Techninės ir organizacinės saugumo priemonės: ką apie tai sako ESTT?

DAP mokymai | Advokato padėjėja Renata Vasiliauskienė

Planas:

1. Techninės ir organizacinės saugumo priemonės: ką apie tai sako BDAR, institucijų gairės ir kiti teisės šaltiniai?

2. Aktualių ESTT bylų apžvalga

3. Išvados

Techninės ir organizacinės saugumo priemonės:

Ką apie saugumą (ne)pasako BDAR ir kiti teisės šaltiniai?

BDAR 32 straipsnis: stiprybė ar silpnybė?

- Pradiniame BDAR 32 str. variante EU Komisija turėjo duoti minimalius saugumo priemonių sąrašus leisdama deleguotuosius aktus.

- Galiausiai sutarta dėl tarpinio 32 str. varianto – pareiga užtikrinti saugumą turi kilti ne iš sąrašų, o iš rizikos vertinimo. Detalūs IT saugumo priemonių sąrašai palikti „*soft law*“ ir tarpusavio reguliavimui (sertifikatų, elgesio kodeksų pagrindu). Komisija neturi galios leisti techninių standartų.

Aktualios BDAR nuostatos: 32 str.

32 straipsnis

Duomenų tvarkymo saugumas

1. Atsižvelgdamas į techninių galimybių išsivystymo lygį, įgyvendinimo sąnaudas bei duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus, taip pat duomenų tvarkymo keliamus įvairios tikimybės ir rimtumo pavojus fizinių asmenų teisėms ir laisvėms, duomenų valdytojas ir duomenų tvarkytojas įgyvendina tinkamas technines ir organizacines priemones, kad būtų užtikrintas pavojų atitinkančio lygio saugumas, įskaitant, *inter alia*, jei reikia:

a) pseudonimų suteikimą asmens duomenims ir jų šifravimą;

b) gebėjimą užtikrinti nuolatinį duomenų tvarkymo sistemų ir paslaugų konfidencialumą, vientisumą, prieinamumą ir atsparumą;

c) gebėjimą laiku atkurti sąlygas ir galimybes naudotis asmens duomenimis fizinio ar techninio incidento atveju;

d) reguliarų techninių ir organizacinių priemonių, kuriomis užtikrinamas duomenų tvarkymo saugumas, tikrinimo, vertinimo ir veiksmingumo vertinimo procesą.

2. Nustatant tinkamo lygio saugumą visų pirma atsižvelgiama į pavojus, kurie kyla dėl duomenų tvarkymo, visų pirma dėl netyčinio arba neteisėto persiųstų, saugomų ar kitaip tvarkomų duomenų sunaikinimo, praradimo, pakeitimo, atskleidimo be leidimo ar neteisėtos prieigos prie jų.

3. <...>.

4. <...>.

Aktualios BDAR nuostatos: 24 str.

24 straipsnis

Duomenų valdytojo atsakomybė

1. Atsižvelgdamas į duomenų tvarkymo pobūdį, aprėptį, kontekstą bei tikslus, taip pat į įvairios tikimybės ir rimtumo pavojus fizinių asmenų teisėms ir laisvėms, duomenų valdytojas įgyvendina tinkamas technines ir organizacines priemones, kad užtikrintų ir galėtų įrodyti, kad duomenys tvarkomi laikantis šio reglamento. Tos priemonės prireikus peržiūrimos ir atnaujinamos.

?????

- Adresatai skiriasi: 24 str. tik valdytojas, 32 str. ir valdytojas ir tvarkytojas. Kodėl? Kokia intencija?
- ESTT paprastai šiuos du straipsnius analizuoja kartu: 24 str. - atskaitingumas ir įrodinėjimo našta, o 32 str. - kriterijai, pagal kurį vertinamos saugumo priemonės.
- Kadangi valdytojas turi įrodyti priemonių tinkamumą, logiška būtų manyti, kad dokumentai: rizikos vertinimas, politikos, testavimas, žurnalai, mokymai, privalomi tik jam. Ar tikrai? Kaip vertinti tuos atvejus, kai baudos skiriamos tik tvarkytojui?

Aktualios BDAR nuostatos: konstatuojamosios dalys

- 15. <...> siekiant, kad būtų išvengta rimtos teisės aktų apėjimo grėsmės, fizinių asmenų apsauga turėtų būti neutrali technologijų atžvilgiu ir turėtų nepriklausyti nuo taikomų metodų. <...>.

- 83. <...> duomenų valdytojas arba duomenų tvarkytojas turėtų įvertinti su duomenų tvarkymu susijusius pavojus ir įgyvendinti jo mažinimo priemones <...>. Šiomis priemonėmis turėtų būti užtikrintas tinkamo lygio saugumas,<...>.

- 81. <...> duomenų valdytojas, patikėdamas duomenų tvarkytojui tvarkymo veiklą, turėtų pasitelkti tik tokius duomenų tvarkytojus, kurie suteikia pakankamų garantijų, susijusių visų pirma su ekspertinėmis žiniomis, patikimumu ir ištekliais, kad būtų įgyvendintos techninės ir organizacinės priemonės, kurios atitiks šio reglamento reikalavimus, įskaitant dėl tvarkymo saugumo.

Institucijų išaiškinimai dėl 32 straipsnio:

- Lietuvos VDAI – 2024 m. Gairės – Paremtos ISO 27001 standartu, taip pat 2019 m. SolPriPra leidiniuose yra išvardinta 10 minimalių priemonių; atskiros gairės sveikatos priežiūros institucijoms.

- Jungtinės Karalystės ICO – 2023 m. Gairės – Nustato keturis tikslus valdytojui: saugumo rizikos valdymas, apsauga nuo kibernetinių atakų, saugumo įvykių aptikimas ir incidentų poveikio mažinimas.

- Prancūzijos CNIL – 2024 m. Gairės – Nustato du saugumo lygius: bazinio lygio kibernetinės higienos reikalavimus ir aukštesnio lygio. Jei saugumo pažeidimas įvyksta dėl bazinių techninių atsargumo priemonių trūkumo, CNIL skirs baudą.

- Airijos duomenų apsaugos institucija - 2020 m. Gairės - Nei BDAR, nei vietos įstatymas nenustato konkrečių saugumo priemonių, tad taikoma bendra saugumo pareiga pagal 25 ir 32 straipsnius kiekvienam duomenų valdytojui ir tvarkytojui, nepriklausomai nuo jo dydžio. Darbuotojai privalo žinoti saugumo priemones.

Kiti teisės šaltiniai: BDAR komentaras*

- Siekiant apsisaugoti nuo incidentų, BDAR nustato bendrinę saugumo pareigą abiem: valdytojams ir tvarkytojams (631 psl.).
- Nors abu: valdytojai ir tvarkytojai privalo laikytis duomenų saugumo reikalavimų, valdytojų atsakomybė yra labiau išreikšta. Valdytojams taikomas atskaitomybės principas įtvirtintas 5(2) straipsnyje, kuris reiškia pareigą pademonstruoti, kad valdytojas užtikrina tinkamą saugumą. (636 psl.)
- Tais atvejais, kai duomenų tvarkytojas yra pasaulinis paslaugų teikėjas ir realiai nustato saugumo priemones, valdytojas yra tas, kuris galutinai jas patvirtina, kaip tinkamas.
- Pirmu žingsniu valdytojai ir tvarkytojai privalo identifikuoti ir įsivertinti konkrečias rizikas, <…>. Antru žingsniu, jie privalo nustatyti ir įgyvendinti saugumo priemones, kaip (riziką) mažinantį atsaką.“ (635 psl.).

**The EU General Data Protection Regulation (GDPR): A Commentary, Oxford University Press, 2020.*

Kiti teisės šaltiniai: BDAR komentaras

- Žodis „tinkamos“ 32 straipsnyje naudojamas tris kartus <...>. Tai indikuoja, kad valdytojai ir tvarkytojai privalo identifikuoti konkrečias-situacines rizikas, įvertinti jų galimą poveikį ir įgyvendinti priemones sumažinančias (bent tas) rizikas, kurios yra labiausiai tikėtinos ir tas, kurios sukeltų pačią didžiausią žalą. <...>.
- Žodžio „tinkamos“ pasirinkimas turėtų būti vertinamas kaip išreiškiantis proporcingumo principo svarbą saugumo užtikrinimo procese (635 psl.)
- Nors 32 straipsnyje nurodytos priemonės nėra privalomos, joms parodoma aiški pirmenybė <...> (636psl.).
- 32 straipsnis nustato tik pareigą taikyti priemones, o ne pareigą pasiekti rezultatą. Tai reiškia, kad įvykus duomenų apsaugos incidentui, nepaisant tinkamų saugumo priemonių įgyvendinimo, gali nebūti BDAR pažeidimo. (637 psl.)

Neatsakyti klausimai:

1. Ką reikia padaryti, kad negautum baudos, juk šimtaprocentinis saugumas internete neegzistuoja?
2. Tvarkytojas, turintis šimtus ar tūkstančius klientų, dažniausiai nežino, kokie duomenys pas jį saugojami, kaip jam įvertinti riziką ir parinkti „tinkamas“ priemones?
3. Kokios tvarkytojo atsakomybės ribos incidento atveju?
4. Kaip 32 str. kriterijai taikomi praktikoje, jeigu jie vienas kitam prieštarauja? Pvz. įgyvendinimo sąnaudos *v.* pavojus teisėms ir laisvėms?
5. Kas vertina rizikos vertinimo kokybę?



ESTT:

Bylos, kuriose nagrinėtas saugumo priemonių klausimas?

C-340/21 Natsionalna agentsia za prihodite, 2023-12-14

Fabula: Bulgarijos mokesčių administratoriaus duomenų nutekėjimas po programišių atakos.

Klausimai:

- Ar fakto, kad įvyko pažeidimas (kurį sukėlė trečioji šalis), pakanka, kad būtų padaryta išvada, jog duomenų valdytojo įgyvendintos priemonės nebuvo „tinkamos“?
- Kaip teisingai įvertinti priemonių „tinkamumą“?
- Kas turi įrodinėjimo naštą?
- Ar valdytojas gali būti neatsakingas už įsilaužimo atvejus?

ESTT:

- *„BDAR 32 straipsnio 1 ir 2 dalyse esančios nuorodos į „riziką atitinkantį saugumo lygį“ ir „tinkamą saugumo lygį“ rodo, kad šiuo reglamentu sukuriama rizikos valdymo sistema ir juo jokiu būdu nesiekiama visiškai panaikinti saugumo pažeidimų rizikos.“*
- *„priemonių tinkamumas turi būti vertinamas konkrečiu atveju – atsižvelgiant į tai, ar duomenų valdytojas jas įgyvendino paisydamas tuose straipsniuose nurodytų įvairių kriterijų, bei į duomenų apsaugos poreikius, konkrečiai būdingus atitinkamam duomenų tvarkymui, ir iš pastarojo kylančią riziką.“*

C-340/21 Natsionalna agentsia za prihodite, 2023-12-14

ESTT:

- *„vien neteisėto duomenų atskleidimo <...> fakto nepakanka išvadai, jog valdytojo patvirtintos priemonės nebuvo tinkamos,<...>, net nesuteikiant valdytojui galimybės pateikti priešingų įrodymų.“*
- *„ES teisėkūra išreiškė ketinimą „sumažinti“ (sušvelninti) duomenų saugumo pažeidimų riziką, neteigdama, kad būtų įmanoma ją visiškai panaikinti.“*
- *„<...> organizacinių ir techninių priemonių tinkamumas turi būti vertinamas dviem etapais. Pirma, būtina nustatyti <...> riziką ir galimas jos pasekmes <...>, atsižvelgiant į tikimybę ir jos sunkumą. Antra, išsiaiškinti, ar <...> įgyvendintos priemonės atitinka šią riziką, atsižvelgiant į [32 str. kriterijus].“*
- *„<...> valdytojas turi tam tikrą diskreciją nustatyti tinkamas technines ir organizacines priemones, <...>. Vis dėlto nacionalinis teismas <...> privalo atlikti šių priemonių esmės (turinio) nagrinėjimą, atsižvelgdamas į visus tame straipsnyje nurodytus kriterijus, konkrečias bylos aplinkybes ir teismui šiuo atžvilgiu prieinamus įrodymus.“*
- *„<...> valdytojui tenka atsakomybė įrodyti, kad duomenys buvo tvarkyti tokiu būdu, jog būtų užtikrintas jų saugumas, kaip apibrėžta reglamento 5 (1) (f) ir 32 straipsniuose.“*
- *„Valdytojas negali būti atleistas nuo prievolės atlyginti duomenų subjekto patirtą žalą <...> vien dėl to, kad ši žala atsirado dėl „trečiojo asmens“ atlikto neteisėtų veiksmų. <...> valdytojas turi įrodyti, kad yra visiškai nekaltas dėl įvykio.*

C-687/21 MediaMarktSaturn, 2024-01-25

Fabula: Darbuotojai per klaidą perdavė dokumentą su asmens duomenimis kitam klientui.

Klausimas: Ar fakto, kad valdytojo darbuotojai per klaidą pateikė trečiajam neįgaliotam asmeniui asmens duomenis, savaime pakanka, kad būtų laikoma, jog duomenų valdytojo įgyvendintos priemonės nebuvo „tinkamos“, kaip tai suprantama pagal 24 ir 32 straipsnius?

ESTT:

- *„BDAR 24 straipsnyje įtvirtinta bendra valdytojo prievolė įgyvendinti tinkamas technines ir organizacines priemones, siekiant užtikrinti ir sugebėti įrodyti, kad duomenys tvarkomi laikantis šio reglamento.“*
- *„Savo ruožtu BDAR 32 straipsnyje nustatytos duomenų valdytojo ir galimo duomenų tvarkytojo prievolės, susijusios su to duomenų tvarkymo saugumu.“*

C-687/21 MediaMarktSaturn, 2024-01-25

ESTT:

- *„Tokį pažodinį aiškinimą patvirtina BDAR 24 ir 32 straipsnių skaitymas kartu su šio reglamento 5 straipsnio 2 dalimi ir 82 straipsniu, atsižvelgiant į jo 74, 76 ir 83 konstatuojamąsias dalis, iš kurių visų pirma matyti, kad duomenų valdytojas privalo sumažinti (sušvelninti) asmens duomenų saugumo pažeidimų riziką, o ne užkirsti kelią absoliučiai visiems tokių duomenų saugumo pažeidimams.“*
- *„Vieno [pažeidimo] fakto <...> nepakanka, kad būtų pripažinta, jog valdytojo įgyvendintos techninės ir organizacinės priemonės nebuvo „tinkamos“*
- *„Pagal reglamento 82 straipsnį pareikštame ieškinyje dėl žalos atlyginimo valdytojui tenka našta įrodyti, kad jo įgyvendintos saugumo priemonės yra tinkamos pagal šio reglamento 32 straipsnį.“*

Kitaip tariant, valdytojas turi teisę gintis ir įrodinėti, kad jo priemonės buvo tinkamos, o įvykis buvo ne sisteminė klaida, o nenuspėjamas žmogiškasis faktorius.

C-683/21 *Nacionalinis visuomenės sveikatos centras*, 2023-12-05

Fabula: VDAI bauda NVSC už BDAR 5, 13, 24, 32 ir 35 straipsnių pažeidimus, susijusius su programėle, kurią sukūrė tvarkytojas.

Klausimas: Ar netinkami tvarkytojo veiksmai automatiškai užtraukia teisinę atsakomybę valdytojui?

ESTT: *„Reikia prisiminti, kad <...> duomenų tvarkytojas – tai „fizinis arba juridinis asmuo, valdžios institucija, agentūra ar kita įstaiga, kuri duomenų valdytojo vardu tvarko asmens duomenis“*

„Kadangi, <...>, duomenų valdytojas yra atsakingas ne tik už bet kokį asmens duomenų tvarkymą, kurį atlieka jis pats, bet ir už tokį duomenų tvarkymą, kuris atliekamas jo vardu, šiam duomenų valdytojui <...> gali būti skiriama administracinė bauda tokioje situacijoje, kai asmens duomenys tvarkomi neteisėtai ir kai minėtą duomenų tvarkymą jo vardu atliko <...> jo pasitelktas duomenų tvarkytojas.

ESTT sprendimų apibendrinimas:

- ESTT laiko, kad techninių ir organizacinių saugumo priemonių pareigą turi ir duomenų valdytojas, ir duomenų tvarkytojas.
- Tačiau atsakomybė ir pareiga įrodyti, kad priemonės buvo tinkamos, tenka valdytojui.
- Tinkamas saugumo lygis vertinamas dviem etapais: pagal riziką, 32 str. kriterijus ir konkrečias aplinkybes.
- Saugumas nėra absoliutus, todėl įvykęs duomenų saugumo pažeidimas nereiškia, kad priemonės buvo netinkamos.
- Teismas iki šiol nėra priėmęs sprendimo, kuriame atskirai vertintų tvarkytojo atsakomybę už BDAR 32 straipsnio pažeidimą.
- Neteisėto įsilaužimo atveju, valdytojui reikės mokėti kompensaciją, nebent įrodys, kad jis jokiu būdu už incidentą nėra atsakingas.

Ačiū už dėmesį!

Lietuvos Advokatūra

Polocko g. 43C, LT-01205, Lithuania
+370 262 4546
www.advokatura.lt

Renata Vasiliauskienė

Advokato padėjėja
+370 616 31650
Renata.vasiliauskiene@cobalt.legal