| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Čia įrašykite registruoto juridinio asmens pavadinimą | | | | | | |
| Dokumento numeris:<br>P16S | | | | | Dokumento pavadinimas:<br>**Duomenų maskavimo ir pseudonimizavimo politika** | | | | | | |
| Versija:<br>1.0 | | Įsigaliojimo data:<br>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 | Skyrius / straipsnis | Komentaras |
|---|---|---|
| ISO/IEC 27001:2022 | 6.1.3 skyrius, 8 skyrius | Informacijos saugumo rizika ir būtinos kontrolės priemonės, įskaitant maskavimą ir pseudonimizavimą |
| ISO/IEC 27002:2022 | Kontrolės priemonės 8.11, 8.12 | Gairės dėl maskavimo ir duomenų iškėlimo prevencijos |
| NIST SP 800-53 Rev.5 | SC-12, SC-28, PT-2, PT-3 | Duomenų maskavimas, privatumą didinančios technologijos |
| ES NIS2 direktyva | 21 straipsnio 2 dalies c punktas | Proporcingos techninės priemonės, pseudonimizavimas kaip kontrolės priemonė |
| ES DORA reglamentas | 10 straipsnio 1 dalis | IRT rizikos kontrolės priemonės, įskaitant duomenų transformavimo apsaugos priemones |
| COBIT 2019 | DSS05.01, DSS06 | Duomenų apsauga, maskavimo ir pseudonimizavimo metodai |
| ES BDAR | 4 straipsnio 5 dalis, 5 straipsnio 1 dalies c punktas, 32 straipsnis | Duomenų minimizavimas, pseudonimizavimas kaip techninė kontrolės priemonė |

**1. Tikslas**

1.1. Ši politika nustato privalomus duomenų maskavimo ir pseudonimizavimo taikymo reikalavimus, siekiant apsaugoti jautrius, asmens ir konfidencialius duomenis mažosiose ir vidutinėse įmonėse (MVĮ).

1.2. Šie metodai yra privalomi visais atvejais, kai tikrieji duomenys nėra būtini, pavyzdžiui, kūrimo, analizės ar trečiųjų šalių paslaugų teikimo scenarijuose, taip padedant sumažinti atskleidimo, netinkamo naudojimo ar duomenų saugumo pažeidimo riziką.

1.3. Ši politika tiesiogiai prisideda prie atitikties ISO/IEC 27001:2022 sertifikavimo reikalavimams, taip pat Europos Sąjungos reguliavimo reikalavimams, tokiems kaip ES BDAR, NIS2 direktyva ir DORA reglamentas, užtikrinimo.

1.4. Transformuodama duomenis prieš juos naudojant už pirminio verslo konteksto ribų, organizacija riboja atsakomybę ir stiprina gebėjimą pagrįsti tinkamą privatumo ir saugumo pareigų vykdymą.

**2. Taikymo sritis**

**2.1. Ši politika taikoma visiems struktūrizuotiems ir nestruktūrizuotiems duomenims, priskirtiems asmens, konfidencialių arba jautrių duomenų kategorijai, neatsižvelgiant į tai, ar jie saugomi ar tvarkomi:**

2.1.1. Produkcinėse, testavimo ar kūrimo aplinkose

2.1.2. Vietiniuose įrenginiuose, serveriuose ar debesijos platformose

2.1.3. Vidaus darbuotojų, rangovų ar trečiųjų šalių paslaugų teikėjų

2.2. Ji taip pat apima visas duomenų transformavimo priemones (maskavimą, tokenizavimą, pseudonimizavimą), neatsižvelgiant į tai, ar jos yra atvirojo kodo, komercinės, ar sukurtos organizacijos viduje.

**2.3. Naudojimo atvejai pagal šią politiką apima:**

2.3.1. Testavimo ar kūrimo duomenų rinkinių parengimą

2.3.2. Duomenų eksportą į analitines sistemas

2.3.3. Tiekėjų ar konsultantų prieigą prie operacinių sistemų

2.3.4. Duomenų subjektų duomenų minimizavimą, siekiant sumažinti tvarkymo riziką

**3. Tikslai**

3.1. Užtikrinti, kad tikrieji asmens ar jautrūs duomenys niekada nebūtų atskleidžiami žemesnio saugumo aplinkose, kuriose jie nėra būtini.

3.2. Nustatyti privalomą maskavimo arba pseudonimizavimo taikymą, kai tikrieji identifikatoriai nėra griežtai būtini užduočiai atlikti.

3.3. Užkirsti kelią neteisėtai prieigai prie duomenų ar jų netinkamam naudojimui, taikant transformavimo kontrolės priemones prieš duomenų perdavimą ar tvarkymą.

3.4. Užtikrinti, kad visi maskavimo ir pseudonimizavimo procesai būtų atsekami, audituojami ir vykdomi naudojant patvirtintas priemones.

3.5. Laikytis taikomų teisinių ir reguliavimo reikalavimų, nustatančių duomenų minimizavimą, konfidencialumą ir transformavimo apsaugos priemones.

**4. Vaidmenys ir atsakomybės**

**4.1. Generalinis vadovas (GV)**

4.1.1. Valdo ir tvirtina šią politiką

4.1.2. Užtikrina, kad visi padaliniai ir paslaugų teikėjai laikytųsi duomenų transformavimo reikalavimų

4.1.3. Peržiūri išimtis, rizikos vertinimus ir transformavimo žurnalus

4.1.4. Koordinuoja teisinius, veiklos ar su tiekėjais susijusius veiksmus pažeidimų atveju

**4.2. IT paslaugų teikėjas / vidaus IT funkcija**

4.2.1. Parenka ir administruoja maskavimo arba pseudonimizavimo priemones

4.2.2. Užtikrina, kad pagal duomenų tipą būtų taikomi tinkami transformavimo metodai

4.2.3. Tvarko transformuotų duomenų rinkinių žurnalus ir raktų valdymo procedūras

4.2.4. Užtikrina, kad maskavimas būtų atliktas prieš naudojant duomenis testavimui, perduodant tiekėjams ar analizei

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

**9. Peržiūros ir atnaujinimo reikalavimai**

**9.1. Kasmetinė peržiūra**

**9.1.1. Šią politiką bent kartą per metus turi peržiūrėti Generalinis vadovas, siekdamas užtikrinti, kad ji atspindėtų:**

9.1.1.1. Taikomų reguliavimo reikalavimų atnaujinimus (pvz., ES BDAR, DORA reglamentą)

9.1.1.2. Naujas verslo sistemas ar duomenų mainus su trečiosiomis šalimis

9.1.1.3. Audito ar incidentų, susijusių su nemaskuotų duomenų naudojimu, išvadas

**9.2. Tarpinės peržiūros**

**9.2.1. Peržiūros taip pat turi būti atliekamos, kai:**

9.2.1.1. Įdiegiamos naujos taikomosios programos ar platformos, tvarkančios jautrius duomenis

9.2.1.2. Reikšmingas incidentas atskleidžia esamų transformavimo kontrolės priemonių spragas

9.2.1.3. Klasifikavimo lygių pakeitimai daro poveikį duomenų tvarkymo procedūroms

**9.3. Versijų kontrolė ir pakeitimų valdymas**

**9.3.1. Visi politikos pakeitimai turi būti:**

9.3.1.1. Patvirtinti GV ir dokumentuoti pakeitimų žurnale

9.3.1.2. Aiškiai komunikuoti paveiktiems darbuotojams ir paslaugų teikėjams

9.3.1.3. Saugiai archyvuojami, ribojant prieigą prie nebegaliojančių versijų

**10. Susijusios politikos ir sąsajos**

**10.1. Ši politika turi būti taikoma kartu su šiomis MVĮ politikomis, siekiant užtikrinti nuoseklią ir privalomą jautrių duomenų apsaugą:**

10.1.1. P13S – Duomenų klasifikavimo ir ženklinimo politika: nustato klasifikavimo lygius (pvz., „Konfidencialūs – asmens duomenys“), pagal kuriuos nustatoma, kada turi būti taikomas maskavimas arba pseudonimizavimas. Ši politika nustato transformavimo taisykles pagal duomenų jautrumo lygius.

10.1.2. P14S – Duomenų saugojimo ir sunaikinimo politika: užtikrina, kad transformuoti duomenų rinkiniai, įskaitant atsargines kopijas su maskuotais ar pseudonimizuotais duomenimis, būtų saugomi ir sunaikinami pagal taikytinas taisykles, įskaitant susiejimo raktų ištrynimą, kai jų nebereikia.

10.1.3. P17S – Duomenų apsaugos ir privatumo politika: suderina transformavimo praktiką su platesniais privatumo įpareigojimais, įskaitant ES BDAR reikalavimus dėl duomenų minimizavimo ir pseudonimizavimo taikymo kaip asmens duomenų tvarkymo apsaugos priemonės.

10.1.4. P30S – Reagavimo į incidentus politika: apima pranešimo ir eskalavimo procedūras neteisėto duomenų atskleidimo atveju, įskaitant netinkamą maskuotų ar pseudonimizuotų duomenų naudojimą ar jų atkūrimą.

10.1.5. P2S – Valdysenos vaidmenų ir atsakomybių politika: nustato bendrą atskaitomybę už politikos įgyvendinimą, rizikos prisiėmimą ir išimčių tvirtinimą, pirmiausia Generaliniam vadovui.

10.2. Šios politikos sudaro integruotą duomenų apsaugos sistemą, užtikrinančią, kad maskavimo ir pseudonimizavimo priemonės prisidėtų prie ISO 27001 sertifikavimo ir atitikties skirtingiems reguliavimo reikalavimams.

**11. Pamatiniai standartai ir sistemos**

**11.1. ISO/IEC 27001**

11.1.1. 6.1.3 skyrius: reikalauja valdyti informacijos saugumo rizikas, įskaitant atskleidimo rizikos mažinimą taikant duomenų transformavimo metodus.

11.1.2. 8.1 skyrius: nustato privalomą kontrolės priemonių, būtinų saugumo tikslams pasiekti, įgyvendinimą, įskaitant pseudonimizavimą ir maskavimą.

**11.2. ISO/IEC 27002**

11.2.1. Kontrolės priemonė 8.11: pateikia gaires dėl jautrių duomenų maskavimo testavimo ir kūrimo sistemose.

11.2.2. Kontrolės priemonė 8.12: nustato strategijas, kaip užkirsti kelią duomenų iškėlimui taikant kontroliuojamą transformavimą ir prieigos valdymo praktikas.

**11.3. NIST SP 800-53 Rev.5**

11.3.1. SC-12: užtikrina informacijos konfidencialumą taikant duomenų maskavimą.

11.3.2. SC-28: saugo naudojamus ir saugomus duomenis.

11.3.3. PT-2/PT-3: skatina naudoti privatumą didinančias technologijas, įskaitant pseudonimizavimą, kai tvarkomi PII.

**11.4. ES BDAR**

11.4.1. 4 straipsnio 5 dalis: teisiškai apibrėžia pseudonimizavimą ir nustato kontrolės priemones susiejimo raktams bei identifikatoriams.

11.4.2. 5 straipsnio 1 dalies c punktas: įtvirtina duomenų minimizavimo principus taikant maskavimą.

11.4.3. 32 straipsnis: pripažįsta pseudonimizavimą kaip techninę kontrolės priemonę, mažinančią privatumo riziką.

**11.5. ES NIS2 direktyva**

11.5.1. 21 straipsnio 2 dalies c punktas: reikalauja proporcingų techninių priemonių duomenų saugumo rizikai mažinti, įskaitant pseudonimizavimą kaip rizikos valdymo kontrolės priemonę.

**11.6. ES DORA reglamentas**

11.6.1. 10 straipsnio 1 dalis: nustato privalomas su IRT susijusias rizikos kontrolės priemones, apimančias duomenų transformavimo apsaugos priemones veiklos tęstinumui ir konfidencialumui užtikrinti perduodant paslaugas išorės paslaugų teikėjams ir kuriant sistemas.

**11.7. COBIT 2019**

11.7.1. DSS05.01: reikalauja apsaugoti informacijos išteklius, įskaitant transformavimą, kai tai įmanoma.

11.7.2. DSS06.06: reikalauja taikyti tinkamus maskavimo ir pseudonimizavimo metodus, siekiant riboti duomenų atskleidimą mažesnio pasitikėjimo aplinkose.