					Čia įrašykite registruoto juridinio asmens pavadinimą							
Dokumento numeris: P17S					Dokumento pavadinimas: **Duomenų apsaugos ir privatumo 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	Punktas / straipsnis	Komentaras
ISO/IEC 27001:2022	5.1, 6.1.3, 8 punktai	
ISO/IEC 27002:2022	5.34, 8.10–8 kontrolės priemonės	
NIST SP 800-53 Rev.5	AR-2, PL-5, AC-6, IR-4	
ES BDAR	5, 6, 12–23, 30, 32–34 straipsniai	
ES NIS2 direktyva	21 straipsnio 2 dalies e ir f punktai	
ES DORA reglamentas	6, 15, 17 straipsniai	
COBIT 2019	APO12, DSS05, MEA	

1. Tikslas

1.1. Ši politika nustato, kaip organizacija saugo asmens duomenis, laikydamasi teisinių įpareigojimų, reguliavimo sistemų ir tarptautinių saugumo standartų.

1.2. Ji užtikrina, kad asmens duomenys, nesvarbu, ar jie susiję su klientais, darbuotojais ar partneriais, būtų renkami, naudojami, saugomi ir ištrinami teisėtai, sąžiningai ir saugiai.

1.3. Ši politika taip pat užtikrina atitiktį ISO/IEC 27001:2022 reikalavimams ir palaiko pasirengimą auditui, taikant nuoseklų, rizika grindžiamą požiūrį į privatumo apsaugą.

1.4. Taikydama šią politiką, organizacija demonstruoja atskaitomybę ir stiprina klientų pasitikėjimą, teikdama pirmenybę skaidrumui, duomenų minimizavimui ir veiksmingai privatumo valdysenai.

2. Taikymo sritis

2.1. Ši politika taikoma:

2.1.1. visiems darbuotojams, rangovams ir paslaugų teikėjams, kurie gauna prieigą prie asmens duomenų, juos tvarko arba valdo;

2.1.2. bet kuriai sistemai, taikomajai programai ar vietai, kurioje asmens duomenys saugomi arba perduodami;

2.1.3. visiems asmens duomenims, neatsižvelgiant į tai, ar jie saugomi elektroniniu formatu, popieriuje, debesijos sistemose ar mobiliuosiuose įrenginiuose.

2.2. Ši politika taikoma duomenims, susijusiems su klientais, darbuotojais, tiekėjais ir kitais identifikuojamais fiziniais asmenimis.

2.3. Ši politika galioja nepriklausomai nuo to, ar duomenys tvarkomi organizacijos viduje, ar juos tvarko trečiųjų šalių paslaugų teikėjai.

3. Tikslai

3.1. Užtikrinti, kad asmens duomenys būtų tvarkomi laikantis privatumo teisės aktų ir saugumo standartų, įskaitant ES BDAR, NIS2 direktyvą ir ISO/IEC 27001.

3.2. Apsaugoti asmens duomenis nuo neteisėtos prieigos, netinkamo naudojimo, pakeitimo ar praradimo, taikant aiškias technines ir organizacines kontrolės priemones.

3.3. Gerbti fizinių asmenų privatumo teises, įskaitant teisę susipažinti su savo duomenimis, juos ištaisyti ir ištrinti.

3.4. Nustatyti aiškius su duomenų apsauga susijusius vaidmenis ir atsakomybes organizacijoje.

3.5. Užtikrinti duomenų minimizavimą, saugų saugojimą ir savalaikį ištrynimą visose sistemose ir procesuose.

3.6. Mažinti neatitikties, teisinių sankcijų, reputacinės žalos ar klientų nepasitikėjimo riziką.

4. Vaidmenys ir atsakomybės

4.1. Generalinis direktorius (GD)

4.1.1. tvirtina šią politiką ir užtikrina jos įgyvendinimą;

4.1.2. skiria reikiamus išteklius privatumo rizikai valdyti ir reaguoti į incidentus;

4.1.3. prisiima bendrą atskaitomybę už atitiktį privatumo teisės aktams ir standartams.

4.2. Privatumo koordinatorius (vidinis arba išorinis)

4.2.1. tvarko duomenų tvarkymo veiklos įrašus;

4.2.2. atsako į fizinių asmenų prašymus, susijusius su privatumu, ir reguliavimo institucijų paklausimus;

4.2.3. padeda atlikti rizikos vertinimą, organizuoti mokymus ir įgyvendinti politiką;

4.2.4. dokumentuoja asmens duomenų saugumo pažeidimus ir, kai privaloma, informuoja institucijas.

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

9. Peržiūros ir atnaujinimo reikalavimai

9.1. Planinės peržiūros

9.1.1. Ši politika turi būti peržiūrima ne rečiau kaip kartą per 12 mėnesių privatumo koordinatoriaus ir tvirtinama generalinio direktoriaus.

9.1.2. Peržiūros metu turi būti įvertintas politikos aktualumas, atitiktis reguliavimo reikalavimams ir veiklos veiksmingumas.

9.2. Tarpinių peržiūrų paleidikliai

9.2.1. Politikos atnaujinimai taip pat turi būti inicijuojami reaguojant į:

9.2.1.1. naujus arba pakeistus duomenų apsaugos teisės aktus (pvz., ES BDAR, DORA reglamentą);

9.2.1.2. saugumo incidentus arba privatumo pažeidimus, susijusius su asmens duomenimis;

9.2.1.3. naujų sistemų, priemonių ar paslaugų, tvarkančių asmens duomenis, įdiegimą;

9.2.1.4. esmines audito išvadas arba reguliuotojo rekomendacijas.

9.3. Pakeitimų kontrolė ir komunikacija

9.3.1. Visi politikos pakeitimai turi būti formaliai dokumentuojami pakeitimų žurnale.

9.3.2. Atnaujintos versijos turi būti išplatinamos visiems darbuotojams ir atitinkamiems rangovams.

9.3.3. Archyvuotos versijos turi būti saugomos siekiant užtikrinti atitikties audito seką.

10. Susijusios politikos ir sąsajos

10.1. Ši politika taikoma kartu su kitomis MVĮ politikomis, siekiant sukurti išsamią ir vykdytiną privatumo sistemą:

10.1.1. P13S – Duomenų klasifikavimo ir ženklinimo politika: užtikrina, kad asmens duomenys būtų tinkamai klasifikuojami, kad privatumo apsaugos priemonės galėtų būti taikomos pagal riziką.

10.1.2. P14S – Duomenų saugojimo ir sunaikinimo politika: nustato aiškias taisykles, kiek laiko turi būti saugomi asmens duomenys ir kokie saugūs jų sunaikinimo metodai turi būti taikomi pasibaigus saugojimo terminui.

10.1.3. P16S – Duomenų maskavimo ir pseudonimizavimo politika: nustato, kaip asmens identifikatoriai turi būti transformuojami prieš naudojant duomenis neprodukcinėse aplinkose arba dalijantis jais su išorės subjektais.

10.1.4. P30S – Reagavimo į incidentus politika: apima veiksmus, kurių reikia imtis reaguojant į asmens duomenų saugumo pažeidimus, įskaitant pranešimą reguliuotojams ir paveiktiems fiziniams asmenims per nustatytus terminus.

10.1.5. P2S – Valdysenos vaidmenų ir atsakomybių politika: paaiškina atskaitomybės struktūrą ir sprendimų priėmimo vaidmenis, taikomus privatumo įgyvendinimui ir priežiūrai.

10.2. Šios susijusios politikos turi būti peržiūrimos ir taikomos kartu, siekiant užtikrinti visapusišką privatumo aprėptį sistemose, darbuotojų veikloje ir tiekimo grandinėje.

11. Pamatiniai standartai ir sistemos

11.1. ISO/IEC 27001

11.1.1. 5.1 punktas – reikalauja, kad aukščiausioji vadovybė demonstruotų lyderystę ir įsipareigojimą saugant asmens duomenis.

11.1.2. 6.1.3 punktas – nustato reikalavimą valdyti rizikas, susijusias su asmens informacijos tvarkymu.

11.1.3. 8.1 punktas – reikalauja įgyvendinti operacines kontrolės priemones duomenims apsaugoti per visą jų gyvavimo ciklą.

11.2. ISO/IEC 27002

11.2.1. Kontrolės priemonė 5.34 – pateikia įgyvendinimo gaires dėl privatumo apsaugos ir saugaus PII tvarkymo.

11.2.2. Kontrolės priemonė 8.10 – reglamentuoja saugų asmens duomenų sunaikinimą, siekiant išvengti likutinio atskleidimo.

11.2.3. Kontrolės priemonė 8.11 – palaiko maskavimo ir pseudonimizavimo taikymą duomenų minimizavimui.

11.2.4. Kontrolės priemonė 8.12 – padeda užkirsti kelią nesankcionuotam duomenų nutekėjimui, taikant duomenų prieigos ir naudojimo kontrolės priemones.

11.3. NIST SP 800-53 Rev.5

11.3.1. AR-2 – priskiria vaidmenis ir atsakomybes už privatumo rizikos valdymą.

11.3.2. PL-5 – reikalauja dokumentuoto privatumo plano, apimančio duomenų naudojimą ir apsaugą.

11.3.3. AC-6 – nustato mažiausių privilegijų principo ir prieigos kontrolės reikalavimus asmens duomenims.

11.3.4. IR-4 – reikalauja incidentų valdymo procesų asmens duomenų saugumo pažeidimams.

11.4. ES BDAR

11.4.1. 5 straipsnis – nustato pagrindinius teisėto, sąžiningo ir skaidraus duomenų tvarkymo principus.

11.4.2. 6 straipsnis – reikalauja galiojančio teisinio pagrindo kiekvienai asmens duomenų tvarkymo veiklai.

11.4.3. 12–23 straipsniai – apibrėžia duomenų subjektų teises, įskaitant teisę susipažinti, ištaisyti, ištrinti duomenis ir nesutikti su tvarkymu.

11.4.4. 30 straipsnis – nustato pareigą tvarkyti duomenų tvarkymo veiklos įrašus.

11.4.5. 32 straipsnis – reikalauja tinkamų techninių ir organizacinių saugumo priemonių.

11.4.6. 33–34 straipsniai – nustato pranešimo apie pažeidimus pareigas institucijoms ir duomenų subjektams.

11.5. ES NIS2 direktyva

11.5.1. 21 straipsnio 2 dalies e punktas – reikalauja priemonių duomenų apsaugai užtikrinti, suderintų su kibernetinio saugumo politikomis.

11.5.2. 21 straipsnio 2 dalies f punktas – nustato mechanizmų reikalavimą asmens ir konfidencialių duomenų saugumui IRT sistemose valdyti.

11.6. ES DORA reglamentas

11.6.1. 6 straipsnis – reikalauja vidinių valdysenos sistemų, skirtų duomenų rizikai ir apsaugai valdyti.

11.6.2. 15 straipsnis – įpareigoja finansų subjektus užtikrinti, kad trečiųjų šalių paslaugų teikėjai saugotų asmens duomenis ir palaikytų atitiktį reguliavimo reikalavimams.

11.6.3. 17 straipsnis – reikalauja užtikrinti, kad IRT sistemos, tvarkančios asmens duomenis, būtų saugios, atsparios ir stebimos.

11.7. COBIT 2019

11.7.1. APO12 – Rizikos valdymas: reikalauja nustatyti ir valdyti privatumo ir duomenų apsaugos rizikas.

11.7.2. DSS05 – Saugumo paslaugų valdymas: nustato apsaugos priemones, skirtas užkirsti kelią neteisėtai prieigai prie asmens duomenų.

11.7.3. MEA03 – Atitikties stebėsena: reikalauja, kad organizacijos užtikrintų nuolatinę atitiktį privatumo ir duomenų apsaugos teisės aktams.