VALSTYBINĖ DUOMENŲ APSAUGOS INSPEKCIJA

SAUGUMO PRIEMONIŲ (PRIVILEGIJUOTŲJŲ PRIEIGOS TEISIŲ, ASMENS DUOMENŲ NAIKINIMO, ŠIFRAVIMO PRIEMONIŲ NAUDOJIMO, PAKEITIMŲ VALDYMO) STEBĖSENOS APIBENDRINIMAS

2025 m.

Valstybinė duomenų apsaugos inspekcija (toliau – Inspekcija), vadovaudamasi Valstybinės duomenų apsaugos inspekcijos 2024 metų planinių patikrinimų ir stebėsenos planu[1], rašytinės apklausos būdu atliko 10 internetinių parduotuvių (toliau – Bendrovės) tvarkomų asmens duomenų saugumo priemonių (privilegijuotųjų prieigos teisių, asmens duomenų naikinimo, šifravimo priemonių naudojimo, pakeitimų valdymo) stebėseną. Stebėsenos buvo atliekamos naudojant patvirtintą kontrolinį klausimyną[2].

Inspekcija, apibendrinusi atliktų stebėsenų rezultatus, išskyrė toliau pateiktus dažniausiai nustatytus su saugumo priemonėmis susijusius 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamento (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) (toliau – BDAR) neatitikimus reglamento reikalavimams.

Privilegijuotosios prieigos teisės

1. Stebėsenų metu patikrinta, ar Bendrovės įgyvendino privilegijuotųjų prieigos teisių kontrolę prie informacinių sistemų ir procesų, susijusių su el. parduotuvėje tvarkomais asmens duomenimis.

BDAR 5 straipsnio 1 dalyje f punkte reglamentuota, kad asmens duomenys turi būti tvarkomi tokiu būdu, kad taikant atitinkamas technines ar organizacines priemones būtų užtikrintas tinkamas asmens duomenų saugumas, įskaitant apsaugą nuo duomenų tvarkymo be leidimo arba neteisėto duomenų tvarkymo ir nuo netyčinio praradimo, sunaikinimo ar sugadinimo (vientisumo ir konfidencialumo principas). Tvarkomų asmens duomenų saugumo priemonių ir rizikos įvertinimo gairių duomenų valdytojams ir duomenų tvarkytojams[3] (toliau – Gairės) 13–20 punktuose pateiktos nuostatos yra skirtos prieigos valdymui. Privilegijuotųjų prieigos teisių naudotojams yra taikomi tie patys baziniai principai, tačiau jie papildomi griežtesniais reikalavimais, kad būtų užtikrinta maksimali duomenų apsauga (pvz., didesnis prieigos kontrolės detalumas: reikalingas išsamus dokumentavimas, kas ir kada turi privilegijuotą prieigą; didesnė stebėsena: privilegijuotų teisių naudojimas turi būti nuolat stebimas, o

---

[1] Valstybinės duomenų apsaugos inspekcijos 2024 metų planinių patikrinimų ir stebėsenos planas, patvirtintas Valstybinės duomenų apsaugos inspekcijos direktoriaus 2024-02-16 įsakymu Nr. 1T-26 (1.12.E) „Dėl Valstybinės duomenų apsaugos inspekcijos 2024 metų planinių patikrinimų ir stebėsenos plano patvirtinimo“.

[2] Kontrolinis klausimynas, skirtas saugumo priemonių (privilegijuotųjų prieigos teisių, asmens duomenų naikinimo, šifravimo priemonių naudojimo, pakeitimų valdymo) stebėsenai, patvirtintas Valstybinės duomenų apsaugos inspekcijos direktoriaus pavaduotojo 2024 m. birželio 17 d. įsakymu Nr. 1T-59 (1.12.E) „Dėl kontrolinio klausimyno, skirto saugumo priemonių (privilegijuotųjų prieigos teisių, asmens duomenų naikinimo, šifravimo priemonių naudojimo, pakeitimų valdymo) stebėsenai, patvirtinimo“

[3] https://vdai.lrv.lt/public/canonical/1725443426/586/VDAI_saugumo_priemoniu_gaires-2024-08-19.pdf

veiklos žurnalai peržiūrimi; mažinamas privilegijuotųjų prieigos teisių naudotojų skaičius: privilegijuotų naudotojų turėtų būti tik tiek, kiek būtina.)

Inspekcija, įvertinusi Bendrovių pateiktą informaciją ir įrodymus dėl el. parduotuvių tvarkomų asmens duomenų, daro išvadą, kad Bendrovės įgyvendino privilegijuotųjų prieigos teisių kontrolę.

Gerosios praktikos pavyzdžiai valdant privilegijuotąsias prieigos teises:

1. **Aiški ir dokumentuota prieigos kontrolės politika** – sukurkite aiškiai apibrėžtą politiką, kuri reglamentuotų privilegijuotųjų prieigos teisių valdymą, suteikimą, peržiūrą ir panaikinimą.
2. **Principų „būtina žinoti“ ir „būtina naudoti“ taikymas** – užtikrinkite, kad privilegijuotos prieigos teisės būtų suteiktos tik tiems naudotojams ir tik tokiam laikotarpiui, kuris būtinas jų funkcijoms atlikti.
3. **Prieigos suteikimo ir peržiūros procesų dokumentavimas** – kiekvienas prieigos teisės suteikimas, keitimas ar panaikinimas turi būti išsamiai dokumentuotas. Registruokite, kas, kada ir kodėl gavo privilegijuotą prieigą.
4. **Daugiafaktorinio autentifikavimo naudojimas** – privilegijuotiems naudotojams privaloma taikyti daugiafaktorinį autentifikavimą, siekiant sustiprinti prieigos apsaugą.
5. **Prieigos teisių reguliari peržiūra** – periodiškai peržiūrėkite privilegijuotas prieigos teises, kad užtikrintumėte, jog jos atitinka naudotojų vaidmenis ir užduotis.
6. **Prieigos veiklos stebėsena ir auditas** – naudokite žurnalus, kad stebėtumėte privilegijuotųjų prieigos teisių naudojimą. Užtikrinkite, kad žurnalai būtų peržiūrimi reguliariai, o anomalijos tiriamos.
7. **Prieigos teisių apribojimas** – mažinkite privilegijuotųjų prieigos teisių naudotojų skaičių, užtikrindami, kad tik būtini asmenys turėtų tokias teises.
8. **Incidentų valdymas ir reagavimo planai** – nustatykite procedūras, kaip reaguoti į privilegijuotųjų prieigos teisių pažeidimus ar įtartinus veiksmus.
9. **Reguliarus darbuotojų mokymas** – mokykite privilegijuotųjų prieigos teisių naudotojus apie jų atsakomybę, geriausią praktiką ir galimas saugumo grėsmes.
10. **Technologinių priemonių taikymas** – naudokite automatizuotas sistemas, skirtas privilegijuotųjų teisių valdymui, pvz., prieigos valdymo įrankius (angl. *Privileged Access Management*).

2. Stebėsenų atlikimo metu nustatyta, kad Bendrovių privilegijuotųjų prieigos teisių suteikimas yra dokumentuotas.

Gairių 15 punkte pateiktos nuostatos yra skirtos prieigos valdymo politikai. Gairėse nurodyta, kad prieigos valdymo politika turi būti išsami ir dokumentuota. Organizacija šiame dokumente turi nustatyti atitinkamas prieigos kontrolės taisykles, prieigos teises ir apribojimus pagal konkrečias naudotojų pareigas, susijusias su asmens duomenų tvarkymo procesais ir procedūromis.

Inspekcija, įvertinusi Bendrovių pateiktą informaciją ir įrodymus dėl internetinių parduotuvių tvarkomų asmens duomenų, daro išvadą, kad Bendrovių privilegijuotųjų prieigos teisių suteikimas yra dokumentuotas.

Gerosios praktikos, susijusios su privilegijuotųjų prieigos teisių suteikimo dokumentavimu, apima aiškios ir išsamios prieigos valdymo politikos parengimą, kurioje nustatomos taisyklės, teisės ir apribojimai pagal naudotojų pareigas. Kiekvienas privilegijuotųjų teisių suteikimas turi būti dokumentuotas, įskaitant suteikimo pagrindimą, procesą ir patvirtinimus. Rekomenduojama standartizuoti prieigos suteikimo procedūras, apibrėžti naudotojų vaidmenis ir susijusias prieigos teises bei pildyti registrus, kuriuose fiksuojama, kas, kada ir kokias teises gavo. Taip pat būtina reguliariai peržiūrėti privilegijuotąsias prieigos teises, užtikrinti veiklos žurnalų saugojimą ir naudoti technologinius procesų valdymo bei stebėsenos sprendimus. Svarbu organizuoti atsakingų darbuotojų mokymus, didinti

jų informuotumą ir reguliariai atlikti atitikties auditus, siekiant užtikrinti prieigos valdymo procesų skaidrumą ir saugumą.

3. Stebėsenų atlikimo metu nustatyta, kad Bendrovių privilegijuotosios prieigos teisės nėra bendrinamos ir yra priskirtos tik individualiems naudotojams.

Gairių 18 punkte pateiktos nuostatos yra skirtos prieigos teisių valdymui. Gairėse nurodyta, kad prieigos teisės turi būti suteikiamos / keičiamos pagal veiklos reikalavimus (vaidmenis) ir prieigos valdymo taisykles bei gavus vadovybės leidimą / patvirtinimą būtų aktyvuojamos tik sėkmingai atlikus visas procedūras. Prieigos teisės turi būti panaikinamos, kai nebereikia prieigos (pasikeitė veikla, pareigos) prie asmens duomenų. Ypač svarbu, kad organizacija nedelsdama panaikintų prieigos teises naudotojams, kurie nutraukė darbo / sutartinius santykius su organizacija (laikas, pvz., ne vėliau kaip paskutinę darbo / sutartinių santykių dieną, turi būti numatytas prieigos valdymo politikoje).

Inspekcija, įvertinusi Bendrovių pateiktą informaciją ir įrodymus dėl internetinių parduotuvių tvarkomų asmens duomenų, daro išvadą, kad Bendrovėse prieigos teisės nėra bendrinamos ir yra priskirtos tik individualiems naudotojams.

4. Stebėsenų atlikimo metu nustatyta, kad dauguma Bendrovių privilegijuotoms prieigos teisėms užtikrinti taiko kelių veiksnių autentifikaciją (MFA).

Gairių 91 punkte pateiktos nuostatos yra skirtos privilegijuotiems prieigos teisių naudotojams. Gairėse nurodyta, kad privilegijuotų naudotojų (pvz., sistemų administratorių) prisijungimui prie asmens duomenų tvarkymo sistemų turi būti taikomas kelių veiksnių autentifikavimas. Visais atvejais, kai į tokias sistemas jungiamasi ne iš vidinio kompiuterių tinklo, turi būti naudojamos ir papildomos saugumo priemonės, tokios kaip IP adreso kontrolė, virtualus privatus tinklas (angl. VPN) ir kiti atitinkami saugumo mechanizmai. Autentifikavimo veiksniais gali būti slaptažodžiai, saugumo žetonai, USB raktai su slapta žyma, biometriniai duomenys ir kt.

Inspekcija, įvertinusi Bendrovių pateiktą informaciją ir įrodymus dėl internetinių parduotuvių tvarkomų asmens duomenų, daro išvadą, kad dauguma Bendrovių įgyvendino kelių veiksnių autentifikaciją (MFA) privilegijuotąsias prieigos teises turintiems naudotojams.

5. Stebėsenų atlikimo metu nustatyta, kad Bendrovės turi nustatytas taisykles, kurios riboja bendrinių naudotojų identifikatorių (pvz., *Root*) naudojimą, įvertinus sistemų konfigūracijos galimybes.

Gairių 112 punkte pateiktos nuostatos yra skirtos privilegijuotiems prieigos teisių naudotojams, turintiems operacinių sistemų administratoriaus (angl. *Root*) teises, atskirti perteklinių funkcijų vykdymą. Gairėse nurodyta, kad duomenų bazės ir taikomųjų programų tarnybinės stotys turi būti sukonfigūruotos taip, kad veiktų naudodamos atskiras paskyras su priskirtomis žemiausiomis operacinės sistemos privilegijomis.

Inspekcija, įvertinusi Bendrovių pateiktą informaciją ir įrodymus dėl internetinių parduotuvių tvarkomų asmens duomenų, daro išvadą, kad Bendrovės riboja bendrinių naudotojų identifikatorių (pvz., *Root*) naudojimą.

6. Stebėsenų atlikimo metu nustatyta, kad dauguma Bendrovių įvykių žurnaluose registruoja visus veiksmus, kuriuos atlieka privilegijuotąsias prieigas turintys naudotojai.

Gairių 119–120 punktuose pateiktos nuostatos yra skirtos privilegijuotųjų prieigos teisių naudotojų veiksmams registruoti. Gairėse nurodyta, kad visi sistemų administratorių veiksmai (taip pat ir jų atliekamas naudotojų teisių papildymas, panaikinimas, keitimas) turi būti registruojami. Turi būti

neįmanoma ištrinti ar pakeisti techninių įrašų turinio. Prieiga prie įrašų taip pat turi būti registruojama, siekiant atlikti neįprastų veiksmų susekimo stebėseną.

Inspekcija, įvertinusi Bendrovių pateiktą informaciją ir įrodymus dėl internetinių parduotuvių tvarkomų asmens duomenų, daro išvadą, kad dauguma Bendrovių įvykių žurnaluose registruoja visus veiksmus, kuriuos atlieka privilegijuotąsias prieigas turintys naudotojai.

Asmens duomenų naikinimas

1. Stebėsenų atlikimo metu nustatyta, kad dauguma Bendrovių yra nustatyti saugojimo terminai naudotojų asmens duomenims saugoti.

Asmens duomenų apsaugos gairių smulkiajam ir vidutiniam verslui[4] (toliau – Gairės SVV) pateiktos nuostatos yra skirtos padėti nustatyti ir apibrėžti asmens duomenų saugojimo terminus. Gairių SVV skyriuje „Koks gali būti saugojimo terminas“ pateikiamas pavyzdys, kuriame nurodoma, kad internetinėje parduotuvėje klientų asmens duomenys gali būti saugomi 1 metus nuo paskutinio kliento prisijungimo prie paskyros. Vis dėlto Gairės SVV nenustato privalomų konkrečių saugojimo terminų, o tik pateikia orientacines rekomendacijas, kurias įmonės gali pritaikyti pagal savo veiklos pobūdį ir teisės aktų reikalavimus.

Dauguma Bendrovių nurodė, kad jos el. parduotuvėje klientų paskyrų duomenys saugomi 1 metus po paskutinio prisijungimo, o duomenys apie nepanaudotus kuponus – 6 mėnesius nuo jų galiojimo pabaigos..

Inspekcija, įvertinusi Bendrovių pateiktą informaciją ir įrodymus dėl internetinių parduotuvių tvarkomų asmens duomenų, daro išvadą, kad dauguma Bendrovių naudotojų asmens duomenys yra saugomi pagal nustatytus terminus.

2. Stebėsenų atlikimo metu nustatyta, kad Bendrovių asmens duomenų saugojimo ir naikinimo tvarka yra aiškiai dokumentuota.

Gairių SVV skyriuje „Kaip elgtis pasibaigus duomenų saugojimo terminui?“ nurodyta, kad pasibaigus nustatytiems duomenų saugojimo terminams asmens duomenis privaloma sunaikinti arba anonimizuoti. Todėl svarbu įdiegti procedūras, užtikrinančias, kad asmens duomenys, pasibaigus jų saugojimo terminui, toliau nebebūtų tvarkomi.

Inspekcija, įvertinusi Bendrovių pateiktą informaciją ir įrodymus dėl internetinių parduotuvių tvarkomų asmens duomenų, daro išvadą, kad Bendrovėse asmens duomenų saugojimo ir naikinimo tvarka yra aiškiai dokumentuota.

Geroji praktika nustatant asmens duomenų saugojimo ir naikinimo tvarką apima aiškiai dokumentuotą procesą, kuriame nustatomi duomenų saugojimo terminai, jų kontrolė ir veiksmai pasibaigus šiems terminams. Svarbu, kad organizacija turėtų procedūras, kurios užtikrintų, jog pasibaigus saugojimo terminui asmens duomenys būtų sunaikinami arba anonimizuojami pagal nustatytas taisykles. Naikinimo veiksmus turi apibrėžti konkretūs veiksmai, pavyzdžiui, skaitmeninių duomenų šalinimas naudojant saugius metodus ar fizinių dokumentų smulkinimas. Be to, atsakomybė už šiuos procesus turi būti aiškiai paskirstyta, o veiksmų dokumentavimas ir stebėsena užtikrintų, kad visi duomenys būtų tvarkomi pagal teisės aktų reikalavimus. Automatizuoti sprendimai, reguliarios procedūrų peržiūros ir atnaujinimai padeda užtikrinti efektyvų ir teisėtą asmens duomenų valdymą.

[4] https://vdai.lrv.lt/uploads/vdai/documents/files/01_%20SolPriPa%20Asmens%20duomenu%20apsaugos%20gaires%20SMULKIAJAM%20IR%20VIDUTINIAM%20VERSLUI%202019-11-08.pdf

3. Stebėsenų atlikimo metu nustatyta, kad Bendrovės užtikrina, kad duomenys nebūtų saugomi ilgiau nei numatyta naudojant patvirtintas priemones.

Bendrovių internetinėse parduotuvėse yra įdiegtas techninis / automatinis duomenų ištrynimo mechanizmas / sprendimas. Taip pat papildomai kiekvienas klientas gali pasinaudoti „Teise būti pamirštam“ ir pateikti užklausą ištrinti jo duomenis profilio skiltyje „Asmens duomenų valdymas“ paspausdamas mygtuką „Noriu ištrinti paskyrą“.

Inspekcija, įvertinusi Bendrovių pateiktą informaciją ir įrodymus dėl internetinių parduotuvių tvarkomų asmens duomenų, daro išvadą, kad Bendrovės užtikrina, kad duomenys nebūtų saugomi ilgiau nei numatyta naudojant patvirtintas priemones.

4. Stebėsenų atlikimo metu nustatyta, kad Bendrovėse yra aprašytos ir įgyvendintos naudotojų asmens duomenų naikinimo arba nuasmeninimo[5] procedūros.

Bendrovių internetinėse parduotuvėse duomenys ištrinami automatiškai suėjus nurodytam duomenų tvarkymo terminui. Klientui priėmus sprendimą savarankiškai ištrinti duomenis, jis savo profilio skiltyje „Asmens duomenų valdymas“ pateikia užklausą ištrinti savo duomenis. Pateikus užklausą, klientas gauna patvirtinimo nuorodą el. paštu, kurią paspaudęs patvirtina, kad tikrai nori būti pamirštas ir ištrinti visus asmeninius duomenis. Patvirtinus užklausą yra ištrinama kliento paskyra ir iš duomenų bazės pašalinami kliento duomenys.

Inspekcija, įvertinusi Bendrovių pateiktą informaciją ir įrodymus dėl internetinių parduotuvių tvarkomų asmens duomenų, daro išvadą, kad Bendrovės turi aprašytas ir įgyvendintas naudotojų asmens duomenų naikinimo arba nuasmeninimo procedūras.

Geroji praktika nustatant asmens duomenų nuasmeninimo procedūras apima aiškiai apibrėžtus ir dokumentuotus procesus, kurie užtikrina, kad asmens duomenys būtų tvarkomi saugiai ir laikantis teisės aktų. Organizacijos turi taikyti nuasmeninimo metodus, tokius kaip pseudonimų suteikimas[6], kuris leidžia duomenis naudoti analizei ar statistikai, tačiau užtikrina, kad asmuo nebūtų tiesiogiai atpažįstamas. Gerosios praktikos pavyzdžiai apima automatizuotus nuasmeninimo procesus, klientų informavimą apie jų duomenų tvarkymo galimybes ir nuolatinę procedūrų peržiūrą, kad būtų užtikrinta nuosekli teisės aktų bei technologijų pažangos atitiktis. Be to, svarbu, kad nuasmeninimo procesai būtų nuolat audituojami ir atnaujinami, užtikrinant efektyvumą ir teisėtumą.

Šifravimo priemonių naudojimas

1. Stebėsenų atlikimo metu nustatyta, kad Bendrovių internetinėse svetainėse / aplikacijose asmens duomenys yra šifruojami, įskaitant atsargines kopijas.

Bendrovių internetinėse parduotuvėse asmens duomenys yra šifruojami (pvz., šifruojami iš e-sveikatos pateikto užsakymo duomenys, taip pat paciento asmens kodas / recepto numeris) jų perdavimo momentu.

BDAR 32 straipsnis numato pareigą gebėti laiku atkurti sąlygas ir galimybes naudotis asmens duomenimis fizinio ar techninio incidento atveju. Gairių 137 punkte pateiktos nuostatos yra skirtos atsarginių kopijų valdymui ir nurodyta, kad atsarginės kopijos turi būti šifruojamos ir saugiai laikomos

---

[5] Fizinio asmens duomenų pakeitimas anoniminiais duomenimis, kad jų nebūtų galima sieti su tuo asmeniu, kurio tapatybė yra žinoma arba gali būti nustatyta, arba fizinio asmens duomenų anonimiškumo užtikrinimas taip, kad nebūtų galima nustatyti to asmens tapatybės.

[6] Pseudonimų suteikimas – asmens duomenų tvarkymas taip, kad asmens duomenys nebegalėtų būti priskirti konkrečiam duomenų subjektui nesinaudojant papildoma informacija, jeigu tokia papildoma informacija yra saugoma atskirai ir jos atžvilgiu taikomos techninės bei organizacinės priemonės siekiant užtikrinti asmens duomenų nepriskyrimą fiziniam asmeniui, kurio tapatybė yra nustatyta arba kurio tapatybę galima nustatyti.

visiškai atsijungus (angl. *Offline*) nuo kompiuterinių tinklų. Nustatyta, kad Bendrovių internetinių parduotuvių atsarginės kopijos yra šifruojamos TDE (angl. *Transparent data encryption*), o diskai, kuriuose saugomos kopijos ir naudojami duomenys, yra papildomai šifruojami SSE su PMK (angl. *Storage Service Encryption with a Platform-Managed Key*).

Geroji praktika ir rekomendacijos dėl asmens duomenų šifravimo apima ne tik duomenų perdavimą ir atsarginių kopijų saugojimą, bet ir pačių duomenų saugojimą. Saugomi duomenys turi būti šifruojami naudojant stiprius šifravimo metodus, kad būtų užtikrintas duomenų saugumas ir apsauga nuo neteisėtos prieigos, net jei jie yra laikomi serveriuose ar kituose saugojimo įrenginiuose. Rekomenduojama naudoti šifravimo technologijas, tokias kaip TDE (angl. *Transparent Data Encryption)* ir SSE su PMK (angl. *Storage Service Encryption with a Platform-Managed Key*), kurios užtikrina tiek duomenų šifravimą, tiek jų saugojimą su papildoma apsauga. Be to, svarbu užtikrinti, kad šifravimo raktai būtų tvarkomi saugiai, o prieiga prie šių duomenų būtų griežtai kontroliuojama ir stebima. Tokios priemonės užtikrina, kad asmens duomenys būtų apsaugoti nuo galimų pažeidimų ir būtų laikomi pagal BDAR reikalavimus, įskaitant atsparumą fiziniams ir techniniams incidentams.

Inspekcija, įvertinusi Bendrovių pateiktą informaciją ir įrodymus dėl internetinių parduotuvių tvarkomų asmens duomenų, daro išvadą, kad Bendrovių internetinėse svetainėse / aplikacijose asmens duomenys yra šifruojami, įskaitant atsargines kopijas.

2. Stebėsenų atlikimo metu nustatyta, kad reikalavimas šifruoti asmens duomenis Bendrovių internetinėse parduotuvėse yra dokumentuotas.

Reikalavimas šifruoti asmens duomenis įtvirtintas Bendrovių internetinėse parduotuvėse informacijos saugumo politikoje, detalizuoti reikalavimai šifravimui patvirtinti pagrindinėse kriptografijos taisyklėse.

Gairių 131 punkte pateiktos nuostatos yra skirtos atsarginių kopijų valdymui ir nurodyta, kad atsarginės kopijos ir duomenų atstatymo procedūros privalo būti apibrėžtos, dokumentuotos ir aiškiai susietos su vaidmenimis ir pareigomis.

BDAR 32 straipsnio 1 dalyje reglamentuota, kad „Duomenų valdytojas ir duomenų tvarkytojas turi įdiegti atitinkamas technines ir organizacines priemones, kad užtikrintų asmens duomenų saugumą, atsižvelgiant į riziką, susijusią su jų tvarkymu, įskaitant, kai tinkama, šifravimą.“ Tai reiškia, kad šifravimas turi būti taikomas ne tik atsarginėms kopijoms, bet ir kitoms asmens duomenų kategorijoms, ypač kai duomenys yra perduodami arba saugomi. Todėl reikalavimas šifruoti asmens duomenis turėtų būti išplėstas ir apimti visus asmens duomenis, kurie yra tvarkomi ir saugomi organizacijose, įskaitant duomenų perdavimą ir jų saugojimą, o ne tik atsargines kopijas.

BDAR 32 straipsnio nuostatos reikalauja, kad organizacijos užtikrintų tinkamą asmens duomenų apsaugą naudojant šifravimą kaip priemonę, kad apsaugotų duomenis nuo neleistinos prieigos ir užtikrintų jų konfidencialumą. Toks požiūris į šifravimą būtų ne tik rekomendacija, bet ir privaloma praktika pagal BDAR, kad būtų laikomasi duomenų apsaugos reikalavimų.

Inspekcija, įvertinusi Bendrovių pateiktą informaciją ir įrodymus dėl internetinių parduotuvių tvarkomų asmens duomenų, daro išvadą, kad Bendrovių internetinėse svetainėse reikalavimas šifruoti asmens duomenis yra dokumentuotas.

3. Stebėsenų atlikimo metu nustatyta, kad Bendrovės internetinėse parduotuvėse naudoja duomenų šifravimo algoritmus, jie yra aiškiai aprašyti ir atitinka pažangius saugumo standartus.

Bendrovės internetinėse parduotuvėse naudoja duomenų tokius šifravimo algoritmus kaip AEAD_AES_256_CBC_HMAC_SHA_256.

Atsižvelgdamas į BDAR 24 straipsnio 1 dalį, duomenų valdytojas įgyvendina tinkamas technines ir organizacines priemones ir Gairių SVV pateiktas asmens duomenų saugumo priemones, kurios gali būti taikomos apsaugant asmens duomenis. Duomenų valdytojas įgyvendina duomenų šifravimą naudodamas algoritmus, atitinkančius pažangius saugumo standartus.

Inspekcija, įvertinusi Bendrovių pateiktą informaciją ir įrodymus dėl internetinių parduotuvių tvarkomų asmens duomenų, daro išvadą, kad Bendrovės internetinėse svetainėse naudoja duomenų šifravimo algoritmus, jie yra aiškiai aprašyti ir atitinka saugumo standartus.

4. Stebėsenų atlikimo metu nustatyta, kad dauguma Bendrovių internetinėse parduotuvėse yra sukurtos ir įdiegtos kriptografijos bei kriptografinių raktų valdymo taisyklės.

Daugumos Bendrovių internetinėse parduotuvėse yra sukurti kriptografiniai raktai, kurie valdomi ir priskiriami tik per tam tikrą (pvz., *Azure key vault*) servisą. Prieiga prie serviso yra susieta su konkrečiu privilegijuotas prieigų teises turinčiu naudotoju.

Inspekcija, įvertinusi Bendrovių pateiktą informaciją ir įrodymus dėl internetinių parduotuvių tvarkomų asmens duomenų, daro išvadą, kad dauguma Bendrovių internetinėse svetainėse yra sukurtos ir įdiegtos kriptografijos bei kriptografinių raktų valdymo taisyklės.

Pakeitimų valdymas

1. Stebėsenų atlikimo metu nustatyta, kad dauguma Bendrovių turi IT keitimų valdymo politikas.

Gairių 139 punkte pateiktos nuostatos yra skirtos keitimų valdymui ir nurodyta, kad turi būti įdiegta išsami ir dokumentais pagrįsta IT keitimų valdymo politika. Keitimų valdymo politika turi apibrėžti: pokyčių įvedimo ir įdiegimo procedūras, pareigybes ir naudotojus, kurių teisės buvo pakeistos, pokyčių įdiegimo laiko terminus. Pokyčių valdymo politika turi būti reguliariai atnaujinama.

Inspekcija, įvertinusi Bendrovių pateiktą informaciją ir įrodymus dėl internetinių parduotuvių tvarkomų asmens duomenų, daro išvadą, kad daugumoje Bendrovių internetinėse svetainėse veikia išsami, dokumentais pagrįsta IT keitimų valdymo politika.

2. Stebėsenų atlikimo metu nustatyta, kad Bendrovėse pakeitimų valdymo procedūros taikomos visoms informacijos apdorojimo priemonėms ir informacinėms sistemoms.

Gairių skyriuje „Keitimų valdymas“ apibrėžtas pakeitimų valdymo procedūrų tikslas – sinchronizuoti ir kontroliuoti visose IT sistemose atliekamus keitimus tvarkant asmens duomenis. Tai yra svarbi saugumo priemonė, nes nesėkmingas keitimų įgyvendinimas gali sukelti neteisėtą duomenų atskleidimą, pakeitimą ar sunaikinimą. Keitimų valdymas yra būtinas duomenų tvarkymo vientisumui užtikrinti, taip pat siekiant įgyvendinti BDAR 5 straipsnio 1 dalies f punktą ir duomenų valdytojo atskaitomybės principą pagal BDAR 5 straipsnio 2 dalį.

Inspekcija, įvertinusi Bendrovių pateiktą informaciją ir įrodymus dėl internetinių parduotuvių tvarkomų asmens duomenų, daro išvadą, kad Bendrovėse pakeitimų valdymo procedūros taikomos visoms informacijos apdorojimo priemonėms ir informacinėms sistemoms.

3. Stebėsenų atlikimo metu nustatyta, kad Bendrovėse visi esminiai IT sistemų keitimai yra stebimi, registruojami ir priskiriami konkrečiam atsakingam asmeniui.

Gairių 138 punkte pateiktos nuostatos yra skirtos keitimų valdymui, kuriame yra nurodyta, kad organizacija turi užtikrinti, kad visi esminiai IT sistemų keitimai būtų stebimi ir registruojami konkretaus asmens (pvz., IT arba saugos specialisto).

Visos Bendrovės turi paskirtą atsakingą asmenį IT sistemų keitimams stebėti ir registruoti.

Inspekcija, įvertinusi Bendrovių pateiktą informaciją ir įrodymus dėl internetinių parduotuvių tvarkomų asmens duomenų, daro išvadą, kad visi esminiai Bendrovių IT sistemų keitimai yra stebimi, registruojami ir priskiriami konkrečiam atsakingam asmeniui.

Toliau pateikiamos rekomendacijos, skirtos organizacijoms, siekiančioms užtikrinti asmens duomenų apsaugą ir atitiktį BDAR reikalavimams, ypač skiriant dėmesį privilegijuotųjų prieigos teisių valdymui, asmens duomenų naikinimui, šifravimo priemonių naudojimui ir pakeitimų valdymui.

Pagrindinės rekomendacijos:

1. Užtikrinti privilegijuotųjų prieigos teisių valdymo kontrolę.

Rekomenduojame atlikti reguliarų privilegijuotųjų prieigos teisių auditą, siekiant užtikrinti, kad prieiga prie asmens duomenų būtų suteikiama tik tiems darbuotojams, kuriems tai būtina pagal jų funkcijas. Taip pat siūlome įdiegti automatizuotas priemones, leidžiančias stebėti ir analizuoti veiksmus, atliekamus su šia prieiga, užtikrinant BDAR atitiktį.

2. Sukurti ir įgyvendinti efektyvius asmens duomenų naikinimo procesus.

Atsižvelgę į atliktos stebėsenos rezultatus, rekomenduojame sukurti aiškias ir dokumentuotas asmens duomenų naikinimo procedūras, kurios užtikrintų, kad pasibaigus nustatytam saugojimo terminui nereikalingi ar pasenę duomenys būtų sunaikinti saugiai ir laiku. Tai svarbu siekiant sumažinti perteklinių duomenų laikymo riziką ir atitikti BDAR reikalavimus.

3. Naudoti pažangias šifravimo priemones duomenų saugumui užtikrinti.

Rekomenduojame diegti pažangius šifravimo sprendimus, kurie apsaugotų asmens duomenis tiek jų perdavimo, tiek saugojimo metu. Šifravimo priemonių naudojimas turėtų būti periodiškai tikrinamas, siekiant užtikrinti jų efektyvumą ir suderinamumą su BDAR nuostatomis.

4. Tobulinti pakeitimų valdymo procesus.

Rekomenduojame įdiegti griežtas pakeitimų valdymo procedūras, kurios apimtų naujų sistemų, programinės įrangos ar duomenų apdorojimo metodų diegimą. Visi pakeitimai turėtų būti iš anksto įvertinti, dokumentuoti ir patvirtinti, kad būtų užtikrintas duomenų saugumas ir BDAR atitiktis.

5. Reguliariai peržiūrėti ir atnaujinti duomenų apsaugos politiką.

Atsižvelgę į atliktos stebėsenos išvadas, siūlome reguliariai peržiūrėti organizacijos duomenų apsaugos politiką, atnaujinant ją pagal naujausius teisės aktų reikalavimus ir geriausias praktikas. Į politiką turėtų būti įtrauktos visos pagrindinės sritys, įskaitant prieigos teisių valdymą, šifravimo priemonių naudojimą, duomenų naikinimą ir pakeitimų valdymą.