TEISINGUMO TEISMO (trečioji kolegija) SPRENDIMAS

2023 m. gruodžio 14 d.*

„Prašymas priimti prejudicinį sprendimą – Fizinių asmenų apsauga tvarkant asmens duomenis – Reglamentas (ES) 2016/679 – 5 straipsnis – Duomenų tvarkymo principai – 24 straipsnis – Duomenų valdytojo atsakomybė – 32 straipsnis – Priemonės, įgyvendinamos duomenų tvarkymo saugumui užtikrinti – Tokių priemonių tinkamumo vertinimas – Teisminės kontrolės apimtis – Įrodymų rinkimas – 82 straipsnis – Teisė į kompensaciją ir atsakomybė – Galimas duomenų valdytojo atleidimas nuo atsakomybės, kai pažeidimą padaro tretieji asmenys – Prašymas atlyginti neturtinę žalą, grindžiamas nuogąstavimu dėl potencialaus piktnaudžiavimo asmens duomenimis“

Byloje C-340/21

dėl *Varhoven administrativen sad* (Aukščiausiasis administracinis teismas, Bulgarija) 2021 m. gegužės 14 d. nutartimi, kurią Teisingumo Teismas gavo 2021 m. birželio 2 d., pagal SESV 267 straipsnį pateikto prašymo priimti prejudicinį sprendimą byloje

**VB**

prieš

**Natsionalna agentsia za prihodite**

TEISINGUMO TEISMAS (trečioji kolegija),

kurį sudaro kolegijos pirmininkė K. Jürimäe, teisėjai N. Piçarra, M. Safjan, N. Jääskinen (pranešėjas) ir M. Gavalec,

generalinis advokatas G. Pitruzella,

kancleris A. Calot Escobar,

atsižvelgęs į rašytinę proceso dalį,

išnagrinėjęs pastabas, pateiktas:

– *Natsionalna agentsia za prihodite*, atstovaujamos R. Spetsov,

– Bulgarijos vyriausybės, atstovaujamos M. Georgieva ir L. Zaharieva,

* Proceso kalba: bulgarų.

– Čekijos vyriausybės, atstovaujamos O. Serdula, M. Smolek ir J. Vláčil,

– Airijos, atstovaujamos *Chief State Solicitor* M. Browne, taip pat A. Joyce, J. Quaney ir M. Tierney, padedamų BL D. Fennelly,

– Italijos vyriausybės, atstovaujamos G. Palmieri, padedamos *avvocato dello Stato* E. De Bonis,

– Portugalijos vyriausybės, atstovaujamos P. Barros da Costa, A. Pimenta, J. Ramos ir C. Vieira Guerra,

– Europos Komisijos, atstovaujamos A. Bouchagiar, H. Kranenborg ir N. Nikolova,

susipažinęs su 2023 m. balandžio 27 d. posėdyje pateikta generalinio advokato išvada,

priima šį

**Sprendimą**

1 Prašymas priimti prejudicinį sprendimą pateiktas dėl 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) (OL L 119, 2016, p. 1; toliau – BDAR) 5 straipsnio 2 dalies, 24, 32 straipsnių ir 82 straipsnio 1–3 dalių išaiškinimo.

2 Šis prašymas pateiktas nagrinėjant fizinio asmens VB ir *Natsionalna agentsia za prihodite* (Nacionalinė pajamų agentūra, Bulgarija, toliau – NAP) ginčą dėl neturtinės žalos atlyginimo; šią žalą fizinis asmuo teigia patyręs dėl tariamo šios valstybės institucijos įstatyminių pareigų, jai tenkančių kaip asmens duomenų valdytojai, nevykdymo.

## Teisinis pagrindas

3 BDAR 4, 10, 11, 74, 76, 83, 85 ir 146 konstatuojamosios dalys suformuluotos taip:

„(4) <…> Šiuo reglamentu paisoma visų [Europos Sąjungos pagrindinių teisių chartijoje pripažintų ir Sutartyse įtvirtintų pagrindinių teisių ir laisvių bei principų, visų pirma teisės į privatų ir šeimos gyvenimą, būsto neliečiamybę ir komunikacijos slaptumą, teisės į asmens duomenų apsaugą, <…> teisės į veiksmingą teisinę gynybą ir teisingą bylos nagrinėjimą <…>;

<…>

(10) siekiant užtikrinti vienodo ir aukšto lygio fizinių asmenų apsaugą ir pašalinti asmens duomenų judėjimo [Europos] Sąjungoje kliūtis, visose valstybėse narėse turėtų būti užtikrinama lygiavertė asmenų teisių ir laisvių apsauga tvarkant tokius duomenis. Visoje Sąjungoje turėtų būti užtikrintas nuoseklus ir vienodas taisyklių, kuriomis reglamentuojama fizinių asmenų pagrindinių teisių ir laisvių apsauga tvarkant asmens duomenis, taikymas. <…>

(11) siekiant veiksmingos asmens duomenų apsaugos visoje Sąjungoje, reikia <…> sustiprinti ir išsamiai nustatyti duomenų subjektų teises ir asmens duomenis tvarkančių ir jų tvarkymą nustatančių subjektų prievoles, <…>

<…>

(74) turėtų būti nustatyta duomenų valdytojo atsakomybė už bet kokį duomenų valdytojo arba jo vardu vykdomą asmens duomenų tvarkymą. Duomenų valdytojas visų pirma turėtų būti įpareigotas įgyvendinti tinkamas ir veiksmingas priemones ir galėti įrodyti, kad duomenų tvarkymo veikla atitinka šį reglamentą, įskaitant priemonių veiksmingumą. Tomis priemonėmis turėtų būti atsižvelgta į duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus, taip pat į pavojų fizinių asmenų teisėms ir laisvėms;

<…>

(76) pavojaus duomenų subjekto teisėms ir laisvėms tikimybė ir rimtumas turėtų būti nustatomi atsižvelgiant į duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus. Pavojus turėtų būti vertinamas remiantis objektyviu įvertinimu, kurio metu nustatoma, ar duomenų tvarkymo operacijos yra susijusios su pavojumi arba dideliu pavojumi;

<…>

(83) siekiant užtikrinti saugumą ir užkirsti kelią šį reglamentą pažeidžiančiam duomenų tvarkymui, duomenų valdytojas arba duomenų tvarkytojas turėtų įvertinti su duomenų tvarkymu susijusius pavojus ir įgyvendinti jo mažinimo priemones, pavyzdžiui, šifravimą. Šiomis priemonėmis turėtų būti užtikrintas tinkamo lygio saugumas, įskaitant konfidencialumą, atsižvelgiant į techninių galimybių išsivystymo lygį ir įgyvendinimo sąnaudas pavojų ir saugotinų asmens duomenų pobūdžio atžvilgiu. Vertinant pavojų duomenų saugumui, reikėtų atsižvelgti į pavojus, kurie kyla tvarkant asmens duomenis, pavyzdžiui, į tai, kad persiųsti, saugomi ar kitaip tvarkomi duomenys gali būti netyčia arba neteisėtai sunaikinti, prarasti, pakeisti, be leidimo atskleisti arba be leidimo prie jų gauta prieiga, ir dėl to visų pirma gali būti padarytas kūno sužalojimas, materialinė ar nematerialinė žala;

<…>

(85) dėl asmens duomenų saugumo pažeidimo, jei dėl jo laiku nesiimama tinkamų priemonių, fiziniai asmenys gali patirti kūno sužalojimą [fizinę], materialinę ar nematerialinę žalą, pavyzdžiui, prarasti savo asmens duomenų kontrolę, patirti teisių apribojimą, diskriminaciją, gali būti pavogta ar suklastota jo asmens tapatybė, jam padaryta finansinių nuostolių, neleistinai panaikinti pseudonimai, gali būti pakenkta jo reputacijai, prarastas asmens duomenų, kurie saugomi profesine paslaptimi, konfidencialumas arba padaryta kita ekonominė ar socialinė žala atitinkamam fiziniam asmeniui. Todėl, vos sužinojęs, kad padarytas asmens duomenų saugumo pažeidimas, duomenų valdytojas turėtų pranešti kompetentingai priežiūros institucijai nepagrįstai nedelsdamas <…>

<…>

(146) bet kokią žalą, kurią asmuo gali patirti dėl duomenų tvarkymo pažeidžiant šį reglamentą, turėtų atlyginti duomenų valdytojas arba duomenų tvarkytojas. Duomenų valdytojas arba duomenų tvarkytojas turėtų būti atleisti nuo atsakomybės, jeigu jie įrodo, kad jokiu būdu nėra atsakingi už žalą. Žalos sąvoka turėtų būti aiškinama plačiai, atsižvelgiant į Teisingumo Teismo praktiką, taip, kad būtų visapusiškai atspindėti šio reglamento tikslai. Tai nedaro poveikio jokiems reikalavimams dėl žalos atlyginimo, kurie pareiškiami dėl kitų Sąjungos ar valstybės narės teisės aktų nuostatų pažeidimo. Duomenų tvarkymas pažeidžiant šį reglamentą taip pat apima duomenų tvarkymą pažeidžiant deleguotuosius ir įgyvendinimo aktus, priimtus pagal šį reglamentą, ir šį reglamentą tikslinančias valstybėje narės teisėje nustatytas taisykles. Duomenų subjektai už patirtą žalą turi gauti visą ir veiksmingą kompensaciją. <…>“

4 Šios direktyvos 4 straipsnyje „Apibrėžtys“ nustatyta:

„Šiame reglamente:

1) asmens duomenys – bet kokia informacija apie fizinį asmenį, kurio tapatybė yra nustatyta arba gali būti nustatyta (duomenų subjektas); <…>

2) duomenų tvarkymas – bet kokia automatizuotomis arba neautomatizuotomis priemonėmis su asmens duomenimis ar asmens duomenų rinkiniais atliekama operacija ar operacijų seka <…>;

<…>

7) duomenų valdytojas – fizinis arba juridinis asmuo, valdžios institucija, agentūra ar kita įstaiga, kuris vienas ar drauge su kitais nustato duomenų tvarkymo tikslus ir priemones; <…>

<…>

10) trečioji šalis [trečiasis asmuo] – fizinis arba juridinis asmuo, valdžios institucija, agentūra ar kita įstaiga, kuri nėra duomenų subjektas, duomenų valdytojas, duomenų tvarkytojas, arba asmenys, kuriems tiesioginiu duomenų valdytojo ar duomenų tvarkytojo įgaliojimu leidžiama tvarkyti asmens duomenis;

<…>

12) asmens duomenų saugumo pažeidimas – saugumo pažeidimas, dėl kurio netyčia arba neteisėtai sunaikinami, prarandami, pakeičiami, be leidimo atskleidžiami persiųsti, saugomi arba kitaip tvarkomi asmens duomenys arba prie jų be leidimo gaunama prieiga;

<…>“

5 Minėto reglamento 5 straipsnyje „Su asmens duomenų tvarkymu susiję principai“ numatyta:

„1. Asmens duomenys turi būti:

a) duomenų subjekto atžvilgiu tvarkomi teisėtu, sąžiningu ir skaidriu būdu (teisėtumo, sąžiningumo ir skaidrumo principas);

<…>

f) 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).

2. Duomenų valdytojas yra atsakingas už tai, kad būtų laikomasi 1 dalies, ir turi sugebėti įrodyti, kad jos laikomasi (atskaitomybės principas).“

6 Šio reglamento 24 straipsnyje „Duomenų valdytojo atsakomybė“ nustatyta:

„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.

2. Kai tai proporcinga duomenų tvarkymo veiklos atžvilgiu, 1 dalyje nurodytos priemonės apima duomenų valdytojo įgyvendinamą atitinkamą duomenų apsaugos politiką.

3. Tuo, kad laikomasi patvirtintų elgesio kodeksų, kaip nurodyta 40 straipsnyje, arba patvirtintų sertifikavimo mechanizmų, kaip nurodyta 42 straipsnyje, gali būti remiamasi kaip vienu iš elementų, kuriuo siekiama įrodyti, kad duomenų valdytojas vykdo prievoles.“

7 BDAR 32 straipsnyje „Tvarkymo teisėtumas“ nurodyta:

„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. Tuo, kad laikomasi patvirtinto elgesio kodekso, kaip nurodyta 40 straipsnyje, arba patvirtinto sertifikavimo mechanizmo, kaip nurodyta 42 straipsnyje, gali būti remiamasi kaip vienu iš elementų, kuriuo siekiama įrodyti, kad laikomasi šio straipsnio 1 dalyje nustatytų reikalavimų.

<…>“

8 Šio reglamento 79 straipsnio „Teisė imtis veiksmingų teisminių teisių gynimo priemonių prieš duomenų valdytoją arba duomenų tvarkytoją“ 1 dalyje nurodyta:

„Nedarant poveikio galimybei imtis bet kokių galimų administracinių arba neteisminių teisių gynimo priemonių, įskaitant teisę pateikti skundą priežiūros institucijai pagal 77 straipsnį, kiekvienas duomenų subjektas turi teisę imtis veiksmingų teisminių teisių gynimo priemonių, jeigu mano, kad šiuo reglamentu nustatytos jo teisės buvo pažeistos, nes jo asmens duomenys buvo tvarkomi pažeidžiant šį reglamentą.“

9 Minėto reglamento 82 straipsnio „Teisė į kompensaciją ir atsakomybė“ 1–3 dalyse numatyta:

„1. Bet kuris asmuo, patyręs materialinę ar nematerialinę žalą dėl šio reglamento pažeidimo, turi teisę iš duomenų valdytojo arba duomenų tvarkytojo gauti kompensaciją už patirtą žalą.

2. Tvarkant duomenis dalyvaujantis duomenų valdytojas atsako už žalą, padarytą dėl vykdyto duomenų tvarkymo pažeidžiant šį reglamentą. <…>

3. Duomenų valdytojas arba duomenų tvarkytojas atleidžiami nuo atsakomybės pagal 2 dalį, jeigu jis įrodo, kad jokiu būdu nėra atsakingas už įvykį, dėl kurio patirta žala.“

## Pagrindinė byla ir prejudiciniai klausimai

10 NAP yra Bulgarijos finansų ministrui pavaldi įstaiga. Vykdydama užduotis, prie kurių, be kita ko, priskiriamas valstybės reikalavimų nustatymas, užtikrinimas ir išieškojimas, ji atlieka asmens duomenų valdytojo funkcijas, kaip tai suprantama pagal BDAR 4 straipsnio 7 punktą.

11 2019 m. liepos 15 d. žiniasklaida pranešė, kad buvo be leidimo prisijungta prie NPA informacinės sistemos ir po šio kibernetinio išpuolio internete paskelbti toje sistemoje saugoti asmens duomenys.

12 Dėl šio incidento nukentėjo daugiau nei šeši milijonai fizinių asmenų (Bulgarijos ir kitų šalių piliečių). Keli šimtai jų, įskaitant pareiškėją pagrindinėje byloje, pateikė NAP ieškinius dėl neturtinės žalos, kilusios dėl jų asmens duomenų atskleidimo, atlyginimo.

13 Šiomis aplinkybėmis pareiškėja pagrindinėje byloje kreipėsi į *Administrativen sad Sofia-grad* (Sofijos miesto administracinis teismas), pagal BDAR 82 straipsnį ir Bulgarijos teisės nuostatas reikalaudama priteisti jai iš NAP 1 000 Bulgarijos levų (BGN) (apie 510 eurų) žalos atlyginimą. Grįsdama šį reikalavimą, ji tvirtino, kad dėl asmens duomenų saugumo pažeidimo, kaip tai suprantama pagal BDAR 4 straipsnio 12 punktą, konkrečiai – dėl saugumo pažeidimo, kurį lėmė NAP, be kita ko, pagal šio reglamento 5 straipsnio 1 dalies f punktą, 24 ir 32 straipsnius tenkančių pareigų nevykdymas, patyrė neturtinę žalą. Jos neturtinė žala pasireiškė nuogąstavimais, kad be jos sutikimo paskelbtais asmens duomenimis ateityje gali būti piktnaudžiaujama arba kad ji bus šantažuojama, užpulta arba pagrobta.

14 Atsikirsdama NAP pirmiausia teigia, kad pareiškėja pagrindinėje byloje jos neprašė informacijos, kokie konkretūs duomenys buvo atskleisti. Toliau NAP pateikė dokumentus, įrodančius, kad ėmėsi visų būtinų priemonių siekdama iš anksto užkirsti kelią jos informacinėje sistemoje saugomų asmens duomenų saugumo pažeidimui, o paskui – apriboti šio pažeidimo poveikį ir

nuraminti piliečius. Be to, ji teigė, kad nėra priežastinio ryšio tarp tariamos neturtinės žalos ir minėto pažeidimo. Galiausiai ji nurodė, kad pati nukentėjo nuo trečiųjų asmenų, kurie nėra jos darbuotojai, tyčinio išpuolio, todėl negali būti laikoma atsakinga už jo sukeltas žalingas pasekmes.

15 2020 m. lapkričio 27 d. sprendimu *Administrativen sad Sofia-grad* (Sofijos miesto administracinis teismas) atmetė pareiškėjos pagrindinėje byloje skundą. Jis laikėsi nuomonės, kad neteisėtą prieigą prie NAP duomenų bazės lėmė trečiųjų asmenų įvykdytas įsilaužimas, o pareiškėja pagrindinėje byloje neįrodė, kad NAP neįvykdė pareigų dėl saugumo priemonių priėmimo. Be to, jis manė, kad pareiškėja nepatyrė neturtinės žalos, suteikiančios teisę į kompensaciją.

16 Pareiškėja pagrindinėje byloje kasacine tvarka apskundė minėtą sprendimą *Varhoven administrativen sad* (Aukščiausiasis administracinis teismas, Bulgarija), t. y. prašymą priimti prejudicinį sprendimą šioje byloje pateikusiam teismui. Grįsdama kasacinį skundą ji tvirtino, kad paskirstydamas įrodinėjimo naštą dėl NAP taikytų saugumo priemonių pirmosios instancijos teismas padarė teisės klaidą ir kad NAP neįrodė įvykdžiusi atitinkamas pareigas. Be to, pareiškėja pagrindinėje byloje teigė, kad nuogąstavimas dėl galimo piktnaudžiavimo asmens duomenimis ateityje yra faktinė, o ne hipotetinė neturtinė žala. Atsikirsdama NAP ginčijo visus nurodytus argumentus.

17 Prašymą priimti prejudicinį sprendimą pateikęs teismas pirmiausia nurodė, kad asmens duomenų saugumo pažeidimo konstatavimas pats savaime galėtų leisti daryti išvadą, kad duomenų valdytojo įgyvendintos priemonės nebuvo „tinkamos“, kaip tai suprantama pagal BDAR 24 ir 32 straipsnius.

18 Vis dėlto, jeigu minėto konstatavimo nepakaktų tokiai išvadai padaryti, jam kilo klausimas, pirma, dėl kontrolės, kurią nacionaliniai teismai turi atlikti siekdami įvertinti tokių priemonių tinkamumą, apimties ir, antra, dėl tokiu atveju taikytinų įrodymų rinkimo taisyklių, kiek tai susiję tiek su įrodinėjimo pareiga, tiek su įrodymais, ypač kai teismams pateikiami BDAR 82 straipsniu grindžiami ieškiniai dėl žalos atlyginimo.

19 Toliau nacionalinis teismas norėtų sužinoti, ar tai, kad asmens duomenų apsaugos pažeidimą lėmė trečiųjų asmenų veika, šiuo atveju – kibernetinis išpuolis, atsižvelgiant į minėto reglamento 82 straipsnio 3 dalį, yra veiksnys, bet kuriuo atveju atleidžiantis šių duomenų valdytoją nuo atsakomybės už duomenų subjektui padarytą žalą.

20 Galiausiai šiam teismui kilo klausimas, ar asmens nuogąstavimas, kad ateityje (nagrinėjamu atveju – kibernetiniams nusikaltėliams neteisėtai gavus prieigą prie jų ir juos atskleidus) gali būti piktnaudžiaujama jo asmens duomenimis, pats savaime gali reikšti neturtinę žalą, kaip tai suprantama pagal BDAR 82 straipsnio 1 dalį. Jeigu gali, toks asmuo neprivalėtų įrodyti, kad tretieji asmenys – dar iki jo prašymo atlyginti žalą pateikimo – neteisėtai pasinaudojo šiais duomenimis, pavyzdžiui, suklastoję jo asmens tapatybę.

21 Šiomis aplinkybėmis *Varhoven administrativen sad* (Aukščiausiasis administracinis teismas) nutarė sustabdyti bylos nagrinėjimą ir pateikti Teisingumo Teismui tokius prejudicinius klausimus:

„1. Ar [BDAR] 24 ir 32 straipsniai aiškintini taip, jog aplinkybės, kad asmens duomenis be leidimo atskleidė arba be leidimo gavo prieigą prie jų, kaip tai suprantama pagal [BDAR] 4 straipsnio 12 punktą, asmenys, kurie nėra duomenų valdytojo administracijos darbuotojai ir kurių jis nekontroliuoja, pakanka, kad būtų galima daryti prielaidą, jog taikytos techninės ir organizacinės priemonės yra netinkamos?

2. Jeigu į pirmąjį klausimą būtų atsakyta neigiamai, koks turėtų būti teisminės teisėtumo kontrolės dalykas ir apimtis vertinant, ar techninės ir organizacinės priemonės, kurių ėmėsi duomenų valdytojas, yra tinkamos pagal [BDAR] 32 straipsnį?

3. Jeigu į pirmąjį klausimą būtų atsakyta neigiamai, ar [BDAR] 5 straipsnio 2 dalyje ir 24 straipsnyje, siejamuose su [jo] 74 konstatuojamąja dalimi, įtvirtintas atskaitomybės principas aiškintinas taip, kad pagal [šio reglamento] 82 straipsnio 1 dalį nagrinėjant ieškinį teisme duomenų valdytojui tenka pareiga įrodyti, kad taikytos techninės ir organizacinės priemonės yra tinkamos pagal [jo] 32 straipsnį?

   Ar gauta eksperto išvada gali būti laikoma būtinu ir pakankamu įrodymu siekiant nustatyti, ar techninės ir organizacinės priemonės, kurių ėmėsi duomenų valdytojas, buvo tinkamos tokiu atveju, kaip šis, kai prieiga prie asmens duomenų be leidimo gauta ir duomenys be leidimo buvo atskleisti įvykdžius „programišių išpuolį“?

4. Ar [BDAR] 82 straipsnio 3 dalis aiškintina taip, kad asmens duomenų atskleidimas be leidimo arba prieigos prie jų gavimas be leidimo, kaip tai suprantama pagal [jo] 4 straipsnio 12 punktą, kaip šioje byloje, kai „programišių išpuolį“ įvykdė asmenys, kurie nėra duomenų valdytojo administracijos darbuotojai ir kurių jis nekontroliuoja, yra aplinkybė, už kurią duomenų valdytojas jokiu būdu nėra atsakingas ir dėl kurios jis gali būti atleistas nuo atsakomybės?

5. Ar [BDAR] 82 straipsnio 1 ir 2 dalys kartu su [jo] 85 ir 146 konstatuojamosiomis dalimis aiškintinos taip, kad tokiu atveju, kaip šis, kai buvo padarytas asmens duomenų saugumo pažeidimas, t. y. be leidimo gauta prieiga prie asmens duomenų ir duomenys be leidimo platinti įvykdžius „programišių išpuolį“, tik duomenų subjekto patirti rūpesčiai, nuogąstavimai ir baimė dėl galimo būsimo piktnaudžiavimo asmens duomenimis patenka į plačiai aiškintiną neturtinės žalos sąvoką ir pagrindžia jo teisę reikalauti atlyginti žalą, jeigu toks piktnaudžiavimas nebuvo nustatytas ir (arba) duomenų subjektas nepatyrė jokios papildomos žalos?“

## Dėl prejudicinių klausimų

### *Dėl pirmojo klausimo*

22 Pirmuoju klausimu prašymą priimti prejudicinį sprendimą pateikęs teismas iš esmės siekia sužinoti, ar BDAR 24 ir 32 straipsnius reikia aiškinti taip, kad vien aplinkybės, jog „tretieji asmenys“, kaip jie suprantami pagal šio reglamento 4 straipsnio 10 punktą, be leidimo atskleidė asmens duomenis arba be leidimo gavo prie jų prieigą, pakanka, kad būtų galima preziumuoti, jog atitinkamo duomenų valdytojo įgyvendintos techninės ir organizacinės priemonės nebuvo „tinkamos“, kaip tai suprantama pagal 24 ir 32 straipsnius.

23 Iš pradžių reikėtų priminti, kad pagal suformuotą jurisprudenciją, kai Sąjungos teisės nuostatoje, kaip antai BDAR 24 ir 32 straipsniuose, aiškiai nedaroma nuorodos į valstybių narių teisę, kuri padėtų nustatyti šios nuostatos prasmę ir apimtį, jos reikšmė visoje Europos Sąjungoje paprastai turi būti aiškinama savarankiškai ir vienodai; taip aiškinti reikia, be kita ko, atsižvelgiant į atitinkamos nuostatos formuluotę, siekiamus tikslus ir kontekstą (šiuo klausimu žr. 1984 m. sausio 18 d. Sprendimo *Ekro*, 327/82, EU:C:1984:11, 11 punktą; 2019 m. spalio 1 d. Sprendimo

*Planet49*, C-673/17, EU:C:2019:801, 47 ir 48 punktus ir 2023 m. gegužės 4 d. Sprendimo *Österreichische Post (Neturtinė žala, susijusi su asmens duomenų tvarkymu)*, C-300/21, EU:C:2023:370, 29 punktą).

24 Pirma, dėl atitinkamų nuostatų formuluotės pažymėtina, kad BDAR 24 straipsnyje yra nustatyta bendroji asmens duomenų valdytojo pareiga įgyvendinti tinkamas technines ir organizacines priemones, siekiant užtikrinti, kad duomenys būtų tvarkomi laikantis šio reglamento, ir galėti tai įrodyti.

25 Šiuo tikslu 24 straipsnio 1 dalyje išvardyti tam tikri kriterijai, į kuriuos reikia atsižvelgti vertinant tokių priemonių tinkamumą, t. y. duomenų tvarkymo pobūdis, aprėptis, kontekstas ir tikslai, taip pat skirtingos tikimybės ir rimtumo pavojai fizinių asmenų teisėms ir laisvėms. Šioje nuostatoje priduriama, kad minėtos priemonės prireikus peržiūrimos ir atnaujinamos.

26 Atsižvelgiant į tai, BDAR 32 straipsnyje patikslinamos duomenų valdytojo ir galimo duomenų tvarkytojo pareigos duomenų tvarkymo saugumo požiūriu. Šio straipsnio 1 dalyje nustatyta, kad valstybės narės turi įgyvendinti tinkamas technines ir organizacines priemones, kad užtikrintų pirmesniame šio sprendimo punkte nurodytą pavojų atitinkantį saugumo lygį, atsižvelgdamos į techninių galimybių išsivystymo lygį, įgyvendinimo sąnaudas ir duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus.

27 Šio straipsnio 2 dalyje taip pat nurodyta, kad nustatant tinkamo lygio saugumą visų pirma atsižvelgiama į pavojus, kurių kyla dėl duomenų tvarkymo, visų pirma dėl netyčinio arba neteisėto tokių duomenų sunaikinimo, praradimo, pakeitimo, atskleidimo be leidimo ar neteisėtos prieigos prie jų.

28 Be to, tiek šio reglamento 24 straipsnio 3 dalyje, tiek jo 32 straipsnio 3 dalyje nurodyta, kad duomenų valdytojas arba duomenų tvarkytojas gali įrodyti, kad laikėsi tų straipsnių 1 dalies reikalavimų, remdamasis tuo, kad laikosi patvirtinto elgesio kodekso arba patvirtinto sertifikavimo mechanizmo, kaip numatyta to reglamento 40 ir 42 straipsniuose.

29 BDAR 32 straipsnio 1 ir 2 dalyse pateikta nuoroda į „pavojų atitinkančio lygio saugumą“ ir „tinkamo lygio saugumą“ rodo, kad šiame reglamente nustatyta pavojaus valdymo sistema ir visiškai nesiekiama pašalinti asmens duomenų saugumo pažeidimų pavojaus.

30 Taigi iš BDAR 24 ir 32 straipsnių formuluočių matyti, kad pagal šias nuostatas tik reikalaujama, kad duomenų valdytojas priimtų technines ir organizacines priemones, kuriomis būtų siekiama kiek įmanoma išvengti bet kokio asmens duomenų apsaugos pažeidimo. Tokių priemonių tinkamumas turi būti vertinamas konkrečiai, nagrinėjant, ar duomenų valdytojas jas įgyvendino, atsižvelgdamas į įvairius minėtuose straipsniuose nurodytus kriterijus ir duomenų apsaugos poreikius, konkrečiai susijusius su atitinkamu duomenų tvarkymu ir su jo keliamais pavojais.

31 Taigi BDAR 24 ir 32 straipsniai negali būti suprantami taip, kad tretiesiems asmenims be leidimo atskleidus asmens duomenis arba be leidimo gavus prie jų prieigą, to pakanka, kad būtų galima daryti išvadą, jog atitinkamo duomenų valdytojo priimtos priemonės buvo netinkamos, kaip tai suprantama pagal šias nuostatas, net jam nesuteikiant galimybės pateikti priešingus įrodymus.

32 Tokiu aiškinimu reikėtų vadovautis juo labiau dėl to, kad BDAR 24 straipsnyje aiškiai numatyta, jog duomenų valdytojas turi galėti įrodyti, kad jo įgyvendintos priemonės atitinka šį reglamentą; šios galimybės jis neturėtų, jeigu būtų vadovaujamasi nenuginčijama prezumpcija.

33 Antra, tokį BDAR 24 ir 32 straipsnių aiškinimą patvirtina kontekstiniai ir teleologiniai aspektai.

34 Dėl šių abiejų straipsnių konteksto, viena vertus, pažymėtina, kad iš BDAR 5 straipsnio 2 dalies matyti, jog duomenų valdytojas turi sugebėti įrodyti, kad laikėsi šio straipsnio 1 dalyje įtvirtintų asmens duomenų tvarkymo principų. Ši pareiga pakartota ir patikslinta minėto reglamento 24 straipsnio 1 ir 3 dalyse ir 32 straipsnio 3 dalyje kalbant apie pareigą įgyvendinti technines ir organizacines priemones siekiant užtikrinti tokių duomenų apsaugą, kai juos tvarko duomenų valdytojas. Tokia pareiga įrodyti šių priemonių tinkamumą neturėtų prasmės, jeigu duomenų valdytojas privalėtų užkirsti kelią bet kokiam minėtų duomenų apsaugos pažeidimui.

35 Be to, BDAR 74 konstatuojamojoje dalyje pabrėžiama, jog svarbu, kad duomenų valdytojas būtų įpareigotas įgyvendinti tinkamas ir veiksmingas priemones ir galėtų įrodyti, kad duomenų tvarkymo veikla atitinka šį reglamentą, įskaitant priemonių, kuriomis turėtų būti atsižvelgiama į 24 ir 32 straipsniuose nustatytus kriterijus, susijusius su atitinkamo duomenų tvarkymo ypatumais ir keliamu pavojumi, veiksmingumą.

36 Pagal šio reglamento 76 konstatuojamąją dalį pavojaus tikimybė ir rimtumas taip pat priklauso nuo atitinkamo duomenų tvarkymo ypatumų ir pavojus turėtų būti vertinamas objektyviai.

37 Be to, iš BDAR 82 straipsnio 2 ir 3 dalių matyti, kad nors duomenų valdytojas yra atsakingas už žalą, padarytą dėl duomenų tvarkymo pažeidžiant šį reglamentą, jis atleidžiamas nuo atsakomybės, jeigu įrodo, kad jokiu būdu nėra atsakingas už įvykį, dėl kurio patirta žala.

38 Kita vertus, šio sprendimo 31 punkte pateiktą aiškinimą patvirtina ir BDAR 83 konstatuojamoji dalis, kurios pirmame sakinyje nurodyta, kad, „siekiant užtikrinti saugumą ir užkirsti kelią šį reglamentą pažeidžiančiam duomenų tvarkymui, duomenų valdytojas arba duomenų tvarkytojas turėtų įvertinti su duomenų tvarkymu susijusius pavojus ir įgyvendinti jo mažinimo priemones“. Taip Sąjungos teisės aktų leidėjas išreiškė ketinimą „mažinti“ asmens duomenų apsaugos pažeidimo pavojus, bet neteigė, kad juos galima pašalinti.

39 Atsižvelgiant į tai, kas išdėstyta, į pirmąjį klausimą atsakytina: BDAR 24 ir 32 straipsnius reikia aiškinti taip, kad vien aplinkybės, jog „tretieji asmenys“, kaip jie suprantami pagal šio reglamento 4 straipsnio 10 punktą, be leidimo atskleidė asmens duomenis arba be leidimo gavo prie jų prieigą, nepakanka, kad būtų galima preziumuoti, jog atitinkamo duomenų valdytojo įgyvendintos techninės ir organizacinės priemonės nebuvo „tinkamos“, kaip tai suprantama pagal 24 ir 32 straipsnius.

### *Dėl antrojo klausimo*

40 Antruoju klausimu prašymą priimti prejudicinį sprendimą pateikęs teismas iš esmės siekia išsiaiškinti, ar BDAR 32 straipsnis turi būti aiškinamas taip, kad techninių ir organizacinių priemonių, kurias pagal šį straipsnį įgyvendina duomenų valdytojas, tinkamumą nacionaliniai teismai turi vertinti konkrečiai, be kita ko, atsižvelgdami į su atitinkamu duomenų tvarkymu susijusius pavojus.

41 Šiuo aspektu primintina, kaip jau buvo pabrėžta atsakant į pirmąjį klausimą, kad pagal BDAR 32 straipsnį iš duomenų valdytojo ir duomenų tvarkytojo reikalaujama, atsižvelgiant į jo 1 dalyje išvardytus vertinimo kriterijus, reikiamais atvejais įgyvendinti tinkamas technines ir organizacines

priemones, kad būtų užtikrintas pavojų atitinkančio lygio saugumas. Be to, šio straipsnio 2 dalyje pateiktas nebaigtinis sąrašas veiksnių, reikšmingų nustatant tinkamo lygio saugumą, atsižvelgiant į pavojus, kylančius dėl atitinkamo duomenų tvarkymo.

42 Iš 32 straipsnio 1 ir 2 dalių matyti, kad tokių techninių ir organizacinių priemonių tinkamumą reikia vertinti dviem etapais. Pirma, reikia nustatyti asmens duomenų saugumo pažeidimo dėl atitinkamo duomenų tvarkymo pavojus ir galimas pasekmes fizinių asmenų teisėms ir laisvėms. Šis vertinimas turi būti atliekamas konkrečiai, atsižvelgiant į nustatyto pavojaus tikimybės ir rimtumo laipsnį. Antra, reikia patikrinti, ar duomenų valdytojo įgyvendintos priemonės pritaikytos šiam pavojui, atsižvelgiant į techninių galimybių išsivystymo lygį, įgyvendinimo sąnaudas ir duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus.

43 Žinoma, duomenų valdytojas turi tam tikrą diskreciją nustatyti tinkamas technines ir organizacines priemones, kad užtikrintų pavojų atitinkančio lygio saugumą, kaip reikalaujama pagal BDAR 32 straipsnio 1 dalį. Vis dėlto nacionalinis teismas turi galėti įvertinti duomenų valdytojo atliktą kompleksinę analizę ir taip įsitikinti, kad jo pasirinktos priemonės yra tinkamos tokiam saugumo lygiui užtikrinti.

44 Be to, toks aiškinimas gali užtikrinti, viena vertus, asmens duomenų apsaugos veiksmingumą, kuris pabrėžiamas šio reglamento 11 ir 74 konstatuojamosiose dalyse, ir, kita vertus, teisę imtis veiksmingų teisminių teisių gynimo priemonių prieš duomenų valdytoją, saugomą pagal minėto reglamento 79 straipsnio 1 dalį, siejamą su jo 4 konstatuojamąja dalimi.

45 Taigi, siekdamas patikrinti pagal BDAR 32 straipsnį įgyvendintų techninių ir organizacinių priemonių tinkamumą, nacionalinis teismas turi ne tik konstatuoti, kaip atitinkamas duomenų valdytojas ketino įvykdyti jam pagal šį straipsnį tenkančias pareigas, bet ir išnagrinėti šias priemones iš esmės, atsižvelgdamas į visus minėtame straipsnyje nurodytus kriterijus, konkretaus atvejo aplinkybes ir teismo šiuo klausimu turimus įrodymus.

46 Nagrinėjant reikia konkrečiai išanalizuoti duomenų valdytojo įgyvendintų priemonių pobūdį ir turinį, jų taikymo būdą ir praktinį poveikį saugumo lygiui, kurį jis privalėjo užtikrinti, atsižvelgdamas į su šiuo duomenų tvarkymu susijusius pavojus.

47 Taigi į antrąjį klausimą atsakytina: BDAR 32 straipsnis turi būti aiškinamas taip, kad techninių ir organizacinių priemonių, kurias pagal šį straipsnį įgyvendina duomenų valdytojas, tinkamumą nacionaliniai teismai turi vertinti konkrečiai, atsižvelgdami į su atitinkamu duomenų tvarkymu susijusius pavojus ir vertindami, ar šių priemonių pobūdis, turinys ir įgyvendinimas pritaikytas tokiems pavojams.

### *Dėl trečiojo klausimo*

#### *Dėl trečiojo klausimo pirmos dalies*

48 Trečiojo klausimo pirma dalimi prašymą priimti prejudicinį sprendimą pateikęs teismas iš esmės siekia išsiaiškinti, ar BDAR 5 straipsnio 2 dalyje įtvirtintas ir jo 24 straipsnyje sukonkretintas duomenų valdytojo atsakomybės principas turi būti aiškinamas taip, kad, nagrinėjant šio reglamento 82 straipsniu grindžiamą ieškinį dėl žalos atlyginimo, atitinkamam duomenų valdytojui tenka pareiga įrodyti saugumo priemonių, kurias įgyvendino pagal minėto reglamento 32 straipsnį, tinkamumą.

49 Šiuo klausimu pirmiausia primintina, kad BDAR 5 straipsnio 2 dalyje yra nustatytas atsakomybės principas, pagal kurį duomenų valdytojas yra atsakingas už šio straipsnio 1 dalyje įtvirtintų asmens duomenų tvarkymo principų laikymąsi, ir numatyta, kad duomenų valdytojas turi sugebėti įrodyti, jog šių principų laikomasi.

50 Konkrečiai kalbant, pagal šio reglamento 5 straipsnio 1 dalies f punkte įtvirtintą asmens duomenų vientisumo ir konfidencialumo principą duomenų valdytojas privalo taikydamas tinkamas technines ar organizacines priemones užtikrinti, kad duomenys būtų tvarkomi taip, kad būtų užtikrintas tinkamas jų saugumas, įskaitant apsaugą nuo duomenų tvarkymo be leidimo ar neteisėto duomenų tvarkymo ir nuo netyčinio praradimo, sunaikinimo ar sugadinimo, ir turi sugebėti įrodyti, kad šio principo laikomasi.

51 Taip pat pažymėtina, kad tiek pagal BDAR 24 straipsnio 1 dalį, siejamą su jo 74 konstatuojamąja dalimi, tiek pagal šio reglamento 32 straipsnio 1 dalį reikalaujama, kad duomenų valdytojas, kai tvarko asmens duomenis pats arba jie tvarkomi jo vardu, įgyvendintų tinkamas technines ir organizacines priemones, kad užtikrintų ir galėtų įrodyti, kad duomenys tvarkomi laikantis minėto reglamento.

52 Iš BDAR 5 straipsnio 2 dalies, 24 straipsnio 1 dalies ir 32 straipsnio 1 dalies formuluočių vienareikšmiškai matyti, kad pareiga įrodyti, jog asmens duomenys tvarkomi taip, kad būtų užtikrintas tinkamas asmens duomenų saugumas, kaip tai suprantama pagal šio reglamento 5 straipsnio 1 dalies f punktą ir 32 straipsnį, tenka atitinkamam duomenų valdytojui (pagal analogiją žr. 2023 m. gegužės 4 d. Sprendimo *Bundesrepublik Deutschland (Teismo elektroninio pašto dėžutė)*, C-60/22, EU:C:2023:373, 52 ir 53 punktus ir 2023 m. liepos 4 d. Sprendimo *Meta Platforms ir kt. (Bendrosios naudojimosi socialiniu tinklu sąlygos)*, C-252/21, EU:C:2023:537, 95 punktą).

53 Taigi šiuose trijuose straipsniuose įtvirtinta bendroji taisyklė, kuri, jeigu BDAR nenurodyta kitaip, taip pat turi būti taikoma nagrinėjant šio reglamento 82 straipsniu grindžiamą ieškinį dėl žalos atlyginimo.

54 Antra, konstatuotina, kad pirmesniuose punktuose išdėstytą lingvistinį aiškinimą patvirtina BDAR siekiami tikslai.

55 Viena vertus, kadangi BDAR numatytos apsaugos lygis priklauso nuo asmens duomenų valdytojų priimtų saugumo priemonių, jie turi būti skatinami, kadangi jiems tenka pareiga įrodyti šių priemonių tinkamumą, dėti visas pastangas, kad būtų užkirstas kelias šio reglamento nuostatų neatitinkančioms duomenų tvarkymo operacijoms.

56 Kita vertus, jeigu reikėtų vadovautis nuostata, kad pareiga įrodyti minėtų priemonių tinkamumą tenka duomenų subjektams, kaip jie apibrėžti BDAR 4 straipsnio 1 punkte, tai reikštų, kad šio reglamento 82 straipsnio 1 dalyje numatyta teisė į kompensaciją netektų didelės dalies savo veiksmingumo, nors Sąjungos teisės aktų leidėjas siekė sustiprinti šių asmenų teises ir duomenų valdytojų pareigas, palyginti su iki šio reglamento galiojusiomis nuostatomis, kaip nurodyta jo 11 konstatuojamojoje dalyje.

57 Taigi į trečiojo klausimo pirmą dalį atsakytina: BDAR 5 straipsnio 2 dalyje įtvirtintas ir jo 24 straipsnyje sukonkretintas duomenų valdytojo atsakomybės principas turi būti aiškinamas taip, kad, nagrinėjant šio reglamento 82 straipsniu grindžiamą ieškinį dėl žalos atlyginimo, atitinkamam duomenų valdytojui tenka pareiga įrodyti saugumo priemonių, kurias įgyvendino pagal minėto reglamento 32 straipsnį, tinkamumą.

*Dėl trečiojo klausimo antros dalies*

58 Trečiojo klausimo antra dalimi prašymą priimti prejudicinį sprendimą pateikęs teismas iš esmės siekia išsiaiškinti, ar BDAR 32 straipsnis ir Sąjungos teisės veiksmingumo principas turi būti aiškinami taip, kad, siekiant įvertinti saugumo priemonių, kurias duomenų valdytojas įgyvendino pagal šį straipsnį, tinkamumą, teismo ekspertizė yra būtinas ir pakankamas įrodymas.

59 Šiuo klausimu primintina, kad pagal suformuotą jurisprudenciją, kai nėra atitinkamą sritį reglamentuojančių Sąjungos teisės normų, pagal procesinės autonomijos principą kiekviena valstybė narė savo nacionalinės teisės sistemoje turi reglamentuoti ieškinių, skirtų teisės subjektų teisių apsaugai užtikrinti, procesinius aspektus su sąlyga, kad Sąjungos teisės reglamentuojamose situacijose šios taisyklės nebūtų mažiau palankios nei taisyklės, reglamentuojančios panašias situacijas, kurioms taikoma vidaus teisė (lygiavertiškumo principas), ir kad dėl jų netaptų praktiškai neįmanoma ar pernelyg sudėtinga pasinaudoti Sąjungos teisės suteiktomis teisėmis (veiksmingumo principas) (šiuo klausimu žr. 2023 m. gegužės 4 d. Sprendimo *Österreichische Post (Neturtinė žala, susijusi su asmens duomenų tvarkymu)*, C-300/21, EU:C:2023:370, 53 punktą ir jame nurodytą jurisprudenciją).

60 Nagrinėjamu atveju pažymėtina, kad BDAR nėra įtvirtintų taisyklių dėl įrodymų, pavyzdžiui, teismo ekspertizės, priimtinumo ir įrodomosios galios; šias taisykles turi taikyti nacionaliniai teismai, nagrinėjantys šio reglamento 82 straipsniu grindžiamus ieškinius dėl žalos atlyginimo ir privalantys, atsižvelgiant į jo 32 straipsnį, įvertinti atitinkamo duomenų valdytojo įgyvendintų saugumo priemonių tinkamumą. Todėl, remiantis tuo, kas buvo priminta pirmesniame šio sprendimo punkte, ir nesant Sąjungos teisės normų šioje srityje, kiekviena valstybė narė savo nacionalinės teisės sistemoje turi nustatyti ieškinių, skirtų iš šio 82 straipsnio kylančių asmenų teisių apsaugai užtikrinti, pareiškimo tvarką, ypač taisykles dėl įrodinėjimo priemonių, leidžiančias įvertinti tokių priemonių tinkamumą šiame kontekste, su sąlyga, kad laikomasi minėtų lygiavertiškumo ir veiksmingumo principų (pagal analogiją žr. 2022 m. birželio 21 d. Sprendimo *Ligue des droits humains*, C-817/19, EU:C:2022:491, 297 punktą ir 2023 m. gegužės 4 d. Sprendimo *Österreichische Post (Neturtinė žala, susijusi su asmens duomenų tvarkymu)*, C-300/21, EU:C:2023:370, 54 punktą).

61 Šioje byloje Teisingumo Teismas neturi jokių duomenų, galinčių sukelti abejonių dėl lygiavertiškumo principo laikymosi. Kitaip yra su atitiktimi veiksmingumo principui, nes pačioje trečiojo klausimo antros dalies formuluotėje teismo ekspertizė nurodoma kaip „būtinas ir pakankamas įrodymas“.

62 Ypač nacionalinė procesinė norma, pagal kurią bet kuriuo atveju nacionaliniams teismams „būtina“ paskirti atlikti teismo ekspertizę, galėtų pažeisti veiksmingumo principą. Iš tiesų sistemingai skirti tokią ekspertizę gali būti nereikalinga atsižvelgiant į kitus teismo, į kurį kreiptasi, turimus įrodymus, be kita ko, kaip savo rašytinėse pastabose nurodė Bulgarijos vyriausybė, atsižvelgiant į asmens duomenų apsaugos priemonių laikymosi kontrolės, kurią atliko

pagal įstatymą įsteigta nepriklausoma institucija, rezultatus, jeigu ši kontrolė atlikta neseniai, nes pagal BDAR 24 straipsnio 1 dalį minėtos priemonės prireikus turi būti peržiūrimos ir atnaujinamos.

63 Be to, kaip savo rašytinėse pastabose pažymėjo Europos Komisija, veiksmingumo principas galėtų būti pažeistas, jeigu žodis „pakankamas“ turėtų būti suprantamas kaip reiškiantis, kad nacionalinis teismas išimtinai arba automatiškai pagal teismo ekspertizės rezultatus turi padaryti išvadą, jog atitinkamo duomenų valdytojo įgyvendintos saugumo priemonės yra „tinkamos“, kaip tai suprantama pagal BDAR 32 straipsnį. Vis dėlto šiame reglamente suteiktų teisių apsauga, kurios siekiama minėtu veiksmingumo principu, o ypač jo 79 straipsnio 1 dalyje garantuojama teisė imtis veiksmingų teisminių teisių gynimo priemonių prieš duomenų valdytoją, reikalauja, kad nešališkas teismas objektyviai įvertintų atitinkamų priemonių tinkamumą, o ne apsiribotų tokios išvados darymu (šiuo klausimu žr. 2023 m. sausio 12 d. Sprendimo *Nemzeti Adatvédelmi és Információszabadság Hatóság*, C-132/21, EU:C:2023:2, 50 punktą).

64 Atsižvelgiant į tai, kas išdėstyta, į trečiojo klausimo antrą dalį atsakytina: BDAR 32 straipsnis ir Sąjungos teisės veiksmingumo principas turi būti aiškinami taip, kad, siekiant įvertinti saugumo priemonių, kurias duomenų valdytojas įgyvendino pagal šį straipsnį, tinkamumą, teismo ekspertizė negali būti bet kuriuo atveju būtinas ir pakankamas įrodymas.

### *Dėl ketvirtojo klausimo*

65 Ketvirtuoju klausimu prašymą priimti prejudicinį sprendimą pateikęs teismas iš esmės siekia išsiaiškinti, ar BDAR 82 straipsnio 3 dalis turi būti aiškinama taip, kad duomenų valdytojas atleidžiamas nuo pareigos pagal šio reglamento 82 straipsnio 1 ir 2 dalis atlyginti asmens patirtą žalą vien dėl to, kad žala kilo „tretiesiems asmenims“, kaip jie suprantami pagal šio reglamento 4 straipsnio 10 punktą, be leidimo atskleidus asmens duomenis arba be leidimo gavus prie jų prieigą.

66 Pirmiausia reikia patikslinti, kad iš BDAR 4 straipsnio 10 punkto matyti, jog „tretieji asmenys“ yra, be kita ko, kiti asmenys nei tie, kuriems tiesioginiu duomenų valdytojo ar duomenų tvarkytojo įgaliojimu leidžiama tvarkyti asmens duomenis. Ši apibrėžtis apima tokius asmenis, kurie nėra duomenų valdytojo darbuotojai ir jo kontroliuojami, kaip antai nurodytus pateiktame klausime.

67 Toliau primintina, pirma, kad BDAR 82 straipsnio 2 dalyje nustatyta, jog „tvarkant duomenis dalyvaujantis duomenų valdytojas atsako už žalą, padarytą dėl vykdyto duomenų tvarkymo pažeidžiant šį reglamentą“, o šio straipsnio 3 dalyje numatyta, jog duomenų valdytojas arba atitinkamais atvejais duomenų tvarkytojas atleidžiamas nuo tokios atsakomybės, „jeigu įrodo, kad jokiu būdu nėra atsakingas už įvykį, dėl kurio patirta žala“.

68 Be to, BDAR 146 konstatuojamosios dalies, kuri konkrečiai susijusi su jo 82 straipsniu, pirmame ir antrame sakiniuose nurodyta, kad „bet kokią žalą, kurią asmuo gali patirti dėl duomenų tvarkymo pažeidžiant šį reglamentą, turėtų atlyginti duomenų valdytojas arba duomenų tvarkytojas“ ir kad duomenų valdytojas arba duomenų tvarkytojas „turėtų būti atleistas nuo atsakomybės, jeigu jie įrodo, kad jokiu būdu nėra atsakingi už žalą“.

69 Iš šių nuostatų matyti, kad, viena vertus, atitinkamas duomenų valdytojas iš esmės turi atlyginti žalą, atsiradusią dėl šio reglamento pažeidimo, susijusio su duomenų tvarkymu, ir, kita vertus, jis gali būti atleistas nuo atsakomybės tik jeigu pateikia įrodymų, kad jokiu būdu nėra atsakingas už šią žalą sukėlusį įvykį.

70 Taigi, tai, kad per teisėkūros procedūrą buvo specialiai pridėtas žodžių junginys „jokiu būdu“, rodo, kad aplinkybės, kuriomis duomenų valdytojas gali reikalauti atleidimo nuo jam tenkančios civilinės atsakomybės pagal BDAR 82 straipsnį, turi būti griežtai apribotos iki aplinkybių, kai duomenų valdytojas gali įrodyti, kad jam negali būti priskirta atsakomybė už žalą.

71 Jeigu, kaip nagrinėjamu atveju, asmens duomenų saugumo pažeidimą, kaip jis suprantamas pagal BDAR 4 straipsnio 12 punktą, padarė kibernetiniai nusikaltėliai, taigi ir „tretieji asmenys“, kaip tai suprantama pagal šio reglamento 4 straipsnio 10 punktą, šis pažeidimas negali būti priskiriamas duomenų valdytojui, nebent jis jam sudarė sąlygas, pažeisdamas BDAR numatytą pareigą, be kita ko, pareigą saugoti duomenis, kuri jam tenka pagal šio reglamento 5 straipsnio 1 dalies f punktą, 24 ir 32 straipsnius.

72 Taigi, jeigu trečiasis asmuo pažeidžia asmens duomenų saugumą, duomenų valdytojas gali būti atleistas nuo atsakomybės pagal BDAR 82 straipsnio 3 dalį, jeigu įrodo, kad nėra jokio priežastinio ryšio tarp jo galimo duomenų apsaugos pareigos pažeidimo ir fizinio asmens patirtos žalos.

73 Antra, pirma pateiktas šio 82 straipsnio 3 dalies aiškinimas taip pat atitinka BDAR tikslą užtikrinti aukštą fizinių asmenų apsaugos tvarkant jų asmens duomenis lygį, nurodytą šio reglamento 10 ir 11 konstatuojamosiose dalyse.

74 Atsižvelgiant į visa tai, kas išdėstyta, į ketvirtąjį klausimą atsakytina: BDAR 82 straipsnio 3 dalis turi būti aiškinama taip, kad duomenų valdytojas negali būti atleistas nuo pareigos pagal šio reglamento 82 straipsnio 1 ir 2 dalis atlyginti asmens patirtą žalą vien dėl to, kad žala kilo „tretiesiems asmenims“, kaip jie suprantami pagal šio reglamento 4 straipsnio 10 punktą, be leidimo atskleidus asmens duomenis arba be leidimo gavus prie jų prieigą, nes duomenų valdytojas privalo įrodyti, kad jokiu būdu nėra atsakingas už įvykį, dėl kurio patirta žala.

### *Dėl penktojo klausimo*

75 Penktuoju klausimu prašymą priimti prejudicinį sprendimą pateikęs teismas iš esmės siekia išsiaiškinti, ar BDAR 82 straipsnio 1 dalis turi būti aiškinama taip, kad vien duomenų subjekto nuogąstavimai, jog tretieji asmenys gali piktnaudžiauti asmens duomenimis dėl šio reglamento pažeidimo, savaime gali reikšti „neturtinę žalą“, kaip ji suprantama pagal šią nuostatą.

76 Pirma, dėl BDAR 82 straipsnio teksto pažymėtina, kad jo 1 dalyje nurodyta, jog „[b]et kuris asmuo, patyręs materialinę ar nematerialinę žalą dėl šio reglamento pažeidimo, turi teisę iš duomenų valdytojo arba duomenų tvarkytojo gauti kompensaciją už patirtą žalą“.

77 Šiuo klausimu Teisingumo Teismas yra pažymėjęs, kad iš BDAR 82 straipsnio 1 dalies formuluotės aiškiai matyti, kad „patirtos žalos“ buvimas yra viena iš šioje nuostatoje numatytos teisės į kompensaciją sąlygų, kaip ir sąlygos, kad turi būti padarytas BDAR pažeidimas ir egzistuoti priežastinis ryšys tarp žalos ir pažeidimo, turint omenyje, kad šios trys sąlygos yra kumuliacinės (2023 m. gegužės 4 d Sprendimo *Österreichische Post (Neturtinė žala, susijusi su asmens duomenų tvarkymu)*, C-300/21, EU:C:2023:370, 32 punktas).

78 Be to, remdamasis lingvistiniu, sisteminiu ir teleologiniu aspektais, Teisingumo Teismas aiškino BDAR 82 straipsnio 1 dalį taip, kad pagal ją draudžiama nacionalinė teisės norma, pagal kurią „neturtinės žalos“ kompensavimas, kaip tai suprantama pagal šią nuostatą, siejamas su sąlyga, kad

duomenų subjekto patirta žala turi pasiekti tam tikrą sunkumo laipsnį (2023 m. gegužės 4 d. Sprendimo *Österreichische Post (Neturtinė žala, susijusi su asmens duomenų tvarkymu)*, C-300/21, EU:C:2023:370, 51 punktas).

79 Tai priminus, nagrinėjamu atveju pažymėtina, kad BDAR 82 straipsnio 1 dalyje nediferencijuojami atvejai, kai esant įrodytam šio reglamento nuostatų pažeidimui tariama duomenų subjekto „neturtinė žala“ siejama, pirma, su trečiųjų asmenų piktnaudžiavimu jo asmens duomenimis, kuris jau yra įvykęs jo prašymo atlyginti žalą pateikimo dieną, arba, antra, su šio asmens baime, kad gali būti piktnaudžiaujama ateityje.

80 Taigi, remiantis BDAR 82 straipsnio 1 dalies formuluote, neatmetama galimybė, kad šioje nuostatoje vartojama sąvoka „neturtinė žala“ apima tokią situaciją, kaip nurodė prašymą priimti prejudicinį sprendimą pateikęs teismas, kai duomenų subjektas, siekdamas gauti kompensaciją pagal šią nuostatą, nurodo nuogąstaujantis, kad ateityje tretieji asmenys piktnaudžiaus jo asmens duomenimis dėl padaryto šio reglamento pažeidimo.

81 Antra, tokį lingvistinį aiškinimą patvirtina BDAR 146 konstatuojamoji dalis, kurioje konkrečiai kalbama apie jo 82 straipsnio 1 dalyje numatytą teisę į kompensaciją ir kurios trečiame sakinyje teigiama, kad „žalos sąvoka turėtų būti aiškinama plačiai, atsižvelgiant į Teisingumo Teismo praktiką, taip, kad būtų visapusiškai atspindėti šio reglamento tikslai“. Sąvokos „neturtinė žala“, kaip ji suprantama pagal šio 82 straipsnio 1 dalį, aiškinimas, kuris neapima situacijų, kai asmuo, kurio atžvilgiu buvo padarytas minėto reglamento pažeidimas, nurodo nuogąstaujantis, kad ateityje gali būti piktnaudžiaujama jo paties asmeniniais duomenimis, neatitiktų plačios šios sąvokos sampratos, kokios siekė Sąjungos teisės aktų leidėjas (pagal analogiją žr. 2023 m. gegužės 4 d. Sprendimo *Österreichische Post (Neturtinė žala, susijusi su asmens duomenų tvarkymu*), C-300/21, EU:C:2023:370, 37 ir 46 punktus).

82 Be to, BDAR 85 konstatuojamosios dalies pirmame sakinyje nurodyta, kad „dėl asmens duomenų saugumo pažeidimo, jei dėl jo laiku nesiimama tinkamų priemonių, fiziniai asmenys gali patirti kūno sužalojimą [fizinę], materialinę ar nematerialinę žalą, pavyzdžiui, prarasti savo asmens duomenų kontrolę, patirti teisių apribojimą, diskriminaciją, gali būti pavogta ar suklastota jo asmens tapatybė, jam padaryta finansinių nuostolių <…> arba padaryta kita ekonominė ar socialinė žala“. Iš šio „žalos“, kurią gali patirti duomenų subjektai, pavyzdžių sąrašo matyti, kad Sąjungos teisės aktų leidėjas ketino į šią sąvoką įtraukti, be kita ko, paprastą jų pačių duomenų „kontrolės praradimą“ dėl šio reglamento pažeidimo, net jeigu aptariamais duomenimis nebuvo konkrečiai piktnaudžiaujama šių asmenų nenaudai.

83 Galiausiai, trečia, šio sprendimo 80 punkte pateiktą aiškinimą patvirtina BDAR tikslai, į kuriuos reikia visapusiškai atsižvelgti siekiant apibrėžti sąvoką „žala“, kaip nurodyta šio reglamento 146 konstatuojamosios dalies trečiame sakinyje. Vis dėlto BDAR 82 straipsnio 1 dalies aiškinimas, pagal kurį sąvoka „neturtinė žala“, kaip ji suprantama pagal šią nuostatą, neapimtų situacijų, kai duomenų subjektas nurodo tik nuogąstaujantis, kad ateityje tretieji asmenys gali piktnaudžiauti jo duomenimis, neatitiktų aukšto lygio fizinių asmenų apsaugos tvarkant asmens duomenis Sąjungoje, kuri numatyta šiame teisės akte.

84 Vis dėlto pabrėžtina, kad asmuo, kurio atžvilgiu padarytas BDAR pažeidimas ir kuris patyrė neigiamų pasekmių, privalo įrodyti, kad šios pasekmės sudaro neturtinę žalą, kaip ji suprantama pagal šio reglamento 82 straipsnį (šiuo klausimu žr. 2023 m. gegužės 4 d. Sprendimo *Österreichische Post (Neturtinė žala, susijusi su asmens duomenų tvarkymu)*, C-300/21, EU:C:2023:370, 50 punktą).

85 Konkrečiai kalbant, kai asmuo, prašantis atlyginti žalą šiuo pagrindu, nurodo nuogąstaujantis, kad dėl tokio pažeidimo ateityje gali būti piktnaudžiaujama jo asmens duomenimis, nacionalinis teismas, į kurį kreiptasi, turi patikrinti, ar toks nuogąstavimas konkrečiomis nagrinėjamomis aplinkybėmis ir atsižvelgiant į duomenų subjektą gali būti laikomas pagrįstu.

86 Atsižvelgiant į tai, kas išdėstyta, į penktąjį klausimą atsakytina: BDAR 82 straipsnio 1 dalis turi būti aiškinama taip, kad duomenų subjekto nuogąstavimai, jog tretieji asmenys gali piktnaudžiauti jo asmens duomenimis dėl šio reglamento pažeidimo, savaime gali reikšti „neturtinę žalą“, kaip ji suprantama pagal šią nuostatą.

## Dėl bylinėjimosi išlaidų

87 Kadangi šis procesas pagrindinės bylos šalims yra vienas iš etapų prašymą priimti prejudicinį sprendimą pateikusio teismo nagrinėjamoje byloje, bylinėjimosi išlaidų klausimą turi spręsti šis teismas. Išlaidos, susijusios su pastabų pateikimu Teisingumo Teismui, išskyrus tas, kurias patyrė minėtos šalys, nėra atlygintinos.

Remdamasis šiais motyvais, Teisingumo Teismas (trečioji kolegija) nusprendžia:

1. **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) 24 ir 32 straipsniai**

   **turi būti aiškinami taip:**

   **vien aplinkybės, jog „tretieji asmenys“, kaip jie suprantami pagal šio reglamento 4 straipsnio 10 punktą, be leidimo atskleidė asmens duomenis arba be leidimo gavo prie jų prieigą, nepakanka, kad būtų galima preziumuoti, jog atitinkamo duomenų valdytojo įgyvendintos techninės ir organizacinės priemonės nebuvo „tinkamos“, kaip tai suprantama pagal 24 ir 32 straipsnius.**

2. **Reglamento 2016/679 32 straipsnis**

   **turi būti aiškinamas taip:**

   **techninių ir organizacinių priemonių, kurias pagal šį straipsnį įgyvendina duomenų valdytojas, tinkamumą nacionaliniai teismai turi vertinti konkrečiai, atsižvelgdami į su atitinkamu duomenų tvarkymu susijusius pavojus ir vertindami, ar šių priemonių pobūdis, turinys ir įgyvendinimas pritaikytas tokiems pavojams.**

3. **Reglamento 2016/679 5 straipsnio 2 dalyje įtvirtintas ir jo 24 straipsnyje sukonkretintas duomenų valdytojo atsakomybės principas**

   **turi būti aiškinamas taip:**

   **nagrinėjant šio reglamento 82 straipsniu grindžiamą ieškinį dėl žalos atlyginimo, atitinkamam duomenų valdytojui tenka pareiga įrodyti saugumo priemonių, kurias įgyvendino pagal minėto reglamento 32 straipsnį, tinkamumą.**

**4. Reglamento 2016/679 32 straipsnis ir Sąjungos teisės veiksmingumo principas**

**turi būti aiškinami taip:**

**siekiant įvertinti saugumo priemonių, kurias duomenų valdytojas įgyvendino pagal šį straipsnį, tinkamumą, teismo ekspertizė negali būti bet kuriuo atveju būtinas ir pakankamas įrodymas.**

**5. Direktyvos 2016/679 82 straipsnio 3 dalis**

**turi būti aiškinama taip:**

**duomenų valdytojas negali būti atleistas nuo pareigos pagal šio reglamento 82 straipsnio 1 ir 2 dalis atlyginti asmens patirtą žalą vien dėl to, kad žala kilo „tretiesiems asmenims“, kaip jie suprantami pagal šio reglamento 4 straipsnio 10 punktą, be leidimo atskleidus asmens duomenis arba be leidimo gavus prie jų prieigą, nes duomenų valdytojas privalo įrodyti, kad jokiu būdu nėra atsakingas už įvykį, dėl kurio patirta žala.**

**6. Direktyvos 2016/679 82 straipsnio 1 dalis**

**turi būti aiškinama taip:**

**duomenų subjekto nuogąstavimai, jog tretieji asmenys gali piktnaudžiauti jo asmens duomenimis dėl šio reglamento pažeidimo, savaime gali reikšti „neturtinę žalą“, kaip ji suprantama pagal šią nuostatą.**

Parašai.