					Čia įrašykite registruoto juridinio asmens pavadinimą						
Dokumento numeris: PII07					Dokumento pavadinimas: **Privatumo rizikos vertinimo ir poveikio duomenų apsaugai vertinimo (DPIA) 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

Standard / Regulation	Clause / Control / Article	Applicability	Coverage Type	Comment
ISO/IEC 27701:2025	Clause 6.1.1	Both	Primary	PIMS rizikos ir galimybės
ISO/IEC 27701:2025	Clause 6.1.2	Both	Primary	Privatumo rizikos vertinimas
ISO/IEC 27701:2025	Clause 6.1.3	Both	Primary	Privatumo rizikos tvarkymas ir SoA sąsaja
ISO/IEC 27701:2025	Clause 6.3	Both	Supporting	Planuojami PIMS pakeitimai ir pakartotinis rizikos vertinimas
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Dokumentuota privatumo rizikos ir DPIA informacija
ISO/IEC 27701:2025	Clause 8.1	Both	Supporting	Operacijų planavimas ir kontrolė
ISO/IEC 27701:2025	Clause 8.2	Both	Primary	Operacinis privatumo rizikos vertinimas
ISO/IEC 27701:2025	Clause 8.3	Both	Primary	Operacinis privatumo rizikos tvarkymas
ISO/IEC 27701:2025	Clause 9.1	Both	Supporting	Privatumo rizikos stebėsena ir matavimas
ISO/IEC 27701:2025	Clause 9.3	Both	Supporting	Vadovybės atliekama privatumo rizikos peržiūra
ISO/IEC 27701:2025	Clause 10.2	Both	Supporting	Su rizika susijusi neatitiktis ir korekciniai veiksmai
ISO/IEC 27701:2025	Annex A.1.2.6	Controller	Primary	Poveikio privatumui vertinimas
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Supporting	Tvarkymo įrašai, pagrindžiantys rizikos vertinimą
ISO/IEC 27701:2025	Annex A.2.2.2	Processor	Supporting	Duomenų tvarkytojo kliento

				sutartis ir pagalba DPIA klausimais
ISO/IEC 27701:2025	Annex A.2.2.6	Processor	Supporting	Duomenų tvarkytojo informacija, pagrindžianti kliento atitiktį
GDPR	Article 5(2)	Controller	Supporting	Atskaitomybės įrodymai
GDPR	Article 24	Controller	Supporting	Duomenų valdytojo atsakomybė ir priemonės
GDPR	Article 25	Controller	Supporting	Duomenų apsauga pagal projektavimą ir pagal numatytuosius nustatymus
GDPR	Article 28	Both	Supporting	Duomenų tvarkytojo pagalba ir nurodymai
GDPR	Article 30	Both	Supporting	Tvarkymo įrašai, pagrindžiantys DPIA
GDPR	Article 32	Both	Supporting	Saugumo rizika ir apsaugos priemonės
GDPR	Article 35	Controller	Primary	Poveikio duomenų apsaugai vertinimas
GDPR	Article 36	Controller	Primary	Išankstinė konsultacija
GDPR	Article 39	Conditional	Supporting	DPO konsultacijos ir stebėsena, kai taikoma
ISO/IEC 29100:2020	Clause 4.7; Clause 5.11; Clause 5.12	Both	Supporting	Privatumo kontrolės priemonės, informacijos saugumas ir privatumo atitiktis
ISO/IEC 29134:2020	Clause 1; Clause 5.1; Clause 6.2; Clause 6.3	Both	Primary	PIA taikymo sritis, nauda, paleidiklis ir pasirengimas
ISO/IEC 29151:2022	Clause 4.1; Clause 4.2	Both	Supporting	PII apsaugos programa ir

				reikalavimų nustatymas
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	Organizacinio privatumo rizikos valdymo integravimas

1. Taikymo sritis

1.1 Ši politika nustato privatumo rizikos vertinimo, pirminio DPIA poreikio vertinimo, išsamaus poveikio duomenų apsaugai vertinimo (DPIA) atlikimo, rizikos tvarkymo, liekamosios rizikos priėmimo, konsultacijų, peržiūros ir įrodymų valdymo reikalavimus PII tvarkymui PIMS taikymo srityje.

1.2 Ši politika taikoma:

1.2.1 naujoms ir iš esmės pakeistoms PII tvarkymo veikloms;

1.2.2 duomenų valdytojo, bendro duomenų valdytojo, duomenų tvarkytojo ir subtvarkytojo tvarkymo kontekstams;

1.2.3 sistemoms, taikomosioms programoms, paslaugoms, verslo procesams, tiekėjams, duomenų tvarkytojams, subtvarkytojams, tarptautiniams perdavimams ir dalijimosi duomenimis susitarimams, kurie turi įtakos PII tvarkymui;

1.2.4 privatumo rizikos ir DPIA įrodymams, saugomiems REG04, ir pagalbinei įrodymų medžiagai, saugomai REG02, REG03, REG08, REG09, REG10, REG11 ir REG12.

1.3 Ši politika nepakeičia tvarkymo veiklos apskaitos kontrolės priemonių, privatumo pranešimo kontrolės priemonių, sutikimų kontrolės priemonių, duomenų subjektų teisių kontrolės priemonių, privatumo pagal projektavimą kontrolės priemonių, tiekėjų kontrolės priemonių, tarptautinio perdavimo kontrolės priemonių, PII saugumo kontrolės priemonių, incidentų kontrolės priemonių, dokumentuotos informacijos kontrolės priemonių ar stebėsenos / audito / tobulinimo kontrolės priemonių. Šie reikalavimai nustatyti susijusiose politikose, išvardytose 12 skyriuje.

1.4 Šioje politikoje privatumo rizikos vertinimas reiškia dokumentuotą galimo neigiamo poveikio privatumui, kylančio dėl PII tvarkymo, nustatymą, analizę, įvertinimą, tvarkymą, peržiūrą ir stebėseną.

1.5 Šioje politikoje DPIA reiškia dokumentuotą vertinimą, naudojamą duomenų valdytojo atliekamam tvarkymui, kuris gali kelti didelę riziką duomenų subjektams, ir kuriuo įvertinamas tvarkymo būtinumas, proporcingumas, rizikos, apsaugos priemonės, liekamoji rizika, konsultacijų poreikis ir patvirtinimo sąlygos.

1.6 Šioje politikoje didelė liekamoji privatumo rizika reiškia privatumo riziką, kuri po pasiūlyto arba įgyvendinto rizikos tvarkymo lieka didesnė už patvirtintą priėmimo slenkstį.

1.7 Šioje politikoje esminis pokytis reiškia bet kokį pakeitimą, darantį poveikį PIMS taikymo sričiai, tvarkymo tikslui, teisiniam pagrindui, PII kategorijoms, duomenų subjektų kategorijoms, tvarkymo mastui, tvarkymo technologijai, stebėsenai ar profiliavimui, automatizuotam sprendimų priėmimui, pažeidžiamiems duomenų subjektams, gavėjams, duomenų tvarkytojams, subtvarkytojams, tarptautiniams perdavimams, saugojimui, saugumo kontrolės priemonėms, rizikos profiliui, kliento nurodymams arba sertifikavimo taikymo sričiai.

2. Tikslas

2.1 Šios politikos tikslas – užtikrinti, kad privatumo rizikos ir DPIA pareigos būtų nustatytos, įvertintos, sutvarkytos, patvirtintos, peržiūrėtos ir pagrįstos įrodymais prieš PII tvarkymui sukeliant nepriimtiną riziką duomenų subjektams arba PIMS.

2.2 Ši politika leidžia organizacijai įrodyti rizika grindžiamą privatumo valdyseną, duomenų valdytojo atskaitomybę už DPIA, duomenų tvarkytojo pagalbą DPIA klausimais, dokumentuotą rizikos tvarkymą, liekamosios rizikos patvirtinimą, sprendimų dėl išankstinės konsultacijos priėmimą ir nuolatinį privatumo kontrolės priemonių tobulinimą.

3. Tikslai

3.1 Šios politikos tikslai yra:

3.1.1 apibrėžti privalomus pirminio privatumo rizikos vertinimo paleidiklius;

3.1.2 apibrėžti, kada reikalingas išsamus poveikio duomenų apsaugai vertinimas (DPIA);

3.1.3 užtikrinti, kad duomenų valdytojo DPIA sprendimai būtų dokumentuoti ir tinkami peržiūrai;

3.1.4 užtikrinti, kad duomenų tvarkytojo ir subtvarkytojo pagalba DPIA klausimais būtų dokumentuota, kai to reikalaujama pagal kliento nurodymą arba susitarimą;

3.1.5 užtikrinti, kad privatumo rizikos būtų įvertintos prieš pradedant naują arba iš esmės pakeistą PII tvarkymą;

3.1.6 užtikrinti, kad privatumo rizikos tvarkymo veiksmai būtų priskirti, įgyvendinti ir patikrinti;

3.1.7 užtikrinti, kad didelės liekamosios privatumo rizikos būtų eskaluotos ir patvirtintos prieš pradedant arba tęsiant tvarkymą;

3.1.8 užtikrinti, kad sprendimai dėl išankstinės konsultacijos būtų dokumentuoti tais atvejais, kai išlieka didelė liekamoji rizika;

3.1.9 užtikrinti, kad privatumo rizikos ir DPIA įrodymai būtų saugomi REG04 ir susieti su susijusiais įrodymų objektais;

3.1.10 vengti atskirų DPIA, rizikos ar konsultacijų registrų kūrimo už REG04 ribų.

4. Politikos nuostatos

4.1 Pirminis privatumo rizikos vertinimas

4.1.1 [Both] Process Owner / Business Owner MUST inicijuoti pirminį privatumo rizikos vertinimą REG04 prieš pradedant naują arba iš esmės pakeistą PII tvarkymą, įregistruotą REG02.

4.1.2 [Both] Privacy Lead / PIMS Manager MUST palaikyti pirminio privatumo rizikos vertinimo kriterijus REG04 prieš pradinį PIMS veikimą ir vėliau kasmet.

4.1.3 [Controller] Process Owner / Business Owner MUST atlikti pirminį DPIA poreikio vertinimą REG04 prieš pradedant duomenų valdytojo tvarkymą, atitinkantį pirminio privatumo rizikos vertinimo kriterijus.

4.1.4 [Processor] Vendor / Procurement Owner MUST įrašyti kliento pagalbos DPIA klausimais reikalavimus REG08 prieš pradedant duomenų tvarkytojo tvarkymą, kai kliento sutartyje arba dokumentuotame nurodyme reikalaujama DPIA pagalbos.

4.1.5 [Both] System Owner / Application Owner MUST pateikti sistemos projektavimo, prieigos, saugumo, žurnalavimo ir duomenų srautų įrodymus REG04 prieš patvirtinant privatumo rizikos vertinimą naujoms arba iš esmės pakeistoms sistemoms, tvarkančioms PII.

4.1.6 [Both] Privacy Lead / PIMS Manager MUST įrašyti pirminio vertinimo rezultatą ir išsamaus DPIA sprendimo pagrindimą REG04 prieš tęsiant tvarkymo veiklą.

4.2 DPIA paleidikliai ir reikalavimo nustatymas

4.2.1 [Controller] Privacy Lead / PIMS Manager MUST reikalauti išsamaus poveikio duomenų apsaugai vertinimo (DPIA) REG04 prieš pradedant duomenų valdytojo tvarkymą, kuris gali kelti didelę riziką.

4.2.2 [Controller] Process Owner / Business Owner MUST nukreipti tvarkymą, apimantį didelį mastą, sistemingą stebėseną, profiliavimą, automatizuotus sprendimus, specialių kategorijų PII, duomenis apie apkaltinamuosius nuosprendžius ar nusikalstamas veikas, pažeidžiamus duomenų subjektus, inovatyvias technologijas arba iš esmės pakeistą tvarkymą, Privacy Lead / PIMS Manager vertinimui REG04 prieš pradedant tvarkymą.

4.2.3 [Controller] Data Protection Officer / Privacy Advisor MUST įrašyti konsultaciją REG04 prieš patvirtinant sprendimą dėl išsamaus DPIA reikalavimo didelės rizikos duomenų valdytojo tvarkymui.

4.2.4 [Both] Process Owner / Business Owner MUST pakartotinai atlikti pirminį privatumo rizikos vertinimą REG04 prieš naudodamas PII naujam tikslui, pridėdamas naują gavėją, įtraukdamas naują duomenų tvarkytoją arba subtvarkytoją, keisdamas sistemos architektūrą arba pradėdamas naują tarptautinį perdavimą.

4.2.5 [Processor] Privacy Lead / PIMS Manager MUST dokumentuoti REG08, ar reikalinga duomenų tvarkytojo pagalba DPIA klausimais, per 10 darbo dienų nuo kliento prašymo suteikti DPIA pagalbą gavimo.

4.2.6 [Subprocessor] Vendor / Procurement Owner MUST dokumentuoti aukštesnės grandies DPIA pagalbos reikalavimus REG08 prieš pradedant subtvarkymą, kai tokios pagalbos reikalaujama pagal aukštesnės grandies kliento arba duomenų tvarkytojo sutartį.

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

9. Išimtys

9.1 Privatumo rizikos ir DPIA išimtys

9.1.1 [All] Process Owner / Business Owner MUST prašyti bet kokios šios politikos išimties REG12 prieš nukrypimui įvykstant.

9.1.2 [All] Privacy Lead / PIMS Manager MUST įvertinti kiekvienos prašomos išimties poveikį privatumui, teisei, sertifikavimui, veiklai ir duomenų subjektams REG04 arba REG12 per 10 darbo dienų nuo prašymo.

9.1.3 [All] Data Protection Officer / Privacy Advisor MUST įrašyti konsultaciją REG12 prieš patvirtinant bet kokią išimtį, turinčią poveikį didelės rizikos tvarkymui, išsamaus DPIA užbaigimui, išankstinei konsultacijai, didelei liekamajai privatumo rizikai arba kliento DPIA pagalbai.

9.1.4 [All] Top Management MUST patvirtinti privatumo rizikos arba DPIA išimtis, turinčias poveikį didelės rizikos tvarkymui, sertifikavimo taikymo sričiai, išankstinei konsultacijai arba neišspręstai didelei liekamajai privatumo rizikai, REG12 prieš išimčiai įsigaliojant.

9.1.5 [All] Privacy Lead / PIMS Manager MUST prieš patvirtinimą REG12 nustatyti kiekvienos patvirtintos privatumo rizikos arba DPIA išimties galiojimo pabaigos datą, neviršijančią 90 dienų.

9.1.6 [All] Process Owner / Business Owner MUST uždaryti arba pakartotinai įvertinti kiekvieną privatumo rizikos arba DPIA išimtį REG12 per penkias darbo dienas nuo galiojimo pabaigos.

10. Įgyvendinimo užtikrinimas

10.1 Privatumo rizikos ir DPIA įgyvendinimo užtikrinimas

10.1.1 [All] Privacy Lead / PIMS Manager MUST įrašyti trūkstamus, netikslius, neišsamius, vėluojančius arba nepatvirtintus REG04 privatumo rizikos arba DPIA įrodymus kaip neatitiktį REG12 per penkias darbo dienas nuo nustatymo.

10.1.2 [Controller] Process Owner / Business Owner MUST sustabdyti naują didelės rizikos duomenų valdytojo tvarkymą, kai prieš paleidimą trūksta reikalaujamų REG04 DPIA patvirtinimo įrodymų.

10.1.3 [Both] System Owner / Application Owner MUST blokuoti sistemų, tvarkančių PII, paleidimą gamybinėje aplinkoje, kai prieš paleidimo patvirtinimą trūksta reikalaujamų REG04 rizikos tvarkymo įrodymų.

10.1.4 [Both] Vendor / Procurement Owner MUST blokuoti tiekėjo, duomenų tvarkytojo, subtvarkytojo arba dalijimosi duomenimis susitarimo įtraukimą, kai prieš sutarties patvirtinimą trūksta reikalaujamų REG04 privatumo rizikos arba DPIA pagalbos įrodymų.

10.1.5 [All] Top Management MUST vadovybės peržiūros metu REG12 peržiūrėti neišspręstas reikšmingas privatumo rizikos arba DPIA neatitiktis.

10.1.6 [All] Privacy Lead / PIMS Manager MUST eskaluoti pasikartojančius REG04 pirminio vertinimo, DPIA peržiūros arba rizikos tvarkymo terminų praleidimus Top Management REG12 per penkias darbo dienas po antrojo atvejo per 12 mėnesių laikotarpį.

10.1.7 [All] Internal Audit / Compliance Reviewer MUST patikrinti korekcinių veiksmų veiksmingumą privatumo rizikos ir DPIA neatitiktims REG12 per kitą suplanuotą auditą arba per 60 dienų nuo uždarymo, atsižvelgiant į tai, kas įvyksta anksčiau.

11. Peržiūra ir palaikymas

11.1 Politikos peržiūra ir palaikymas

11.1.1 [All] Privacy Lead / PIMS Manager MUST kasmet ir per 30 dienų nuo esminio privatumo rizikos, DPIA, išankstinės konsultacijos, duomenų tvarkytojo pagalbos arba sertifikavimo reikalavimų pakeitimo peržiūrėti šią politiką REG12.

11.1.2 [All] Privacy Lead / PIMS Manager MUST kasmet REG12 peržiūrėti REG04 pirminio vertinimo kriterijus, DPIA paleidiklių kriterijus, rizikos vertinimo balais kriterijus ir liekamosios rizikos priėmimo kriterijus.

11.1.3 [All] Data Protection Officer / Privacy Advisor MUST peržiūrėti privatumui reikšmingus šios politikos pakeitimus REG12 prieš patvirtinimą.

11.1.4 [All] Top Management MUST patvirtinti esminius šios politikos pakeitimus REG12 prieš paskelbimą.

11.1.5 [All] Privacy Lead / PIMS Manager MUST atnaujinti REG03 ir REG04 per 15 darbo dienų po patvirtintų politikos pakeitimų, kuriais keičiami kontrolės priemonių taikomumas, rizikos kriterijai arba pirminio DPIA poreikio vertinimo reikalavimai.

11.1.6 [All] Privacy Lead / PIMS Manager MUST įrašyti patvirtintų šios politikos pakeitimų komunikaciją REG11 per 30 dienų nuo paskelbimo.

12. Susijusios politikos

12.1 Šią politiką palaiko šios susijusios politikos:

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 PII05 - Sutikimų ir nuostatų valdymo politika

12.7 PII06 - Duomenų subjektų teisių valdymo politika

12.8 PII08 - Privatumo pagal projektavimą ir pagal numatytuosius nustatymus politika

12.9 PII09 - PII rinkimo, naudojimo, atskleidimo ir dalijimosi politika

12.10 PII10 - PII saugojimo, ištrynimo ir sunaikinimo politika

12.11 PII11 - PII tikslumo ir kokybės politika

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

12.13 PII13 - Tarptautinio PII perdavimo politika

12.14 PII14 - PII saugumo ir prieigos kontrolės politika

12.15 PII15 - PII incidentų ir pažeidimų valdymo politika

12.16 PII17 - PIMS dokumentuotos informacijos ir įrodymų valdymo politika

12.17 PII18 - PIMS stebėsenos, audito ir tobulinimo politika

13. Pamatiniai standartai ir sistemos

13.1 Ši politika susieta su toliau nurodytais standartais ir reglamentais. Susiejimas paaiškina, kaip politika palaiko nurodytus reikalavimus, ir nustato vidaus nuostatas, kuriomis jie įgyvendinami arba palaikomi.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 6.1.1** - Susieta su veiksmų, skirtų privatumo rizikoms ir galimybėms, nustatymu ir planavimu naudojant pirminio vertinimo kriterijus, rizikos slenksčius, eskalavimą ir vadovybės peržiūros įvestinius duomenis. 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** - Susieta su pirminio privatumo rizikos vertinimo, privatumo rizikos vertinimo, rizikos lygio nustatymo, pakartotinio vertinimo ir DPIA paleidiklių vertinimo atlikimu prieš tęsiant naują arba iš esmės pakeistą tvarkymą. 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** - Susieta su privatumo rizikos tvarkymo planavimu, kontrolės priemonių taikomumo atnaujinimais, tvarkymo įgyvendinimu, liekamosios rizikos priėmimu ir SoA sąsaja. 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** - Susieta su planuojamais PIMS ir tvarkymo pakeitimais, inicijuojančiais pakartotinį privatumo rizikos vertinimą ir DPIA peržiūrą. Addressed by clauses [4.2.4; 4.6.1; 11.1.1].

13.2.5 **Clause 7.5** - Susieta su kontroliuojama dokumentuota informacija dėl pirminio privatumo rizikos vertinimo, DPIA įrodymų, rizikos tvarkymo, liekamosios rizikos priėmimo, sprendimų dėl išankstinės konsultacijos, išimčių, neatitikčių ir politikos peržiūros įrodymų. 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** - Susieta su privatumo rizikos ir DPIA kontrolės priemonių veikimu prieš paleidimą gamybinėje aplinkoje, įtraukimą, tvarkymo patvirtinimą, tvarkymo uždarymą ir susiejimą su korekciniais veiksmais. 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** - Susieta su operaciniu privatumo rizikos vertinimu, taikomu naujiems, pakeistiems, sistemų, tiekėjų, perdavimų ir incidentų nulemtiems tvarkymo pakeitimams. 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** - Susieta su operaciniu privatumo rizikos tvarkymu, tvarkymo veiksmų priskyrimu, tvarkymo įgyvendinimu, vėluojančio tvarkymo eskalavimu ir veiksmingumo patikrinimu. 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** - Susieta su pirminio vertinimo aprėpties, DPIA būsenos, atvirų rizikų, vėluojančių tvarkymo veiksmų, tiekėjų veiksmų, saugumo tvarkymo veiksmų, incidentų pakartotinio vertinimo veiksmų ir audito išvadų stebėsena bei matavimu. 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** - Susieta su vadovybės atliekama didelių liekamųjų privatumo rizikų, vėluojančių tvarkymo veiksmų, išsamaus DPIA būsenos, sprendimų dėl išankstinės konsultacijos ir reikšmingų privatumo rizikos išimčių peržiūra. Addressed by clauses [4.6.6; 6.1.1; 6.1.2; 6.1.3; 10.1.5].

13.2.11 **Clause 10.2** - Susieta su privatumo rizikos ir DPIA neatitiktimis, išimtimis, korekcinių veiksmų pradėjimu, eskalavimu ir veiksmingumo patikrinimu. 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** - Susieta su poreikio atlikti poveikio privatumui vertinimą naujam arba pakeistam duomenų valdytojo tvarkymui įvertinimu ir jo įgyvendinimu, kai tinkama. 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** - Susieta su tvarkymo įrašais, pagrindžiančiais privatumo rizikos ir DPIA vertinimo įvestinius duomenis, įskaitant tikslą, kategorijas, sistemas, gavėjus, perdavimus ir tiekėjus. Addressed by clauses [4.3.1; 6.1.4; 8.1.1].

13.2.14 **Annex A.2.2.2** - Susieta su duomenų tvarkytojo klientų sutartimis ir pareigomis padėti klientui DPIA klausimais. 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** - Susieta su duomenų tvarkytojo teikiama informacija, reikalinga kliento atitikčiai, įskaitant pagalbą DPIA klausimais ir kliento palaikymo įrodymus. Addressed by clauses [4.2.5; 4.2.6; 4.5.4; 8.1.5].

13.3 GDPR

13.3.1 **Article 5(2)** - Susieta su atskaitomybės įrodymais dėl pirminio DPIA poreikio vertinimo, išsamaus DPIA sprendimų, rizikos tvarkymo, liekamosios rizikos priėmimo, sprendimų dėl išankstinės konsultacijos, išimčių, audito išvadų ir korekcinių veiksmų. 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** - Susieta su duomenų valdytojo atsakomybe už tinkamas privatumo rizikos priemones, didelės liekamosios rizikos peržiūrą, vadovybės patvirtinimą ir politikos palaikymą. Addressed by clauses [4.4.5; 4.5.3; 6.1.2; 10.1.5; 11.1.4].

13.3.3 **Article 25** - Susieta su privatumo pagal projektavimą ir privatumo pagal numatytuosius nustatymus įrodymais, naudojamais rizikos vertinime ir prieš patvirtinant paleidimą gamybinėje aplinkoje. Addressed by clauses [4.1.5; 4.3.4; 7.1.5].

13.3.4 **Article 28** - Susieta su duomenų tvarkytojo ir subtvarkytojo pagalba DPIA klausimais, kliento nurodymų tvarkymu ir tiekėjų rizikos tvarkymo įrodymais. 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** - Susieta su tvarkymo įrašais, pagrindžiančiais privatumo rizikos vertinimo ir DPIA įvestinius duomenis. Addressed by clauses [4.3.1; 6.1.4; 8.1.1].

13.3.6 **Article 32** - Susieta su PII saugumo rizikos įvestiniais duomenimis, apsaugos priemonių parinkimu, saugumo rizikos tvarkymu ir saugumo kontrolės priemonių būsenos atnaujinimais. Addressed by clauses [4.1.5; 4.3.3; 4.4.2; 8.1.6].

13.3.7 **Article 35** - Susieta su pirminiu DPIA poreikio vertinimu, išsamaus DPIA reikalavimo nustatymu, DPIA turiniu, DPO konsultacija, peržiūra ir didelės rizikos tvarkymo blokavimu, kai nėra reikalaujamo DPIA patvirtinimo. 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** - Susieta su sprendimų dėl išankstinės konsultacijos priėmimu, DPO konsultacija, Top Management patvirtinimu ir tęsimo, sustabdymo, pertvarkymo arba konsultacijos veiksmais, kai išlieka didelė liekamoji rizika. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 6.1.2].

13.3.9 **Article 39** - Susieta su Data Protection Officer / Privacy Advisor konsultacija ir stebėsena, kai taikoma, dėl DPIA sprendimų, didelės rizikos tvarkymo, išankstinės konsultacijos ir politikos pakeitimų. 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** - Susieta su privatumo kontrolės priemonių nustatymu, saugumo apsaugos priemonėmis, privatumo atitiktimi, privatumo rizikos įrodymais, stebėsena ir peržiūra. 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** - Susieta su PIA proceso taikymo sritimi, nauda, paleidiklių nustatymu, pasirengimu, vertinimo įvestiniais duomenimis, suinteresuotųjų šalių įrodymais ir DPIA ataskaitos struktūra, saugoma REG04. 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** - Susieta su PII apsaugos programos reikalavimais, PII apsaugos reikalavimų nustatymu, rizika grindžiamu kontrolės priemonių parinkimu ir privatumo rizikos tvarkymo sąsaja. 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** - Susieta su organizacinės privatumo rizikos principais, lyderyste, integravimu, rizikos vertinimu, rizikos tvarkymu, stebėsena ir peržiūra bei įrašymu ir ataskaitų teikimu. 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].