					Čia įrašykite registruoto juridinio asmens pavadinimą							
Dokumento numeris: P17					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	Pastaba
ISO/IEC 27001:2022	5.1, 6.1.3, 8.1, 10 punktai	Aktualios bendrosios, techninės ir nuolatinio tobulinimo / duomenų apsaugos kontrolės priemonės
ISO/IEC 27002:2022	5.34, 8.10, 8.11, 8.12 kontrolės priemonės	Kontrolės priemonės, skirtos AII tvarkymui, saugojimui, ištrynimui, anoniminimui ir duomenų subjektų teisėms
NIST SP 800-53 Rev.5	AR-1, AR-2, AR-4, AR-5; PL-2, PL-8; AC-2, AC-6; AU-2, AU-6, AU-9; IR-4, IR-5, IR-6; PM-1, PM-21, PM-23	Valdysenos, rizikos, prieigos valdymo, žurnalų tvarkymo, reagavimo į pažeidimus ir privatumo programos reikalavimai
ES BDAR	5, 6, 12–23, 25, 28, 30, 32–34 straipsniai; 78 konstatuojamoji dalis	Visi pagrindiniai privatumo, atskaitomybės, duomenų subjektų teisių, DSR, pažeidimų, projektavimo ir numatytųjų nustatymų principai
ES NIS2 direktyva	21 straipsnio 2 dalies e ir f punktai	Rizika grindžiamos saugumo kontrolės priemonės esminiams ir svarbiems subjektams
ES DORA reglamentas	6 straipsnio 2 dalies d punktas, 11 straipsnio 1 dalies c punktas, 15 straipsnio 1 dalis, 17 straipsnis	Valdysenos, trečiųjų šalių rizikos ir saugaus tvarkymo terminų reikalavimai
COBIT 2019	APO12, DSS01, DSS05, MEA	Rizikos valdymas, saugios operacijos, atitikties stebėsena

1. Tikslas

1.1 Ši politika nustato privalomus organizacinius principus ir techninius reikalavimus asmens duomenų apsaugai bei duomenų apsaugos pagal projektavimą principo taikymui visose aplinkose.

1.2 Ji įtvirtina organizacijos atsakomybes pagal tarptautinius standartus ir reguliavimo sistemas, užtikrindama, kad asmens duomenys būtų renkami, tvarkomi, saugomi, perduodami ir sunaikinami teisėtai, saugiai ir skaidriai.

1.3 Ši politika taip pat stiprina atitiktį taikomiems privatumo teisės aktams ir sistemoms, įskaitant ES Bendrąjį duomenų apsaugos reglamentą (BDAR), ES NIS2 direktyvą, ES Skaitmeninio operacinio atsparumo reglamentą (DORA), ISO/IEC 27001:2022 ir COBIT 2019.

2. Taikymo sritis

2.1 Ši politika taikoma visiems organizaciniams padaliniams, darbuotojams ir sistemoms, susijusiems su asmens duomenų tvarkymu, įskaitant:

2.1.1 darbuotojus, rangovus, konsultantus ir trečiųjų šalių paslaugų teikėjus.

2.1.2 duomenis, renkamus iš vidinių ir išorinių šaltinių visose verslo funkcijose.

2.1.3 fizines ir skaitmenines laikmenas, įskaitant debesijos paslaugas, SaaS platformas, mobiliuosius įrenginius ir popierinius įrašus.

2.1.4 visas aplinkas, įskaitant produkcines, kūrimo, testavimo ir atsarginių kopijų sistemas, kuriose gali būti asmens duomenų.

2.2 Ji apima visas tvarkymo veiklas, reglamentuojamas taikomų privatumo teisės aktų ir standartų, įskaitant, bet neapsiribojant:

2.2.1 asmens duomenų rinkimą, saugojimą, naudojimą, perdavimą ir sunaikinimą.

2.2.2 duomenų subjektų teisių įgyvendinimą, teisinio pagrindo dokumentavimą ir sutikimų valdymą.

2.2.3 tarpvalstybinius perdavimus, pranešimą apie pažeidimus ir duomenų atskleidimą trečiosioms šalims.

2.2.4 saugaus projektavimo ir duomenų apsaugos pagal numatytuosius nustatymus užtikrinimą sistemose ir procesuose.

3. Tikslai

3.1 Užtikrinti teisėtą, skaidrų ir atskaitingą asmens duomenų tvarkymą pagal ISO/IEC 27001:2022 ir susijusius teisinius reikalavimus.

3.2 Integruoti duomenų apsaugos pagal projektavimą ir pagal numatytuosius nustatymus principus į visas informacines sistemas, paslaugas ir verslo procesus.

3.3 Taikyti technines ir organizacines priemones (TOM), kurios per visą asmens duomenų gyvavimo ciklą užtikrina jų konfidencialumą, vientisumą ir prieinamumą.

3.4 Apibrėžti valdysenos vaidmenis ir atskaitomybės struktūras duomenų apsaugos srityje, įskaitant duomenų apsaugos pareigūno (DAP), informacijos saugos, teisės funkcijos ir duomenų savininkų atsakomybes.

3.5 Užtikrinti visišką atitiktį BDAR 5, 6, 25, 30 ir 32 straipsniams, taip pat NIS2 ir DORA nustatytiems rizikos mažinimo ir atsparumo reikalavimams.

3.6 Užtikrinti duomenų subjektų teises, įskaitant teisę susipažinti su duomenimis, juos ištaisyti, ištrinti, apriboti jų tvarkymą, perkelti duomenis, nesutikti su tvarkymu ir būti apsaugotiems nuo automatizuoto sprendimų priėmimo.

3.7 Mažinti reguliavimo, reputacines, teisines ir operacines rizikas, kylančias dėl neteisėtos prieigos, netinkamo naudojimo ar asmens duomenų praradimo.

4. Vaidmenys ir atsakomybės

4.1 Vadovybė

4.1.1 Užtikrina strateginę priežiūrą ir skiria pakankamus išteklius privatumo programai palaikyti.

4.1.2 Tvirtina šią politiką ir užtikrina jos taikymą visoje organizacijoje.

4.2 Duomenų apsaugos pareigūnas (DAP)

4.2.1 Veikia nepriklausomai, vykdydamas duomenų apsaugos reikalavimų laikymosi priežiūrą.

4.2.2 Tvarko tvarkymo veiklos įrašus (RoPA) pagal BDAR 30 straipsnį.

4.2.3 Vadovauja bendravimui su priežiūros institucijomis, atlieka poveikio duomenų apsaugai vertinimus (DPIA) ir valdo pranešimo apie pažeidimus procesus.

4.2.4 Peržiūri privatumo išimtis ir tvarko Privatumo išimčių registrą.

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

9. Peržiūros ir atnaujinimo reikalavimai

9.1 Ši politika turi būti peržiūrima ne rečiau kaip kartą per metus arba anksčiau, jei atsiranda bent viena iš šių sąlygų:

9.1.1 reikšmingi teisiniai ar reguliavimo atnaujinimai (pvz., BDAR pakeitimai, DORA terminai).

9.1.2 naujos sistemos arba tvarkymo veiklos, susijusios su asmens duomenimis.

9.1.3 vidaus audito išvados, rodančios politikos spragas.

9.1.4 reikšmingi pažeidimų incidentai arba priežiūros institucijos grįžtamasis ryšys.

9.2 Peržiūros atsakomybės

9.2.1 DAP inicijuoja politikos peržiūrą, koordinuodamas veiksmus su teisės, rizikos, informacijos saugos funkcijomis ir vadovybe.

9.2.2 Visi atnaujinimai turi būti registruojami ISVS dokumentų kontrolės registre ir išplatinami susijusioms suinteresuotosioms šalims.

9.3 Pakeitimų kontrolė

9.3.1 Bet koks šios politikos pakeitimas turi būti formaliai patvirtintas vadovybės.

9.3.2 Nebegaliojančios versijos turi būti saugiai archyvuojamos, o atnaujintoje versijoje turi būti dokumentuota pakeitimų istorija.

10. Susijusios politikos ir sąsajos

10.1 P1 – Informacijos saugumo politika. Nustato bendruosius saugumo valdysenos principus, kuriais grindžiama ši privatumo politika. P1 palaiko asmens duomenų konfidencialumą, vientisumą ir prieinamumą visose sistemose ir paslaugose.

10.2 P6 – Rizikos valdymo politika. Apibrėžia organizacijos rizikos tvarkymo metodiką, kuri yra būtina privatumo rizikoms vertinti, DPIA procesams vykdyti ir liekamosios rizikos vertinimams pagal BDAR ir ISO/IEC 27001 6.1.3 punktą atlikti.

10.3 P13 – Duomenų klasifikavimo ir ženklinimo politika. Nustato asmens ir jautrių duomenų kategorizavimo tvarką, kuri sudaro pagrindą taikyti tinkamas privatumo kontrolės priemones, įskaitant saugojimo terminų laikymąsi, prieigos ribojimą ir saugų sunaikinimą.

10.4 P14 – Duomenų saugojimo ir sunaikinimo politika. Tiesiogiai palaiko BDAR 5 straipsnio 1 dalies e punkto ir 17 straipsnio privatumo reikalavimus, užtikrindama, kad asmens duomenys būtų saugomi tik tiek, kiek būtina, ir saugiai sunaikinami pagal teisinius įpareigojimus.

10.5 P16 – Duomenų maskavimo ir pseudonimizavimo politika. Nustato kontrolės priemones, skirtas mažinti asmens duomenų identifikuojamumą taikant technines priemones, tokias kaip tokenizavimas, dinaminis maskavimas ir pseudonimizavimas, taip užtikrinant BDAR 32 straipsnio ir ISO/IEC 27002 5.34 kontrolės priemonės įgyvendinimą.

10.6 P30 – Reagavimo į incidentus politika. Nustato privalomus reagavimo į pažeidimus protokolus, kurie integruojami su privatumo pažeidimų valdymo ir pranešimo terminais pagal BDAR 33 ir 34 straipsnius.

10.7 P33 – Audito ir atitikties stebėsenos politika. Užtikrina planinius privatumo programos veiksmingumo, politikos taikymo ir korekcinių veiksmų stebėsenos vertinimus organizaciniuose padaliniuose ir pas trečiųjų šalių tvarkytojus.

11. Pamatiniai standartai ir sistemos

11.1 ISO/IEC 27001

11.1.1 5.1 punktas – Lyderystė ir įsipareigojimas: nustato vadovybės lygmens atsakomybę už asmens duomenų apsaugą ir privatumo principų įgyvendinimą.

11.1.2 6.1.3 punktas – Informacijos saugos rizikos tvarkymas: palaiko privatumo rizikų identifikavimą, vertinimą ir tvarkymą atliekant DPIA ir taikant išimtis.

11.1.3 8.1 punktas – Operacijų planavimas ir valdymas: reikalauja techninių ir procedūrinių apsaugos priemonių, kad asmens duomenys būtų tvarkomi saugiai.

11.1.4 10.1 punktas – Nuolatinis tobulinimas: nustato periodinio privatumo programos vertinimo ir pritaikymo reikalavimą.

11.2 ISO/IEC 27002:2022 5.34, 8.10, 8.11, 8.12 kontrolės priemonės: pateikia gaires dėl AII tvarkymo, saugojimo terminų taikymo, ištrynimo, anoniminimo ir skaidrumo užtikrinimo įgyvendinant duomenų subjektų teises.

11.3 NIST SP 800-53 Rev.5

11.3.1 AR-1, AR-2, AR-4, AR-5: apibrėžia valdyseną, vaidmenis, atskaitomybę ir privatumo mokymų atsakomybes.

11.3.2 PL-2, PL-8: reikalauja privatumo kontrolės priemonių integravimo į sistemos gyvavimo ciklą ir įmonės architektūrą.

11.3.3 AC-2, AC-6: nustato mažiausių privilegijų principo ir paskyrų valdymo taikymą asmens duomenų apsaugai.

11.3.4 AU-2, AU-6, AU-9: nustato žurnalų tvarkymo, atsekamumo ir audito vientisumo reikalavimus asmens duomenų prieigai.

11.3.5 IR-4, IR-5, IR-6: apibrėžia struktūruotus aptikimo, analizės ir pranešimo procesus privatumo pažeidimams.

11.3.6 PM-1, PM-21, PM-23: nustato išsamią privatumo programą, suderintą su strateginiais rizikos ir duomenų valdysenos tikslais.

11.4 ES BDAR (2016/679)

11.4.1 5, 6, 12–23, 25, 28, 30, 32–34 straipsniai: reglamentuoja teisėtą tvarkymą, paskirties apribojimą, duomenų subjektų teises, atskaitomybę, duomenų apsaugą pagal projektavimą ir pagal numatytuosius nustatymus, trečiųjų šalių prievoles ir pažeidimų valdymą.

11.4.2 78 konstatuojamoji dalis: sustiprina duomenų apsaugos pagal projektavimą principus.

11.5 ES NIS2 direktyva (2022/2555)

11.5.1 21 straipsnio 2 dalies e ir f punktai: reikalauja įgyvendinti rizika grindžiamas saugumo kontrolės priemones ir asmens duomenų apsaugą subjektams, patenkantiems į esminių ir svarbių subjektų taikymo sritį.

11.6 ES DORA reglamentas (2022/2554)

11.6.1 6 straipsnio 2 dalies d punktas: nustato vidaus valdyseną IRT rizikai, susijusiai su duomenų tvarkymu.

11.6.2 11 straipsnio 1 dalies c punktas: nustato trečiųjų šalių rizikos priežiūros reikalavimą su duomenimis susijusioms paslaugoms.

11.6.3 15 straipsnio 1 dalis ir 17 straipsnis: reikalauja saugaus duomenų tvarkymo paslaugų teikėjų veikloje ir savalaikio informavimo priežiūros institucijoms po su IRT susijusių incidentų.

11.7 COBIT 2019

11.7.1 APO12 – Rizikos valdymas: integruoja privatumo riziką į platesnę įmonės rizikos priežiūrą.

11.7.2 DSS01 – Valdomos operacijos ir DSS05 – Saugumo paslaugos: užtikrina saugias operacijas, įskaitant prieigos kontrolę, saugojimą ir sistemų vientisumą.

11.7.3 MEA03 – Atitikties stebėsena: reikalauja nuolatinės atitikties būklės peržiūros pagal reguliavimo ir politika grindžiamus privatumo įpareigojimus.