskiprofiili, kliendi juhiseid või sertifitseerimise kohaldamisala.

2. Eesmärk

2.1 Käesoleva poliitika eesmärk on tagada, et privaatsusriskid ja DPIA kohustused tuvastatakse, hinnatakse, käsitletakse, kinnitatakse, vaadatakse läbi ja tõendatakse enne seda, kui PII töötlemine tekitab isikuandmesubjektidele või PIMS-ile lubamatu riski.

2.2 Käesolev poliitika võimaldab organisatsioonil tõendada riskipõhist privaatsuse juhtimist, vastutava töötleja DPIA vastutust, volitatud töötleja DPIA-ga seotud abi, dokumenteeritud riskikäsitlust, jääkriski heakskiitmist, eelneva konsulteerimise otsustamist ning privaatsuskontrollide pidevat täiustamist.

3. Eesmärgid

3.1 Käesoleva poliitika eesmärgid on järgmised:

3.1.1 määratleda kohustuslikud privaatsusriski sõelumise käivitajad;

3.1.2 määratleda, millal on nõutav täiemahuline DPIA;

3.1.3 tagada, et vastutava töötleja DPIA otsused dokumenteeritakse ja on läbivaadatavad;

3.1.4 tagada, et volitatud töötleja ja alltöötleja DPIA-ga seotud abi dokumenteeritakse, kui seda nõuab kliendi juhis või leping;

3.1.5 tagada, et privaatsusriskid hinnatakse enne uue või oluliselt muudetud PII töötlemise jätkamist;

3.1.6 tagada, et privaatsusriskide käsitlused määratakse, rakendatakse ja kontrollitakse;

3.1.7 tagada, et kõrged privaatsuse jääkriskid eskaleeritakse ja kinnitatakse enne töötlemise alustamist või jätkamist;

3.1.8 tagada, et eelneva konsulteerimise otsused dokumenteeritakse, kui kõrge jääkrisk püsib;

3.1.9 tagada, et privaatsusriski ja DPIA tõendusmaterjali hoitakse REG04-s ning seotakse seotud tõendusobjektidega;

3.1.10 vältida eraldi DPIA-, riski- või konsulteerimisregistrite loomist väljaspool REG04.

4. Poliitika põhimõtted

4.1 Privaatsusriski sõelumine

4.1.1 [Both] Process Owner / Business Owner PEAB algatama privaatsusriski sõelumise REG04-s enne REG02-s registreeritud uue või oluliselt muudetud PII töötlemise alustamist.

4.1.2 [Both] Privacy Lead / PIMS Manager PEAB hoidma privaatsusriski sõelumiskriteeriume REG04-s enne PIMS-i esmast käitamist ja seejärel kord aastas.

4.1.3 [Controller] Process Owner / Business Owner PEAB lõpule viima DPIA vajaduse hindamise REG04-s enne sellise vastutava töötleja töötlemise alustamist, mis vastab privaatsusriski sõelumiskriteeriumidele.

4.1.4 [Processor] Vendor / Procurement Owner PEAB registreerima kliendi DPIA-ga seotud abi nõuded REG08-s enne volitatud töötleja töötlemise alustamist, kui kliendileping või dokumenteeritud juhis nõuab DPIA tuge.

4.1.5 [Both] System Owner / Application Owner PEAB esitama süsteemi disaini, juurdepääsu, turbe, logimise ja andmevoogude tõendusmaterjali REG04-s enne privaatsusriskide hindamise heakskiitmist uute või oluliselt muudetud PII-d töötlevate süsteemide puhul.

4.1.6 [Both] Privacy Lead / PIMS Manager PEAB registreerima sõelumise tulemuse ja täiemahulise DPIA otsuse põhjenduse REG04-s enne töötlemistoimingu jätkamist.

4.2 DPIA käivitajad ja nõude kindlaksmääramine

4.2.1 [Controller] Privacy Lead / PIMS Manager PEAB nõudma täiemahulist DPIA-d REG04-s enne sellise vastutava töötleja töötlemise alustamist, mis tõenäoliselt põhjustab suurt riski.

4.2.2 [Controller] Process Owner / Business Owner PEAB suunama suuremahulise töötlemise, süstemaatilise seire, profiilianalüüsi, automatiseeritud otsused, eriliiki PII, süüdimõistvate kohtuotsuste või süütegudega seotud andmed, haavatavad isikuandmesubjektid, innovaatilise tehnoloogia või oluliselt muudetud töötlemise rollile Privacy Lead / PIMS Manager REG04-s enne töötlemise alustamist.

4.2.3 [Controller] Data Protection Officer / Privacy Advisor PEAB registreerima nõuande REG04-s enne kõrge riskiga vastutava töötleja töötlemise täiemahulise DPIA nõude otsuse heakskiitmist.

4.2.4 [Both] Process Owner / Business Owner PEAB privaatsusriski REG04-s uuesti sõeluma enne PII kasutamist uuel eesmärgil, uue vastuvõtja lisamist, uue volitatud töötleja või alltöötleja kaasamist, süsteemiarhitektuuri muutmist või uue rahvusvahelise edastuse alustamist.

4.2.5 [Processor] Privacy Lead / PIMS Manager PEAB dokumenteerima REG08-s 10 tööpäeva jooksul pärast kliendi DPIA-ga seotud abitaotluse saamist, kas volitatud töötleja DPIA tugi on nõutav.

4.2.6 [Subprocessor] Vendor / Procurement Owner PEAB dokumenteerima ülesvoolu DPIA-ga seotud abi nõuded REG08-s enne alltöötlemise alustamist, kui ülesvoolu klient või volitatud töötleja leping nõuab sellist abi.

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

9. Erandid

9.1 Privaatsusriski ja DPIA erandid

9.1.1 [All] Process Owner / Business Owner PEAB taotlema mis tahes erandit käesolevast poliitikast REG12-s enne kõrvalekalde tekkimist.

9.1.2 [All] Privacy Lead / PIMS Manager PEAB hindama iga taotletud erandi privaatsus-, õiguslikku, sertifitseerimise, operatiivset ja isikuandmesubjektile avalduvat mõju REG04-s või REG12-s 10 tööpäeva jooksul pärast taotlust.

9.1.3 [All] Data Protection Officer / Privacy Advisor PEAB registreerima nõuande REG12-s enne mis tahes erandi heakskiitmist, mis mõjutab kõrge riskiga töötlemist, täiemahulise DPIA lõpetamist, eelnevat konsulteerimist, kõrget privaatsuse jääkriski või kliendi DPIA-ga seotud abi.

9.1.4 [All] Top Management PEAB kinnitama REG12-s privaatsusriski või DPIA erandid, mis mõjutavad kõrge riskiga töötlemist, sertifitseerimise kohaldamisala, eelnevat konsulteerimist või lahendamata kõrget privaatsuse jääkriski, enne erandi jõustumist.

9.1.5 [All] Privacy Lead / PIMS Manager PEAB määrama iga heakskiidetud privaatsusriski või DPIA erandi jaoks REG12-s enne heakskiitmist aegumiskuupäeva, mis ei ületa 90 päeva.

9.1.6 [All] Process Owner / Business Owner PEAB sulgema või uuesti hindama iga privaatsusriski või DPIA erandi REG12-s viie tööpäeva jooksul pärast aegumist.

10. Järgimise tagamine

10.1 Privaatsusriski ja DPIA järgimise tagamine

10.1.1 [All] Privacy Lead / PIMS Manager PEAB registreerima puuduva, ebatäpse, mittetäieliku, tähtaja ületanud või kinnitamata REG04 privaatsusriski või DPIA tõendusmaterjali mittevastavusena REG12-s viie tööpäeva jooksul pärast tuvastamist.

10.1.2 [Controller] Process Owner / Business Owner PEAB peatama uue kõrge riskiga vastutava töötleja töötlemise, kui nõutav REG04 DPIA heakskiidu tõendusmaterjal enne käivitamist puudub.

10.1.3 [Both] System Owner / Application Owner PEAB blokeerima PII-d töötlevate süsteemide tootmiskeskkonda kasutuselevõtu, kui nõutav REG04 riskikäsitluse tõendusmaterjal puudub enne tootmiskeskkonda kasutuselevõtu heakskiitmist.

10.1.4 [Both] Vendor / Procurement Owner PEAB blokeerima tarnija, volitatud töötleja, alltöötleja või andmejagamise kaasamise, kui nõutav REG04 privaatsusriski või DPIA-ga seotud abi tõendusmaterjal puudub enne lepingu heakskiitmist.

10.1.5 [All] Top Management PEAB juhtkonnapoolse läbivaatamise käigus REG12-s läbi vaatama lahendamata olulised privaatsusriski või DPIA mittevastavused.

10.1.6 [All] Privacy Lead / PIMS Manager PEAB eskaleerima korduvad REG04 sõelumise, DPIA läbivaatamise või riskikäsitluse tähtaegade ületamised rollile Top Management REG12-s viie tööpäeva jooksul pärast teist esinemist 12-kuulise perioodi jooksul.

10.1.7 [All] Internal Audit / Compliance Reviewer PEAB kontrollima privaatsusriski ja DPIA mittevastavuste parandusmeetmete tõhusust REG12-s järgmisel kavandatud auditil või 60 päeva jooksul pärast sulgemist, olenevalt sellest, kumb toimub varem.

11. Läbivaatamine ja haldus

11.1 Poliitika läbivaatamine ja haldus

11.1.1 [All] Privacy Lead / PIMS Manager PEAB käesoleva poliitika REG12-s läbi vaatama kord aastas ning 30 päeva jooksul pärast olulist muudatust privaatsusriski, DPIA, eelneva konsulteerimise, volitatud töötleja abi või sertifitseerimisnõuete osas.

11.1.2 [All] Privacy Lead / PIMS Manager PEAB läbi vaatama REG04 sõelumiskriteeriumid, DPIA käivituskriteeriumid, riskihinnangu kriteeriumid ja jääkriski aktsepteerimise kriteeriumid REG12-s kord aastas.

11.1.3 [All] Data Protection Officer / Privacy Advisor PEAB enne heakskiitmist REG12-s läbi vaatama käesoleva poliitika privaatsuse seisukohast olulised muudatused.

11.1.4 [All] Top Management PEAB kinnitama käesoleva poliitika olulised muudatused REG12-s enne avaldamist.

11.1.5 [All] Privacy Lead / PIMS Manager PEAB ajakohastama REG03 ja REG04 15 tööpäeva jooksul pärast heakskiidetud poliitikamuudatusi, mis muudavad kontrollimeetmete kohaldatavust, riskikriteeriume või DPIA sõelumisnõudeid.

11.1.6 [All] Privacy Lead / PIMS Manager PEAB registreerima käesoleva poliitika heakskiidetud muudatuste teavitamise REG11-s 30 päeva jooksul pärast avaldamist.

12. Seotud poliitikad

12.1 Käesolevat poliitikat toetavad järgmised seotud poliitikad:

12.1.1 PII01 - Privaatsusteabe haldussüsteemi poliitika

12.1.2 PII02 - Privaatsusrollide, vastutuste ja vastutuse poliitika

12.1.3 PII03 - PII töötlemisregistri ja õigusliku aluse poliitika

12.1.4 PII04 - Privaatsusteate ja läbipaistvuse poliitika

12.1.5 PII05 - Nõusoleku ja eelistuste haldamise poliitika

12.1.6 PII06 - Isikuandmesubjektide õiguste haldamise poliitika

12.1.7 PII08 - Lõimitud andmekaitse ja vaikimisi andmekaitse poliitika

12.1.8 PII09 - PII kogumise, kasutamise, avaldamise ja jagamise poliitika

12.1.9 PII10 - PII säilitamise, kustutamise ja kõrvaldamise poliitika

12.1.10 PII11 - PII täpsuse ja kvaliteedi poliitika

12.1.11 PII12 - Volitatud töötleja, alltöötleja ja kolmanda osapoole privaatsushalduse poliitika

12.1.12 PII13 - Rahvusvahelise PII edastuse poliitika

12.1.13 PII14 - PII turbe ja juurdepääsukontrolli poliitika

12.1.14 PII15 - PII intsidendi ja rikkumise haldamise poliitika

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

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

13. Viitestandardid ja raamistikud

13.1 Käesolev poliitika on vastendatud järgmiste standardite ja regulatsioonidega. Vastendus selgitab, kuidas poliitika toetab viidatud nõudeid, ning tuvastab sisemised punktid, mis neid rakendavad või toetavad.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 6.1.1** - Vastendatud privaatsusriskide ja võimaluste tuvastamisele ning nendega seotud tegevuste kavandamisele, kasutades sõelumiskriteeriume, riskilävendeid, eskaleerimist ja juhtkonnapoolse läbivaatamise sisendeid. Addressed by clauses [4.1.2; 4.4.5; 4.5.6; 6.1.1; 6.1.2; 8.1.2].

13.2.2 **Clause 6.1.2** - Vastendatud privaatsusriski sõelumise, privaatsusriskide hindamise, riskihinnangu, kordushindamise ja DPIA käivitaja hindamise tegemisele enne uue või oluliselt muudetud töötlemise jätkamist. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.6; 4.2.1; 4.2.4; 4.3.1; 4.3.7; 4.6.1].

13.2.3 **Clause 6.1.3** - Vastendatud privaatsusriski käsitlemise planeerimisele, kontrollimeetmete kohaldatavuse ajakohastamisele, käsitluse rakendamisele, jääkriski aktsepteerimisele ja SoA seosele. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 6.1.5; 7.1.7; 11.1.5].

13.2.4 **Clause 6.3** - Vastendatud kavandatud PIMS-i ja töötlemise muudatustele, mis käivitavad privaatsusriski kordushindamise ja DPIA läbivaatamise. Addressed by clauses [4.2.4; 4.6.1; 11.1.1].

13.2.5 **Clause 7.5** - Vastendatud kontrollitud dokumenteeritud teabele privaatsusriski sõelumise, DPIA tõendusmaterjali, riskikäsitluse, jääkriski aktsepteerimise, eelneva konsulteerimise otsuste, erandite, mittevastavuste ja poliitika läbivaatamise tõendusmaterjali kohta. Addressed by clauses [4.1.6; 4.3.7; 4.4.1; 4.5.1; 5.1.2; 7.1.1; 9.1.1; 10.1.1; 11.1.1].

13.2.6 **Clause 8.1** - Vastendatud privaatsusriski ja DPIA kontrollimeetmete toimimisele enne tootmiskeskkonda kasutuselevõttu, kaasamist, töötlemise heakskiitmist, käsitluse sulgemist ja parandusmeetmetega sidumist. Addressed by clauses [4.1.1; 4.1.5; 7.1.2; 7.1.3; 7.1.4; 7.1.5; 7.1.6; 7.1.7; 7.1.8].

13.2.7 **Clause 8.2** - Vastendatud operatiivsele privaatsusriskide hindamisele uute, muudetud, süsteemi-, tarnija-, edastus- ja intsidendipõhiste töötlemismuudatuste puhul. Addressed by clauses [4.1.1; 4.2.4; 4.3.1; 4.3.5; 4.5.5; 4.6.1].

13.2.8 **Clause 8.3** - Vastendatud operatiivsele privaatsusriski käsitlemisele, käsitluse määramisele, käsitluse rakendamisele, tähtaja ületanud käsitluse eskaleerimisele ja tõhususe kontrollimisele. Addressed by clauses [4.4.1; 4.4.3; 4.4.4; 4.4.6; 4.4.7; 8.1.3; 10.1.7].

13.2.9 **Clause 9.1** - Vastendatud sõelumise katvuse, DPIA staatuse, avatud riskide, tähtaja ületanud käsitlustegevuste, tarnijategevuste, turbekäsitluse tegevuste, intsidendi kordushindamise tegevuste ja auditileidude seirele ja mõõtmisele. Addressed by clauses [4.6.3; 4.6.4; 4.6.5; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 8.1.6; 8.1.7; 8.1.8].

13.2.10 **Clause 9.3** - Vastendatud juhtkonnapoolsele läbivaatamisele, mis hõlmab kõrgeid privaatsuse jääkriske, tähtaja ületanud käsitlustegevusi, täiemahulise DPIA staatust, eelneva konsulteerimise otsuseid ja olulisi privaatsusriski erandeid. Addressed by clauses [4.6.6; 6.1.1; 6.1.2; 6.1.3; 10.1.5].

13.2.11 **Clause 10.2** - Vastendatud privaatsusriski ja DPIA mittevastavustele, eranditele, parandusmeetme avamisele, eskaleerimisele ja tõhususe kontrollimisele. Addressed by clauses [4.4.6; 9.1.1; 9.1.2; 9.1.4; 9.1.6; 10.1.1; 10.1.5; 10.1.6; 10.1.7].

13.2.12 **Annex A.1.2.6** - Vastendatud privaatsusmõju hindamise vajaduse hindamisele ja vajaduse korral rakendamisele uue või muudetud vastutava töötleja töötlemise puhul. Addressed by clauses [4.1.3; 4.2.1; 4.2.2; 4.2.3; 4.3.2; 4.5.1; 4.6.2; 7.1.4; 10.1.2].

13.2.13 **Annex A.1.2.9** - Vastendatud töötlemiskirjetele, mis toetavad privaatsusriski ja DPIA hindamise sisendeid, sealhulgas eesmärki, kategooriaid, süsteeme, vastuvõtjaid, edastusi ja tarnijaid. Addressed by clauses [4.3.1; 6.1.4; 8.1.1].

13.2.14 **Annex A.2.2.2** - Vastendatud volitatud töötleja kliendilepingutele ja kliendi DPIA-ga seotud abi kohustustele. Addressed by clauses [4.1.4; 4.2.5; 4.5.4; 5.1.7; 7.1.6].

13.2.15 **Annex A.2.2.6** - Vastendatud volitatud töötleja poolt kliendi vastavuseks vajaliku teabe esitamisele, sealhulgas DPIA-ga seotud abi ja klienditoe tõendusmaterjalile. Addressed by clauses [4.2.5; 4.2.6; 4.5.4; 8.1.5].

13.3 GDPR

13.3.1 **Article 5(2)** - Vastendatud vastutuse tõendusmaterjalile DPIA sõelumise, täiemahulise DPIA otsuste, riskikäsitluse, jääkriski aktsepteerimise, eelneva konsulteerimise otsuste, erandite, auditileidude ja parandusmeetmete kohta. Addressed by clauses [4.1.6; 4.3.7; 4.4.5; 4.5.1; 4.6.4; 10.1.1; 10.1.7].

13.3.2 **Article 24** - Vastendatud vastutava töötleja vastutusele asjakohaste privaatsusriski meetmete, kõrge jääkriski läbivaatamise, juhtkonna heakskiidu ja poliitika halduse eest. Addressed by clauses [4.4.5; 4.5.3; 6.1.2; 10.1.5; 11.1.4].

13.3.3 **Article 25** - Vastendatud lõimitud andmekaitse ja vaikimisi andmekaitse tõendusmaterjalile, mida kasutatakse riskihindamisel ja enne tootmiskeskkonda kasutuselevõtu heakskiitmist. Addressed by clauses [4.1.5; 4.3.4; 7.1.5].

13.3.4 **Article 28** - Vastendatud volitatud töötleja ja alltöötleja DPIA-ga seotud abile, kliendi juhiste käsitlemisele ja tarnija riskikäsitluse tõendusmaterjalile. Addressed by clauses [4.1.4; 4.2.5; 4.2.6; 4.4.4; 4.5.4; 7.1.6; 8.1.5].

13.3.5 **Article 30** - Vastendatud töötlemiskirjetele, mis toetavad privaatsusriskide hindamise ja DPIA sisendeid. Addressed by clauses [4.3.1; 6.1.4; 8.1.1].

13.3.6 **Article 32** - Vastendatud PII turvariski sisenditele, kaitsemeetmete valikule, turvariski käsitlemisele ja turbekontrolli staatuse ajakohastamisele. Addressed by clauses [4.1.5; 4.3.3; 4.4.2; 8.1.6].

13.3.7 **Article 35** - Vastendatud DPIA vajaduse hindamisele, täiemahulise DPIA nõude kindlaksmääramisele, DPIA sisule, DPO nõuandele, läbivaatamisele ja kõrge riskiga töötlemise blokeerimisele ilma nõutava DPIA heakskiiduta. Addressed by clauses [4.1.3; 4.2.1; 4.2.2; 4.2.3; 4.3.2; 4.3.6; 4.5.1; 4.6.2; 7.1.4; 10.1.2].

13.3.8 **Article 36** - Vastendatud eelneva konsulteerimise otsustamisele, DPO nõuandele, Top Management heakskiidule ning jätkamise, peatamise, ümberkujundamise või konsulteerimise tegevustele, kui kõrge jääkrisk püsib. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 6.1.2].

13.3.9 **Article 39** - Vastendatud Data Protection Officer / Privacy Advisor nõustamisele ja seirele, kui see on kohaldatav, DPIA otsuste, kõrge riskiga töötlemise, eelneva konsulteerimise ja poliitikamuudatuste puhul. Addressed by clauses [4.2.3; 4.3.6; 4.5.2; 5.1.3; 6.1.3; 9.1.3; 11.1.3].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 4.7; Clause 5.11; Clause 5.12** - Vastendatud privaatsuse kontrollimeetmete tuvastamisele, turbekaitsemeetmetele, privaatsusnõuete täitmisele, privaatsusriski tõendusmaterjalile, seirele ja läbivaatamisele. Addressed by clauses [4.3.3; 4.4.1; 4.4.2; 4.4.7; 4.6.3; 4.6.5; 8.1.6; 10.1.7].

13.5 ISO/IEC 29134:2020

13.5.1 **Clause 1; Clause 5.1; Clause 6.2; Clause 6.3** - Vastendatud PIA protsessi kohaldamisalale, kasule, käivitaja kindlaksmääramisele, ettevalmistamisele, hindamise sisenditele, sidusrühmade tõendusmaterjalile ja REG04-s hoitavale DPIA aruande struktuurile. Addressed by clauses [4.1.1; 4.1.3; 4.1.6; 4.2.1; 4.3.1; 4.3.2; 4.3.7; 7.1.1].

13.6 ISO/IEC 29151:2022

13.6.1 **Clause 4.1; Clause 4.2** - Vastendatud PII kaitse programmi nõuetele, PII kaitse nõuete tuvastamisele, riskipõhisele kontrollimeetmete valikule ja privaatsusriski käsitluse seosele. Addressed by clauses [4.3.3; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 6.1.5].

13.7 ISO/IEC 27557:2022

13.7.1 **Clause 4; Clause 5.2; Clause 5.3; Clause 6.4; Clause 6.5; Clause 6.6; Clause 6.7** - Vastendatud organisatsioonilistele privaatsusriski põhimõtetele, juhtimisele, integreerimisele, riskihindamisele, riskikäsitlusele, seirele ja läbivaatamisele ning registreerimisele ja aruandlusele. Addressed by clauses [4.1.2; 4.3.1; 4.3.7; 4.4.1; 4.4.5; 4.6.3; 4.6.4; 5.1.1; 6.1.1; 6.1.2; 8.1.1; 8.1.3].