# TECHNINĖS IR ORGANIZACINĖS SAUGUMO PRIEMONĖS

Tvarkydamas Asmens duomenis, Tvarkytojas įgyvendina žemiau išvardintas organizacines ir technines asmens duomenų apsaugos priemones, skirtas apsaugoti tvarkomus Asmens duomenis nuo atsitiktinio ar neteisėto sunaikinimo, sugadinimo, pakeitimo, praradimo, atskleidimo, taip pat nuo bet kokio kito neteisėto tvarkymo.

Atsižvelgiant į tai, kad duomenų tvarkymas yra susijęs su specialiųjų kategorijų asmens duomenų tvarkymu, kuriam taikomas Reglamento (ES) 2016/679 9 straipsnis, turėtų būti nustatytas „aukštas“ saugumo lygis.

Duomenų tvarkytojas turi teisę ir privalo priimti sprendimus dėl techninių ir organizacinių saugumo priemonių naudojimo užtikrinti reikiamą (ir suderintą) duomenų saugumo lygį.

Tvarkytojas užtikrina ir įsipareigoja:

## 1. Organizacinės duomenų saugumo priemonės

1.1. **Asmens duomenų saugumo politika ir procedūros:**

1.1.1. Asmens duomenų ir jų tvarkymo saugumas turi būti dokumentuotas kaip informacijos saugumo politikos dalis;

1.1.2. Saugumo politika turi būti peržiūrima ir prireikus atnaujinama ne rečiau kaip kartą per metus.

**1.2. Vaidmenys ir atsakomybės:**

1.2.1. Su asmens duomenų tvarkymu susiję vaidmenys ir atsakomybės turi būti aiškiai apibrėžti ir paskirstyti pagal saugumo politiką;

1.2.2. Turi būti aiškiai apibrėžtas darbuotojų teisių ir pareigų atšaukimas taikant atitinkamas vaidmenų ir atsakomybių perdavimo ar perleidimo procedūras (vidaus organizacijos pertvarkymo ar darbuotojų atleidimo, funkcijų pasikeitimo metu).

**1.3. Prieigos valdymo politika:**

1.3.1. Kiekvienam vaidmeniui, susijusiam su asmens duomenų tvarkymu, turi būti priskirtos konkrečios prieigos kontrolės teisės, vadovaujantis „būtina žinoti“ (angl. need to know) principu.

**1.4. Išteklių ir turto valdymas:**

1.4.1. Tvarkytojas turi turėti IT išteklių (naudojamų asmens duomenims tvarkyti) registrą (techninės, programinės ir tinklo įrangos sąrašą). IT išteklių registras turi apimti bent tokią informaciją: IT išteklių tipą (pvz., tarnybinę stotį, kompiuterinę darbo vietą), vietą (fizinę ar elektroninę). IT išteklių registro tvarkymas turi būti priskirtas konkrečiam asmeniui, pvz., IT specialistui.

1.4.2. IT išteklių registras turi būti reguliariai peržiūrimas ir atnaujinamas.

**1.5. Keitimų valdymas:**

1.5.1. Tvarkytojas turi užtikrinti, kad visi esminiai IT sistemų keitimai būtų stebimi ir registruojami konkretaus asmens (pvz., IT arba saugos specialisto);

**1.6. Žmogiškieji ištekliai:**

1.6.1. Tvarkytojas užtikrina, kad jo darbuotojai tvarko informaciją laikydamiesi tokio konfidencialumo lygio, kurio reikalaujama pagal Sutartį ir šią Duomenų tvarkymo sutartį;

1.6.2. Tvarkytojas užtikrina, kad atitinkami Tvarkytojo darbuotojai būtų susipažinę su informacijos, įrenginių ir sistemų naudojimo reikalavimais (įskaitant nustatytus naudojimo apribojimus) pagal Sutartį ir Duomenų tvarkymo sutartį. Valdytojas turi teisę pareikalauti Tvarkytojo pateikti įrodymus, kad jo darbuotojai susipažino su Saugumo reikalavimų turiniu ir sutinka laikytis šių reikalavimų;

1.6.3. Tvarkytojas užtikrina, kad Tvarkytojo darbuotojai, atsakingi už saugumą, yra tinkamai apmokyti vykdyti su saugumu susijusias pareigas;

1.6.4. Tvarkytojas paskiria bent vieną asmenį, turintį tinkamos kompetencijos saugumo srityje, kuris yra atsakingas už Saugumo reikalavimuose numatytų saugumo priemonių įgyvendinimą;

1.6.5. Tvarkytojas turi užtikrinti, kad visi darbuotojai būtų tinkamai informuoti apie IT sistemų saugumo reikalavimus, susijusius su jų kasdieniu darbu. Darbuotojai, susiję su asmens duomenų tvarkymu, turi būti

mokomi apie atitinkamus duomenų saugumo reikalavimus ir atsakomybes, rengiant reguliarius mokymus, informavimo renginius ar instruktažus.

## 2. Techninės duomenų saugumo priemonės

### 2.1. Prieigų kontrolė ir autentifikavimas (taikoma, jeigu asmens duomenys tvarkomi tvarkytojo sistemose):

2.1.1. Turi būti įdiegta, įgyvendinta prieigų kontrolės sistema, kuri taikoma visiems IT sistemos naudotojams. Prieigų kontrolės sistema turi leisti kurti, patvirtinti, peržiūrėti ir panaikinti naudotojų paskyras;

2.1.2. Turi būti vengiama naudoti bendras naudotojų paskyras. Vietose, kur bendra naudotojų paskyra yra būtina, turi būti užtikrinta, kad visi bendros paskyros naudotojai turi tokias pat teises ir pareigas;

2.1.3. Turi būti veikiantis autentifikavimo mechanizmas, leidžiantis prieigą prie IT sistemos (paremtas Prieigų kontrolės politika). Minimalus reikalavimas naudotojui prisijungti prie IT sistemos – naudotojo prisijungimo vardas ir slaptažodis.;

2.1.4. Slaptažodis turi būti sudaromas iš ne mažiau 8 simbolių, naudojant didžiąsias, mažąsias raides ir skaičius arba naudoti kelių faktorių autorizaciją;

2.1.5. Prieigų kontrolės sistema turi turėti galimybę aptikti ir neleisti naudoti slaptažodžių, kurie neatitinka nustatyto kompleksiškumo lygio;

2.1.6. Vartotojo slaptažodžiai turi būti saugomi naudojant kodavimo formą (angl. hash form);

2.1.7. Turi būti nustatytos ir dokumentais patvirtintos slaptažodžių naudojimo taisyklės. Taisyklėse turi būti apibrėžtas slaptažodžio ilgis, sudėtingumas, galiojimo laikas, nesėkmingų bandymų įvesti slaptažodį skaičius.

### 2.2. Techninių žurnalų įrašai ir stebėsena (taikoma, jeigu asmens duomenys tvarkomi tvarkytojo sistemose):

2.2.1. Techninių žurnalų įrašai turi būti įgyvendinti IT sistemai, naudojamai asmens duomenims tvarkyti. Techninių žurnalų įrašuose turi būti matoma visa įmanoma prieigų prie asmens duomenų informacija (pvz., data, laikas, peržiūrėjimo, keitimo, panaikinimo veiksmai);

2.2.2. Techninių žurnalų įrašai turi turėti laiko žymas ir būti apsaugoti nuo galimo sugadinimo, suklastojimo ar neautorizuotos prieigos. IT sistemose naudojami laiko apskaitos mechanizmai turi būti sinchronizuoti pagal bendrą laiko atskaitos šaltinį.

### 2.3. Duomenų bazių apsauga (taikoma, jeigu asmens duomenys tvarkomi tvarkytojo sistemose):

2.3.1. Duomenų bazės ir taikomųjų programų tarnybinės stotys turi būti sukonfigūruotos taip, kad veiktų naudodamos atskiras paskyras su priskirtomis žemiausiomis operacinės sistemos (OS) privilegijomis;

2.3.2. Duomenų bazėse ir taikomųjų programų tarnybinėse stotyse turi būti tvarkomi tik tie asmens duomenys, kurie yra reikalingi darbui, atitinkančiam duomenų tvarkymo tikslus;

2.3.3. Duomenų bazėse turi būti naudojami pseudonimizavimo metodai, atskiriant tiesioginius identifikatorius nuo esamų sąsajų su kitais duomenimis ir konkrečioms saugomoms byloms ar įrašams apsaugoti turėtų būti naudojamas šifravimas, įdiegiant atitinkamą programinę ar techninę įrangą;

### 2.4. Darbo vietų apsauga:

2.4.1. Naudotojams negalima turėti galimybės išjungti ar apeiti, išvengti IT sistemų saugos nustatymų;

2.4.2. Antivirusinės taikomosios programos ir jų informacijos apie virusus duomenų bazės turi būti atnaujinamos ne rečiau kaip kas savaitę, rekomenduojama kartą per parą ar dažniau;

2.4.3. Naudotojams negalima turėti privilegijų (teisių) diegti, šalinti, administruoti neautorizuotos programinės įrangos;

2.4.4. Slaptažodis turi būti sudaromas iš ne mažiau 8 simbolių, naudojant didžiąsias, mažąsias raides ir skaičius arba naudoti kelių faktorių autorizaciją;

2.4.5. Prieigų kontrolės sistema turi turėti galimybę aptikti ir neleisti naudoti slaptažodžių, kurie neatitinka nustatyto kompleksiškumo lygio;

2.4.6. Vartotojo slaptažodžiai turi būti saugomi naudojant kodavimo formą (angl. hash form);

2.4.7. Turi būti nustatytos ir dokumentais patvirtintos slaptažodžių naudojimo taisyklės. Taisyklėse turi būti apibrėžtas slaptažodžio ilgis, sudėtingumas, galiojimo laikas, nesėkmingų bandymų įvesti slaptažodį skaičius;

2.4.8. IT sistemos turi turėti nustatytą sesijos laiką, t. y. naudotojui esant neaktyviam sistemoje nustatytą laiką, jo sesija privalo būti nutraukta. Neaktyvios sesijos laikas – ne ilgiau kaip 15 min.;

2.4.9. Kritiniai operacinės sistemos saugos atnaujinimai privalo būti diegiami reguliariai ir nedelsiant;

2.4.10. Nešiojamieji kompiuteriai turi būti apsaugoti tokiomis apsaugos priemonėmis, kurios atitiktų duomenų tvarkymo keliamą riziką, t. y. nešiojamųjų kompiuterių šifravimas ir kitas reikalingas priemones;
2.4.11. Kompiuterinės darbo vietos, turi būti valdomos centralizuotai.

**2.5. Tinklo ir komunikacijos sauga:**

2.5.1. Kai prieiga prie naudojamų IT sistemų yra vykdoma internetu, privaloma naudoti šifruotą komunikacijos kanalą, t. y. kriptografinius protokolus (pvz., TLS/SSL) ir kitus atitinkamus šifravimo protokolus;
2.5.2. Bet koks duomenų judėjimas iš, į IT sistemą turi būti stebimas ir kontroliuojamas naudojant ugniasienes ir įsibrovimo (įsilaužimo) aptikimo ir prevencijos sistemas;
2.5.3. Įsibrovimo testavimą atlikti (angl. Penetration testing) tinklui ir naudojamai sistemai, kuri pasiekiama iš išorinio tinklo bent kartą į 1 metus.

**2.6. Atsarginės kopijos (taikoma, jeigu asmens duomenys tvarkomi tvarkytojo sistemose):**

2.6.1. Atsarginės kopijos ir duomenų atstatymo procedūros privalo būti apibrėžtos, dokumentuotos ir aiškiai susietos su vaidmenimis ir pareigomis;
2.6.2. Atsarginių kopijų laikmenoms privalo būti užtikrintas tinkamas fizinis aplinkos, patalpų saugos lygis, priklausantis nuo saugomų duomenų;
2.6.3. Atsarginių kopijų darymo procesas turi būti stebimas, siekiant užtikrinti užbaigtumą ir išsamumą;
2.6.4. Pilnos atsarginės duomenų kopijos privalo būti daromos reguliariai. Rekomenduojamas atsarginių kopijų darymo dažnumas: kasdien – pridedamoji kopija, kas savaitę – pilna kopija;
2.6.5. Atsarginės kopijos turi būti šifruotos;

2.7. Turi būti parengtas detalus verslo tęstinumo planas ir paskirti atsakingi asmenys rizikoms kontroliuoti ir joms valdyti bei turi būti apibrėžtas garantuotos paslaugų kokybės lygis (angl. Service-level agreement (SLA), kuris nustatomas pagrindiniams veiklos procesams, kurie užtikrina asmens duomenų saugumą.

**2.8. Mobilieji, nešiojamieji įrenginiai:**

2.8.1. Mobiliųjų, nešiojamųjų įrenginių administravimo procedūros privalo būti nustatytos ir dokumentuotos, aiškiai aprašant tinkamą tokių įrenginių naudojimą;
2.8.2. Mobilieji ir nešiojamieji įrenginiai, kuriais bus naudojamasi darbui su informacinėmis sistemomis, prieš naudojimąsi turi būti užregistruoti ir autorizuoti;
2.8.3. Mobilieji, nešiojamieji įrenginiai turi būti pakankamo prieigos kontrolės procedūrų lygio, kaip ir kita naudojama įranga asmens duomenims tvarkyti;
2.8.4. Mobiliųjų, nešiojamųjų įrenginių valdymo funkcijos ir atsakomybės turi būti aiškiai apibrėžtos;
2.8.5. Darbui iš namų turi būti taikomos atitinkamos saugumo priemonės asmens duomenų saugumui ir turėti patvirtintą politiką.

**2.9. Programinės įrangos sauga (taikoma, jeigu asmens duomenys tvarkomi tvarkytojo sistemose):**

2.9.1. Informacinėse sistemose naudojama programinė įranga (asmens duomenims tvarkyti) turi atitikti programinės įrangos saugos gerąją praktiką, programinės įrangos kūrime taikomą saugos gerąją praktiką, programinės įrangos kūrimo struktūras (angl. frameworks), standartus (pvz., Agile, OWASP ir kt.);
2.9.2. Programinės įrangos kūrimas turi būti atliekamas specialioje aplinkoje, kuri nėra prijungta prie IT sistemų, naudojamų tvarkant asmens duomenis. Testuojant sistemas, reikia naudoti testinius duomenis. Tais atvejais, kai tai neįmanoma, turi būti nustatytos specialios testavimo metu naudojamų asmens duomenų apsaugos procedūros;
2.9.3. Po programinės įrangos kūrimo, testavimo ir verifikacijos, pradedant sistemos įdiegimą ir eksploataciją, jau turi būti laikomasi pagrindinių saugos reikalavimų;
2.9.4. Tais atvejais, kai Tvarkytojas iš Valdytojo gautų asmens duomenų tvarkymui pasitelkia debesijos ar kitas duomenų talpyklų paslaugas (pvz., talpina ir saugo asmens duomenis debesies saugykloje):
2.9.4.1. Tvarkytojas arba tvarkytojo paslaugų teikėjas teikiantis paslaugas turi būti sertifikuotas pagal ISO 27001 standartą, arba turėti kitus lygiaverčius informacijos saugumo valdymo užtikrinimo priemonių įrodymus (aprašus)
2.9.4.2. paslaugų duomenų centrai turi būti Europos ekonominės erdvės šalyje, o saugomi duomenys negali būti perkelti už Europos ekonominės erdvės ribų.

**2.10. Duomenų naikinimas, šalinimas:**

2.10.1. Prieš pašalinant bet kokią duomenų laikmeną, turi būti sunaikinti visi joje esantys duomenys, naudojant tam skirtą programinę įrangą, kuri palaiko patikimus duomenų naikinimo algoritmus. Jei to padaryti

neįmanoma (pvz., USB laikmenos), turi būti įvykdytas fizinis duomenų laikmenos sunaikinimas be galimybės atstatyti;

2.10.2. Popierinės ir nešiojamosios duomenų laikmenos (pvz., USB laikmenos), kuriose buvo saugomi, kaupiami asmens duomenys, turi būti naikinamos tam skirtais smulkintuvais arba kitomis mechaninėmis priemonėmis.

**2.11. Fizinė prieigos kontrolė:**

2.11.1. Turi būti įgyvendinta fizinė aplinkos, patalpų, kuriose yra IT sistemų infrastruktūra, apsauga nuo neautorizuotos prieigos.

## 3. Atitiktis

3.1. Valdytojo prašymu Tvarkytojas nedelsiant pateikia Valdytojui atitikties Saugumo reikalavimams ataskaitą. Ataskaitos formą Valdytojas pateiks Tvarkytojui kartu su prašymu.

3.2. Aukščiau paminėti reikalavimai ne mažesne apimtimi taikomi visiems Tvarkytojo pasitelktiems pagalbiniams tvarkytojams, jeigu Valdytojas neprieštarauja, kad Tvarkytojas pasitelktų pagalbinius tvarkytojus.

3.3. Valdytojas kaip nurodyta šioje Sutartyje, turi teisę audito būdu įsitikinti, kad Tvarkytojas laikosi šių reikalavimų.

| Valdytojas | Tvarkytojas |
| --- | --- |