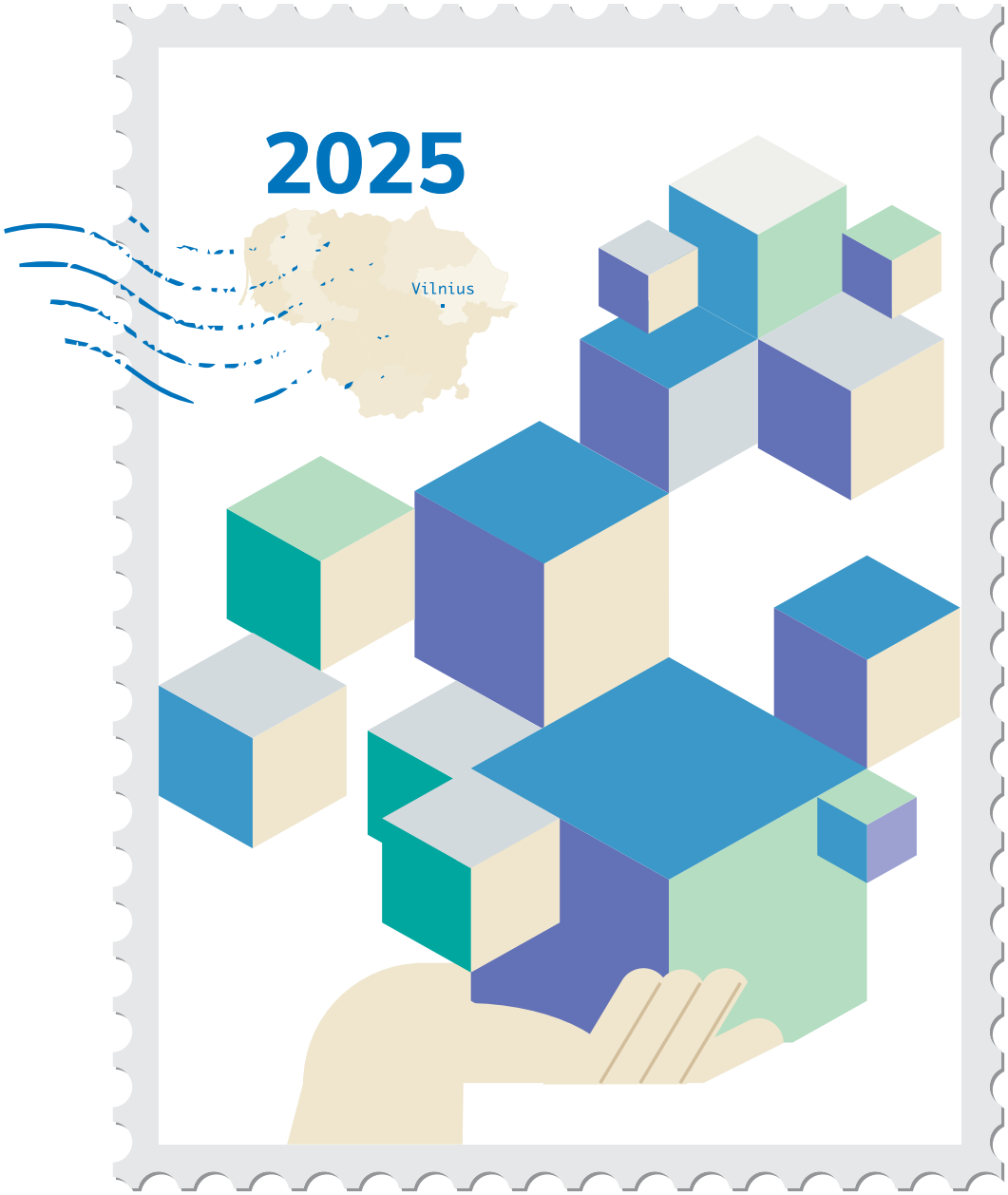
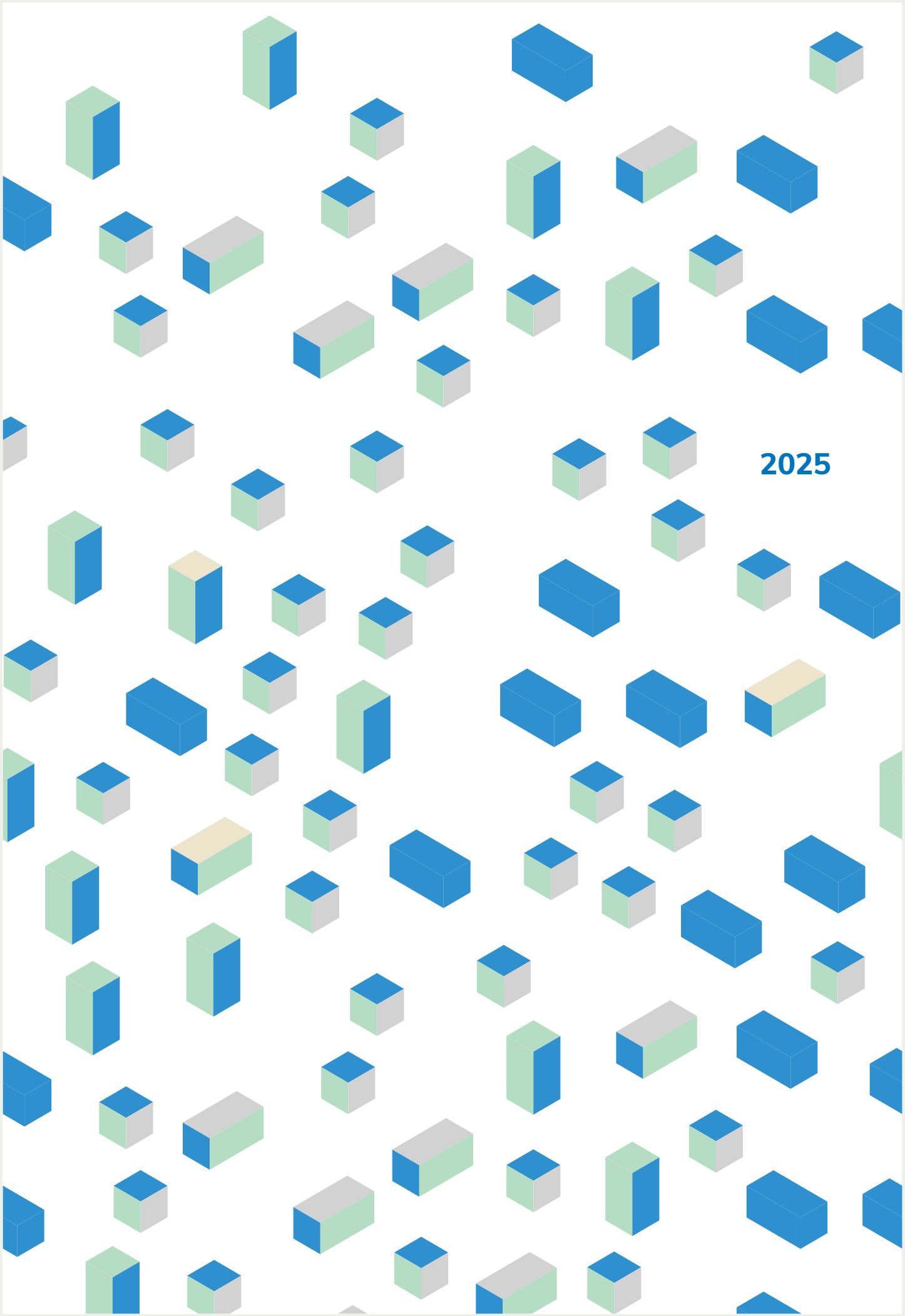
ASMENS DUOMENŲ APSAUGOS PRIEŽIŪROS LIETUVOJE APŽVALGA

REVIEW OF PERSONAL DATA PROTECTION SUPERVISION IN LITHUANIA




2025

VALSTYBINĖ
DUOMENŲ
APSAUGOS
INSPEKCIJA

ŽURNALISTŲ ETIKOS
INSPEKTORIAUS
TARNYBA

LT

Lietuvoje asmens duomenų apsaugos priežiūros veiklą vykdo dvi institucijos – Valstybinė duomenų apsaugos inspekcija ir Žurnalistų etikos inspektoriaus tarnyba, kai asmens duomenys tvarkomi žurnalistikos arba akademinės, meninės ar literatūrinės saviraiškos tikslais. 2025 metų asmens duomenų apsaugos priežiūros Lietuvoje apžvalgoje pateikiama abiejų institucijų informacija.

STATE DATA
PROTECTION
INSPECTORATE

THE OFFICE OF
THE INSPECTOR OF
JOURNALIST ETHICS

EN

Personal data protection supervision activities in Lithuania are carried out by two institutions – the State Data Protection Inspectorate and the Office of the Inspector of Journalist Ethics when personal data are processed for the purposes of journalistic, academic, artistic or literary purposes. The Review of the Personal Data Protection Supervision in Lithuania in 2025 contains information from both institutions.

TURINYS

CONTENT

VALSTYBINĖS DUOMENŲ APSAUGOS INSPEKCIJOS ASMENS DUOMENŲ APSAUGOS PRIEŽIŪROS LIETUVOJE APŽVALGA

Dijana Šinkūnienė
Valstybinės duomenų apsaugos inspekcijos direktorė

VALSTYBINĖS DUOMENŲ APSAUGOS INSPEKCIJOS VADOVĖS ŽODIS

Valstybinė duomenų apsaugos inspekcija (toliau – VDAI) yra nepriklausoma asmens duomenų apsaugos priežiūros institucija, vykdanti Bendrojo duomenų apsaugos reglamento (toliau – BDAR) taikymo priežiūrą ir įgyvendinanti kituose Lietuvos ir Europos Sąjungos (toliau – ES) teisės aktuose nustatytas užduotis. VDAI, kaip asmens duomenų apsaugos priežiūros institucijos, misija – ginti žmogaus teisę į asmens duomenų apsaugą.

Asmens duomenų apsaugos teisės aktų taikymo nuoseklumas priklauso nuo visų ES šalių priežiūros institucijų bendrų pastangų. 2025 m. liepos mėn. Europos duomenų apsaugos valdyba (toliau – EDAV) priėmė vadinamąjį *Helsinkio pareiškimą*, kuriame numatytos priemonės, skirtos sustiprinti bendradarbiavimą tarp institucijų, padidinti BDAR reikalavimų aiškumą ir suteikti papildomos pagalbos mažoms bei vidutinėms organizacijoms. Šis žingsnis prisideda prie didesnio asmens duomenų apsaugos reikalavimų taikymo nuoseklumo visoje ES.

Technologijų raidos ir sparčiai kintančios skaitmeninės aplinkos kontekste duomenų apsaugos sistemos veiksmingumas vis labiau priklauso nuo aktyvaus visų suinteresuotų šalių dalyvavimo. Svarbu ne tik institucijų, bet ir žmonių bei organizacijų žinios, gebėjimas pasinaudoti suteiktomis teisėmis ir atsakingai vykdyti pareigas.

2025 m. siekiant didinti visuomenės informuotumą apie asmens duomenų apsaugą, daug dėmesio skirta metodinės medžiagos rengimui ir viešinimui. Gyventojų susidomėjimas šia tema pastebimai augo – gauta net 48 proc. daugiau skundų ir pranešimų nei 2024 m., tai rodo didėjantį visuomenės sąmoningumą ir ryžtą aktyviau ginti savo teises.

2025 m. augo pasitikėjimas duomenų apsaugos sistema. Reprezentatyvi apklausa parodė, kad 58 proc. gyventojų mano, jog įmonės ir įstaigos Lietuvoje tinkamai užtikrina asmens duomenų apsaugą – tai 6 procentiniais punktais daugiau nei 2024 m. Be to, 50 proc. respondentų įsitikinę, kad visuomenė yra pakankamai informuota apie asmens duomenų apsaugą (4 procentiniais punktais daugiau nei ankstesniais metais). Šie rodikliai rodo, kad nuoseklus švietimas ir prevencija kuria brandesnę duomenų apsaugos kultūrą.

2025 m. rezultatai – tai visų VDAI darbuotojų įsitraukimo, pastangų ir atsakomybės pasekmė. Žvelgiant į ateitį, toliau bus ieškoma būdų, kaip žmonėms dar labiau palengvinti teisės į asmens duomenų apsaugą įgyvendinimą ir užtikrinti jų veiksmingą gynimą.

SANTRUMPOS

ADSP – asmens duomenų saugumo pažeidimas.

ADTAĮ – Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas.

BDAR – 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (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).

EDAV – ES valstybių narių asmens duomenų apsaugos priežiūros institucijas vienijanti Europos duomenų apsaugos valdyba yra nepriklausoma ES institucija, kuri padeda užtikrinti nuoseklų duomenų apsaugos taisyklių taikymą visoje ES.

ERĮ – Lietuvos Respublikos elektroninių ryšių įstatymas.

ES – Europos Sąjunga.

Teisėsaugos ADTAĮ – Lietuvos Respublikos asmens duomenų, tvarkomų nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas, bausmių vykdymo arba nacionalinio saugumo ar gynybos tikslais, teisinės apsaugos įstatymas.

VDAI – Valstybinė duomenų apsaugos inspekcija.

Vieno langelio procedūros (angl. *one-stop-shop*) – vieno langelio principu siekiama užtikrinti, kad organizacijos ir asmenys galėtų spręsti su asmens duomenų tvarkymu susijusius tarpvalstybinius klausimus su priežiūros institucija, įsikūrusia toje pačioje valstybėje narėje, kurioje yra jų pagrindinė buveinė (dažniausiai jų ES būstinė), taip pat, kad tokie klausimai galėtų būti nuosekliai sprendžiami visoje ES. O tai reiškia, kad priežiūros institucijos turi bendradarbiauti, kad suteiktų viena kitai susijusią informaciją ir savitarpio pagalbą, kai to prašoma. Kiekvienoje užklausoje dėl savitarpio pagalbos suteikimo turi būti pateikiama visa būtina informacija, pvz., užklausos tikslas ir motyvai. Paprastai kiekviena priežiūros institucija privalo atsakyti į užklausą nustatytais terminais.

VEIKLOS PRIORITETAI

VDAI įgyvendinama teisės į asmens duomenų apsaugą priežiūros sistema siekiama kurti pasitikėjimą Lietuvoje veikiančių duomenų valdytojų vykdomu asmens duomenų tvarkymu, kartu didinant visuomenės informuotumą apie galinčias kilti rizikas fizinių asmenų teisėms ir laisvėms.

Ekonominis ir socialinis gyvenimas nuolat kinta, sparčiai vystomos naujos technologijos. Su didesne skaitmenizacija atsiranda ir naujų rizikų teisei į asmens duomenų apsaugą bei kitoms teisėms ir laisvėms, todėl technologijų tobulėjimo nulemti pokyčiai turėtų būti orientuoti į naudą žmogui ir paremti pasitikėjimu.

Nustatydama veiklos prioritetus VDAI atsižvelgė ir į minėtus pokyčius visuomenės gyvenime, ir į Lietuvos Respublikos Vyriausybės programoje, patvirtintoje Lietuvos Respublikos Seimo 2024 m. gruodžio 12 d. nutarimu Nr. XV-54 „Dėl Devynioliktosios Lietuvos Respublikos Vyriausybės programos“, nustatytas valstybės veiklos kryptis, susijusias su dirbtinio intelekto (toliau – DI) teikiamų galimybių išnaudojimu, duomenų įveiklinimu, visuomenės skaitmeninių įgūdžių stiprinimu, sąlygų antriniam duomenų panaudojimui sudarymu ir pan.

2025 m. VDAI įgyvendino du numatytus veiklos prioritetus.

1. Stiprinti pažeidimų asmens duomenų apsaugos srityje prevenciją ir prisidėti prie pasitikėjimo viešuoju sektoriumi didinimo.

Siekdama stiprinti pažeidimų asmens duomenų apsaugos srityje prevenciją ir didinti pasitikėjimą viešuoju sektoriumi, VDAI daug dėmesio 2025 m. skyrė asmens duomenų tvarkymo veiklos dalyvių švietimui. Tik didinant duomenų valdytojų ir duomenų tvarkytojų bei duomenų apsaugos pareigūnų žinias, kompetenciją ir įgūdžius, įmanoma užtikrinti aukštesnį asmens duomenų apsaugos lygį (toliau – ADASL), o esant didesniam duomenų subjektų informuotumui – siekti veiksmingos jų teisių apsaugos. Planuota, kad šis rodiklis 2025 m. sieks 64 proc., apklausos duomenys rodo, kad rodiklis siekė 63 proc. ir nuo 2021 m. faktiškai padidėjo 3 proc. 2025 m. gyventojų pasitikėjimas įmonėmis bei įstaigomis asmens duomenų apsaugos srityje augo. Remiantis apklausa,

58 proc. **gyventojų mano, kad įmonės ir įstaigos Lietuvoje užtikrina teisę į duomenų apsaugą.**

(tai yra 6 procentiniais punktais daugiau nei 2024 m.). Taip pat augo gyventojų pasitikėjimas duomenų apsaugos išmanymu, nes 50 proc. respondentų teigia, kad žmonės yra informuoti apie asmens duomenų apsaugą (4 procentiniais punktais daugiau nei 2024 m.).

Duomenų apsaugos kultūros sklaidai itin svarbus bendradarbiavimas su kitomis institucijomis, asociacijomis ir kitais socialiniais partneriais, todėl VDAI deda pastangas, kad būtų kuriamos ir palaikomos įvairios bendradarbiavimo iniciatyvos. Kartu su socialiniais partneriais organizuoti seminarai, mokymai, konferencijos tikslinėms grupėms, kurių metu aptartos IT saugumo, kibernetinių grėsmių prevencijos, vaizdo stebėjimo, asmens duomenų saugumo ir kitos aktualios temos. Kelintus metus iš eilės VDAI, bendradarbiaudama su Nacionaliniu kibernetinio saugumo centru prie Krašto apsaugos ministerijos (toliau – NKSC) ir Lietuvos policija, prisideda prie kibernetinio saugumo pratybų organizavimo ir vykdymo. Duomenų apsaugos pareigūnams (toliau – DAP) surengti kasmetiniai nemokami nuotoliniai DAP mokymai, kurie buvo skirti ne tik Lietuvos DAP, tačiau ir organizacijų vadovams, asmens duomenų apsaugos profesionalams, IT specialistams ir visiems, kam kasdienėje veikloje tenka spręsti su asmens duomenų tvarkymu susijusias situacijas.

Įgyvendinant šį veiklos prioritetą, daug dėmesio skiriama stebėsenos procedūrai ir taikiam skundų išsprendimui. Nors 2025 m. taikiai išspręstų skundų šiek tiek sumažėjo, nuo 2022 m., kai pradėta taikyti ši praktika, tokių atvejų padaugėjo 65 proc.

Siekdama stiprinti pažeidimų prevenciją ir pateikti išsamesnės informacijos aktualiais asmens duomenų ir privatumo apsaugos klausimais didesnėms suinteresuotųjų asmenų grupėms, VDAI 2025 m. daug dėmesio skyrė metodinės informacijos rengimui, kuri yra naudinga tiek organizacijoms, tiek ir gyventojams. Iš viso parengta 18 metodinių priemonių: 8 DUK, 4 VDAI apibendrinimai ir 6 rekomendacijos.

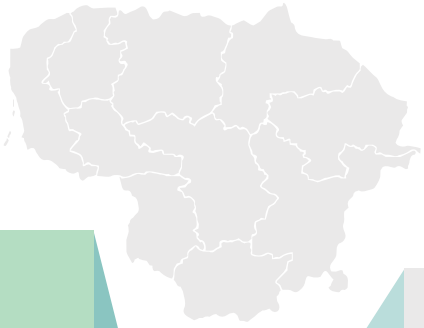
2. Stiprinti tarptautinį bendradarbiavimą asmens duomenų apsaugos srityje.

Siekdama stiprinti tarptautinį bendradarbiavimą asmens duomenų apsaugos srityje, VDAI vykdo aktyvią tarptautinę veiklą bei bendradarbiauja su kitų valstybių narių priežiūros institucijomis. Daugiausiai buvo dalyvauta EDAV pogrupių veikloje, kuriuose buvo rengiami ir derinami nuosekliam BDAR taikymui visoje ES svarbūs dokumentai, keičiamasi nuomonėmis su kitomis ES priežiūros institucijomis įvairiais praktikos formavimo klausimais. 2025 m. VDAI dalyvavo EDAV ir kitų ES institucijų bei tarptautinių organizacijų darbo grupių ir pogrupių iš viso 102 posėdžiuose ir kituose darbiniuose susitikimuose. VDAI bendradarbiauja su ES ir Europos ekonominės erdvės valstybių priežiūros institucijomis nagrinėjant skundus taikant nuoseklumo užtikrinimo mechanizmą. Per 2025 m. gauti 34 tarptautiniai skundai, kuriuose VDAI veikia kaip vadovaujanti priežiūros institucija. Per šį laikotarpį veikdama kaip vadovaujanti priežiūros institucija VDAI priėmė 28 sprendimus, kurie buvo derinami su susijusiomis priežiūros institucijomis.

Siekiant gilinti bendradarbiavimą ir keistis geriausia praktika, kasmet vyksta Baltijos šalių – Lietuvos, Latvijos ir Estijos – duomenų apsaugos institucijų susitikimai.

2025 m. rugsėjo 4–5 d. šis susitikimas vyko Vilniuje. Susitikimo metu aptarti praėjusių metų veiklos rezultatai, pasidalinta duomenų apsaugos reikalavimų taikymo praktika bei nuomonėmis, aptarti kiti aktualūs bendradarbiavimo klausimai.

KONTEKSTO ANALIZĖ



VDAI yra Lietuvos Respublikos Vyriausybės įstaiga, veikianti teisingumo veiklos srityje. Šiai sričiai 2021–2030 metų Nacionaliniame pažangos plane numatytas 8-asis strateginis tikslas – didinti teisinės sistemos ir viešojo valdymo veiksmingumą.

VDAI prisideda prie 2021–2030 metų plėtros programos valdytojos Lietuvos Respublikos teisingumo ministerijos teisingumo sistemos plėtros programos (toliau – Teisingumo sistemos plėtros programa) pažangos priemonės „Modernizuoti teisinės apsaugos procesus“ siekdama rezultato rodiklio – Asmens duomenų apsaugos sąlygų lygis (proc.).

2025 m. ADASL siekė 63 proc. ir nuo 2021 m. padidėjo 3 proc.

VDAI veiklos tikslas – užtikrinti pagarbą fizinių asmenų teisei į asmens duomenų apsaugą, nuoseklų asmens duomenų taisyklių taikymą ir prisidėti prie sąlygų sudarymo laisvam asmens duomenų judėjimui užtikrinti.

Įgyvendinant VDAI veiklos tikslą, siekta poveikio rodiklio – „Gyventojų pasitikėjimo valstybės institucijomis, kurios prižiūri, ar kitos įmonės ir įstaigos tinkamai užtikrina asmens duomenų apsaugą, didinimas, proc.“ 2025 m. gyventojų pasitikėjimas įmonėmis bei įstaigomis asmens duomenų apsaugos srityje šiek tiek augo. Lūkestis buvo pasiekti 55 proc. pasitikėjimo, tačiau remiantis apklausa, 56 proc. gyventojų pasitiki valstybės institucijomis, kurios prižiūri ar kitos įmonės ir įstaigos tinkamai užtikrina asmens duomenų apsaugą, t. y. 2 proc. daugiau nei 2024 m. (2024 m. – 54 proc.).

VDAI vykdo BDAR, Lietuvos Respublikos asmens duomenų, tvarkomų nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas, bausmių vykdymo arba nacionalinio saugumo ar gynybos tikslais, teisinės apsaugos įstatymo (toliau – Teisėsaugos ADTAĮ), Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo (toliau – ADTAĮ), jos kompetencijai priskirtų Lietuvos Respublikos elektroninių ryšių įstatymo (toliau – ERĮ) nuostatų taikymo priežiūrą.

Valstybės pažangos strategija „Lietuvos ateities vizija „Lietuva 2050“ kaip vieną iš valstybės tarnybos pažangos kriterijų numato ateities technologijų ir jų paskatintų pokyčių stebėseną. Numatoma, kad pažangiosios technologijos ir duomenys bus etiškai ir teisėtai integruoti į sprendimų priėmimo procesus.

ES priimtos iniciatyvos, susijusios su bendrosios skaitmeninės rinkos[1] ir DI vystymu (pavyzdžiui: Skaitmeninių paslaugų aktas, Duomenų aktas, DI aktas), pagrindiniai tikslai yra sukurti saugesnę skaitmeninę erdvę, kurioje užtikrinamos pagrindinės skaitmeninių paslaugų vartotojų teisės, ir sudaryti vienodas sąlygas inovacijoms, augimui ir konkurencingumui skatinti.

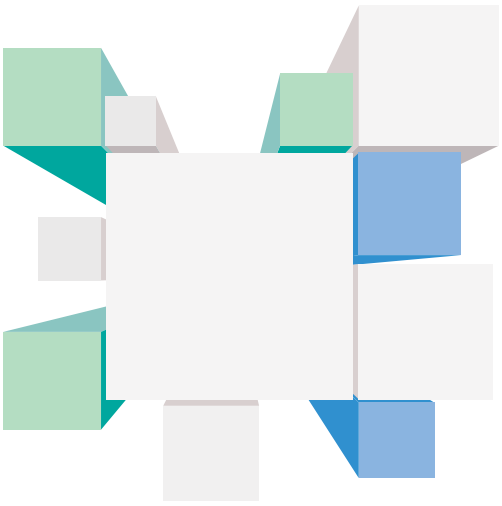
2024 m. birželio 13 d. Europos Parlamento ir Tarybos reglamentu (ES) 2024/1689, kuriuo nustatomos suderintos DI taisyklės ir iš dalies keičiami tam tikri Sąjungos teisėkūros procedūra priimti aktai (DI aktas) visoje ES sukurta patikimo ir į žmogų orientuoto DI bendroji rinka. Jo tikslas – skatinti inovacijas ir DI diegimą, kartu užtikrinant aukšto lygio sveikatos, saugos ir pagrindinių teisių, įskaitant demokratiją ir teisinę valstybę, apsaugą.

[1]https://www.europarl.europa.eu/factsheets/lt/sheet/43/visur-esanti-bendroji-skaitmenine-rinka#_ftnref1.

Paminėtina, kad 2025 m. Europos Komisija pateikė du Omnibus pasiūlymus dėl BDAR keitimo bei pateikė pasiūlymą dėl Europos Parlamento ir Tarybos reglamento, kuriuo iš dalies keičiami Reglamentai (ES) 2024/1689 ir (ES) 2018/1139, siekiant supaprastinti DI harmonizuotų taisyklių įgyvendinimą (toliau – Omnibusas dėl DI[2]).

Svarbu pažymėti, kad BDAR nuo 2016 m. tapo kertiniu ES teisės aktu, stiprinančiu asmens duomenų apsaugą ir pasitikėjimą tarpvalstybiniais duomenų srautais. Tačiau kintant ES skaitmeniniam reguliavimui, pastaraisiais metais akcentuotas poreikis supaprastinti reikalavimus ir mažinti administracinę naštą, kad Europa taptų konkurencingesnė. Pirmuoju Omnibusu[3] siekiama supaprastinti ES taisykles ir sumažinti administracinę naštą, t. y. siekiama suteikti daugiau lankstumo pasirinkti tinkamiausią atitikties BDAR užtikrinimo būdą. Tuo tarpu antruoju, Skaitmeniniu Omnibusu[4], siekiama ne tik palengvinti BDAR nuostatų laikymąsi, visų pirma labai mažoms, mažosioms ir vidutinėms organizacijoms, tačiau tuo pačiu siekiama išlaikyti nuolatinę ES politikos kryptį: išsaugoti pagrindinius BDAR principus, užtikrinti aiškesnes, praktiškesnes ir rizika pagrįstas reglamento taikymo gaires bei nesumažinti fizinio asmens (duomenų subjekto) asmens duomenų apsaugos lygio.

VDAI taip pat yra viena iš institucijų, įgyvendinančių kibernetinio saugumo politiką. Įgyvendindama šią politiką VDAI dalyvauja Kibernetinio saugumo tarybos veikloje, prisideda prie kibernetinio saugumo pratybų, kartu su kitomis atsakingomis institucijomis rengia kasmetinę Nacionalinę kibernetinio saugumo būklės ataskaitą. Kibernetinis saugumas tiesiogiai susijęs su asmens duomenų saugumo užtikrinimu ir VDAI atliekama asmens duomenų saugumo pažeidimų (toliau – ADSP) nagrinėjimo veikla, kai tiriant ADSP prireikus bendradarbiaujama ir su NKSC.



[2]2025 m. lapkričio 19 d. Europos Komisijos Pasiūlymas dėl Europos Parlamento ir Tarybos reglamento, kuriuo iš dalies keičiami Reglamentai (ES) 2024/1689 ir (ES) 2018/1139, siekiant supaprastinti dirbtinio intelekto harmonizuotų taisyklių įgyvendinimą (toliau – Omnibusas dėl DI).

[3]2025 m. gegužės 21 d. Europos Komisijos Pasiūlymas dėl Europos Parlamento ir Tarybos reglamento, kuriuo iš dalies keičiami reglamentai (ES) 2016/679, (ES) 2016/1036, (ES) 2016/1037, (ES) 2017/1129, (ES) 2023/1542 ir (ES) 2024/573, kiek tai susiję su tam tikrų mažoms ir vidutinėms įmonėms taikomų palengvinimo (švelninamųjų) priemonių taikymo išplėtimu mažoms vidutinės kapitalizacijos įmonėms ir tolesnėmis supaprastinimo priemonėmis (toliau – Pirmasis Omnibusas).

[4]2025 m. lapkričio 19 d. Europos Komisijos Pasiūlymas dėl Europos Parlamento ir Tarybos reglamento, kuriuo iš dalies keičiami reglamentai (ES) 2016/679 [Bendrasis duomenų apsaugos reglamentas / BDAR], (ES) 2018/1724, (ES) 2018/1725, (ES) 2023/2854 (Duomenų aktas), ir direktyvos 2002/58/EB, (ES) 2022/2555 ir (ES) 2022/2557, dėl skaitmeninės teisės aktų sistemos supaprastinimo panaikinant Reglamentus (ES) 2018/1807, (ES) 2019/1150, (ES) 2022/868 ir direktyvą (ES) 2019/1024 (Atvirų duomenų direktyva) (Skaitmeninis Omnibusas), projektą (toliau – Skaitmeninis Omnibusas).

SKIRTAS BIUDŽETAS IR PERSONALO KLAUSIMAI

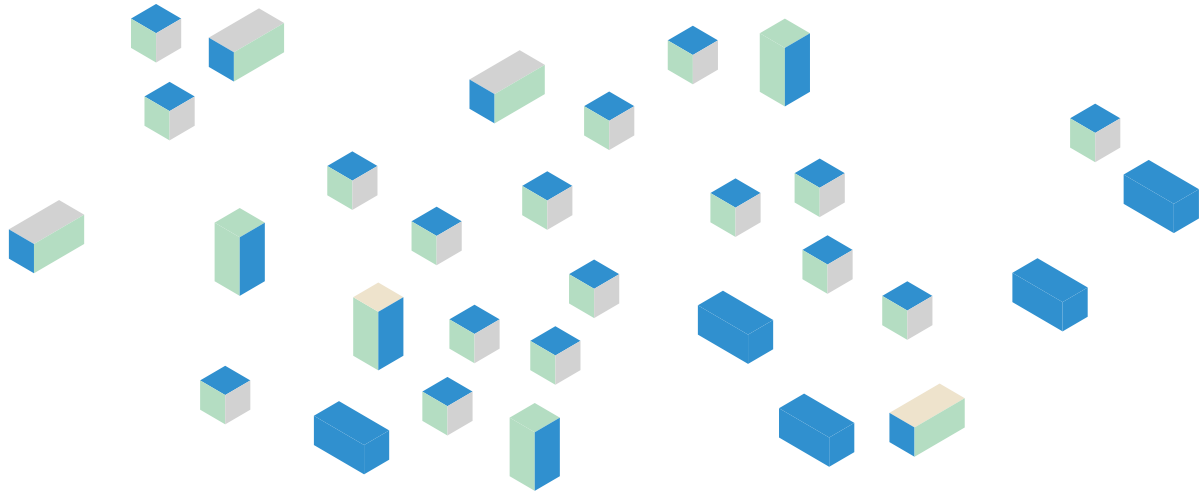
VDAI yra patrauklus darbdavys, suteikiantis galimybę įgyti aukštą kvalifikaciją perspektyvioje srityje, tačiau susiduria su didesnėmis personalo pritraukimo problemomis, nei įprasta kitose valstybės institucijose. Perspektyva įgyti aukštą kvalifikaciją yra nepakankama pritraukti naujus darbuotojus, turi būti sudaryta ir konkurencinga darbo apmokėjimo sistema. Šis poreikis atsižvelgiant į VDAI biudžetą yra patenkinamas tik iš dalies, net ir pritaikius papildomas motyvavimo priemones.

1 lentelė

Finansai ir žmogiškieji ištekliai 2023–2025 m.

VEIKLA	2023 m.	2024 m.	2025 m.
Biudžetas (tūkst. Eur)	1 592,0	1 727,0	2 198,0
iš jo darbo užmokesčiui (tūkst. Eur)	1 318,0	1 463,0	1 892,0
Pareigybių skaičius	52	46	54*

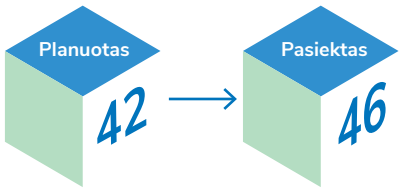
*Atsižvelgiant į gautus papildomus finansinius išteklius 2025 m. pareigybių skaičius padidintas



2025 m. paskelbti 32 konkursai į laisvas karjeros valstybės tarnautojo pareigas, iš kurių įvyko 16. Naujų darbuotojų pritraukimui skirtas itin didelis dėmesys bei išplėstos paieškos galimybės: ieškota galimų kandidatų, kurie galėtų prisijungti prie kolektyvo tarnybinio kaitumo būdu, organizuoti 5 atvirų durų dienų renginiai, informacija apie konkursus skelbiama ne tik interneto svetainėje ir socialiniuose tinkluose, bet ir darbo pasiūlos portaluose, siunčiama į aukštąsias mokyklas.

Siekiant ne tik pritraukti, bet ir išlaikyti profesionalius specialistus, didelis dėmesys skiriamas darbuotojų kvalifikacijos tobulinimui.

2025 m. planuotas vertinimo kriterijus dėl VDAI darbuotojų, dalyvavusių kvalifikacijos kėlimo kursuose ir mokymuose, – 42 vnt., pasiektas – 46 vnt.



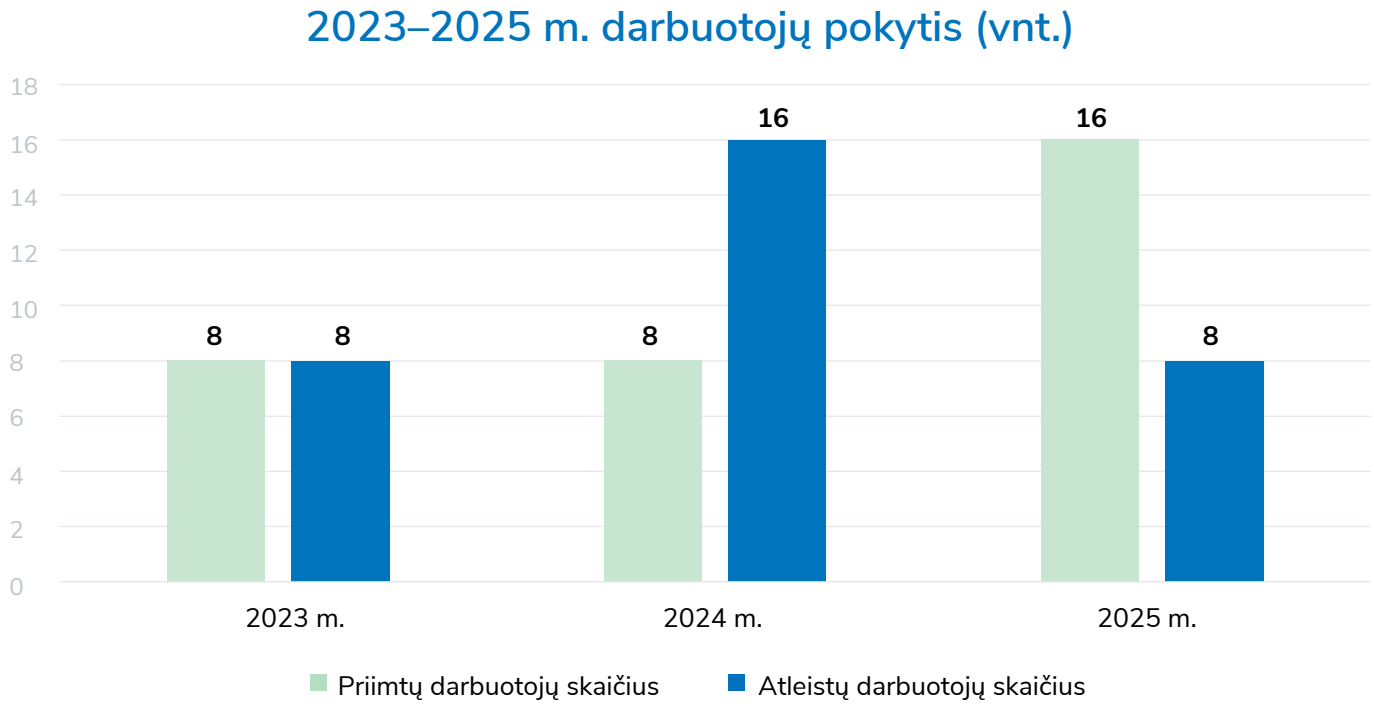
Darbuotojai dalyvavo renginiuose, kuriuose gilino komunikacijos kompetencijas, profesinės etikos, korupcijos prevencijos, skaitmeninės kompetencijos ir kibernetinio saugumo žinias. Specialistai taip pat mokėsi efektyvaus bendravimo su klientais, sudėtingų aptarnavimo situacijų valdymo ir klientų aptarnavimo psichologinių aspektų.

Siekiant kelti darbuotojų kompetenciją asmens duomenų apsaugos srityje bei dalintis gerąja patirtimi su kitomis ES valstybėmis, pagal stažuočių programą 2025 m. 4 savaitėms buvo priimti du darbuotojai iš Vokietijos. Programos tikslas – stiprinti duomenų apsaugos įgūdžius bei gerinti BDAR nuostatų įgyvendinimo ir vykdymo užtikrinimą, siekiant šiuos gebėjimus tobulinti per praktinę patirtį.

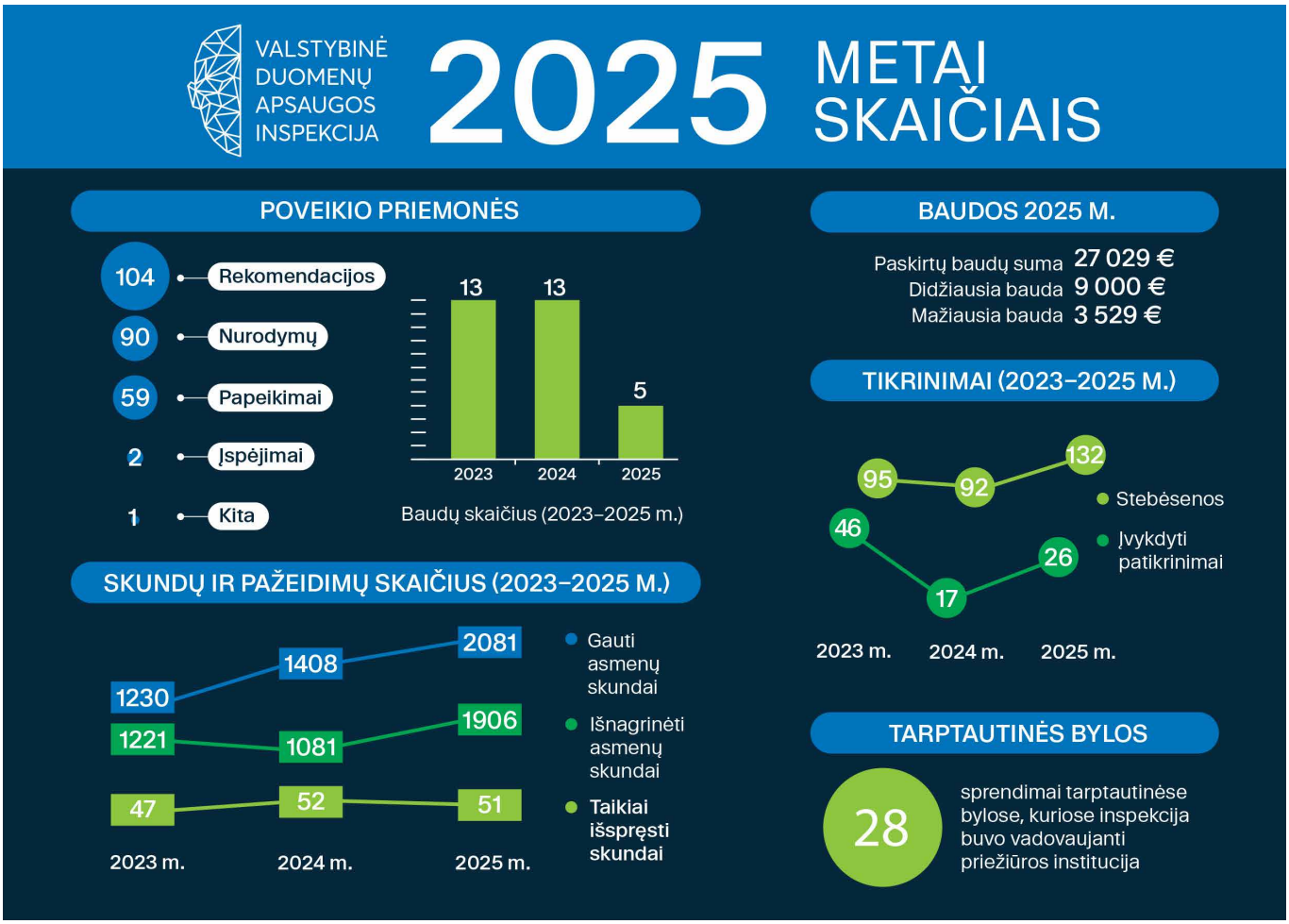
Personalo tendencijos darbo rinkoje rodo, kad duomenų apsaugos specialistai išlieka itin paklausūs. Dėl šios priežasties išlieka didelė personalo kaitos rizika.

2025 m. iš viso priimta 14 valstybės tarnautojų ir 2 darbuotojai, dirbantys pagal darbo sutartį. Atleisti 8 valstybės tarnautojai.

1 grafikas



ŪKIO SUBJEKTŲ IR KITŲ DUOMENŲ VALDYTOJŲ PRIEŽIŪRA



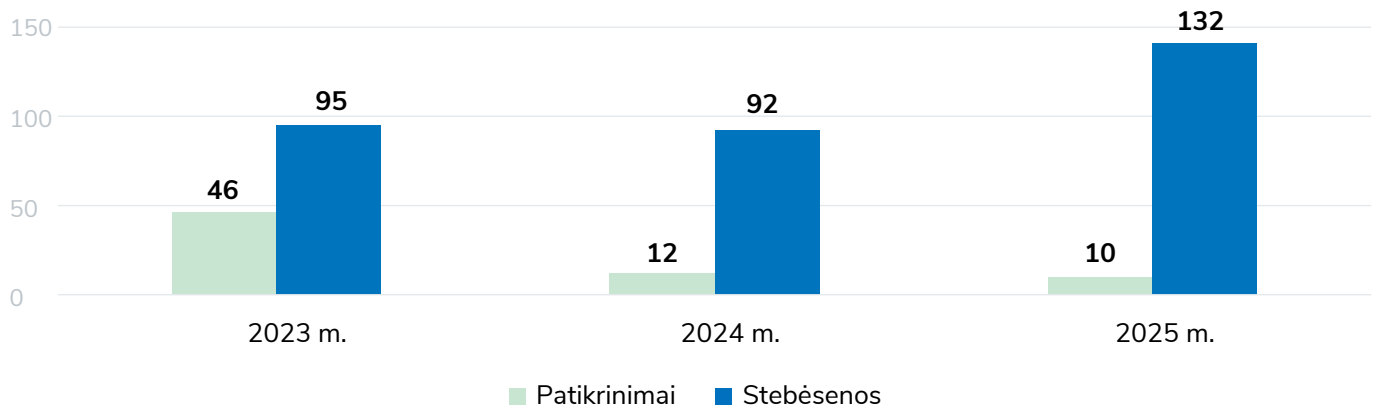
Patikrinimai ir stebėsena

2025 m. VDAI atliko 16 planinių patikrinimų (2024 m. – 12, 2023 m. – 46). Pasitaikė atvejų, kai reikėjo atlikti ir neplaninius patikrinimus – jų buvo atlikta 10.

2025 m. neplaniniai patikrinimai buvo pradedami gavus informaciją apie galimus ADSP ir siekiant operatyviai įvertinti galimas rizikas bei užtikrinti teisėtą ir saugų duomenų tvarkymą.

2 grafikas

2023–2025 m. patikrinimų ir stebėsenų skaičiaus pasiskirstymas (vnt.)



VDAI pagal BDAR 57 str. 1 dalies a punktą turi teisę atlikti BDAR taikymo stebėseną. Jos metu atliekama pirminė tam tikros asmens duomenų tvarkymo operacijos analizė ir pateikiami pastebėjimai, rekomendacijos dėl tinkamo teisės aktų reikalavimų įgyvendinimo.

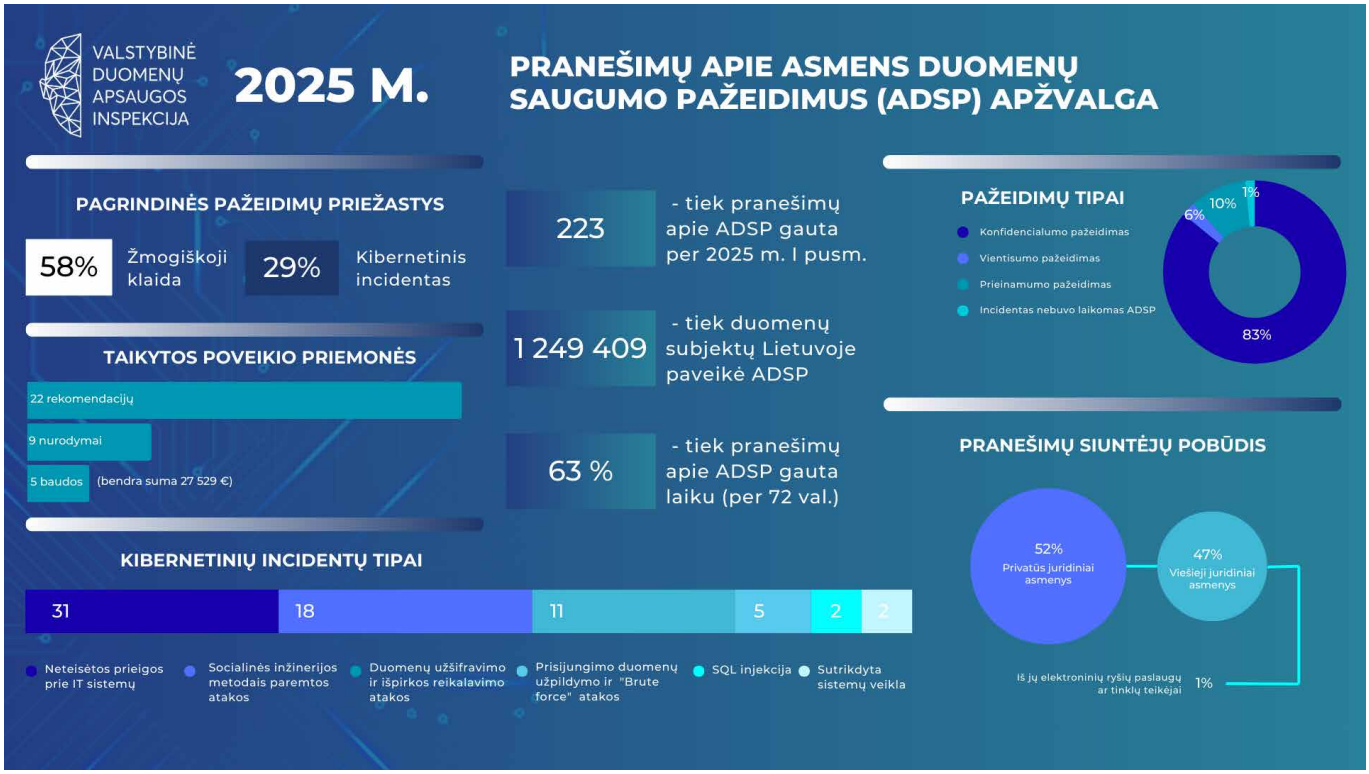
2022 m.

Tokia veikla pradėta taikyti 2022 m. ir leidžia paprasčiau reaguoti į galimus ADSP.

Jeigu po stebėsenos veiksmų paaiškėtų, kad organizacijos savanoriškai nepašalino veiklos trūkumų ir vis dar gali būti BDAR pažeidimų, VDAI gali pradėti patikrinimą savo iniciatyva ir taikyti poveikio priemones.

2025 m. stebėsenos veiksmai taikyti 132 atvejais. Stebėsena dažniausiai buvo susijusi su galimais pažeidimais tiesioginės rinkodaros srityje ir jos vykdymo priemonėmis (el. pašto naudojimu, sekimo pikseliais, slapukais), galimais ADSP, vaizdo stebėjimu. Pavieniais atvejais kreiptasi dėl galimo perteklinio duomenų rinkimo, duomenų saugumo, asmens kodo bei tapatybės dokumentų kopijų tvarkymo, duomenų gavimo iš registrų apimties.

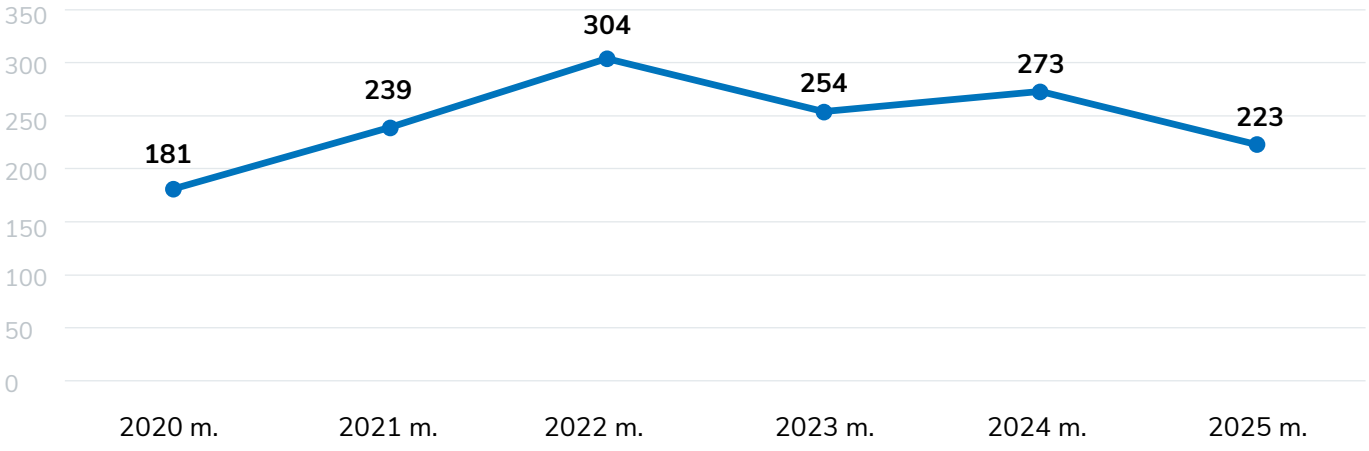
Asmens duomenų saugumo pažeidimai



Įvykus ADSP, organizacijos turi imtis pažeidimo valdymo veiksmų, taip pat įgyvendinti priemones, skirtas pažeidimui sustabdyti bei užtikrinti, kad pažeidimai nesikartotų ateityje. Visais atvejais organizacijos turi tokius pažeidimus ištirti, dokumentuoti ir laikytis kitų BDAR nustatytų procedūrų. Nustačius, kad dėl įvykusio pažeidimo kyla pavojus fizinių asmenų teisėms ir laisvėms, privaloma apie tai pranešti VDAI ne vėliau kaip per 72 valandas. VDAI gautus pranešimus apie ADSP įvertina ir, jei reikia, atlieka tyrimą.

3 grafikas

2020–2025 m. gauti pranešimai dėl įvykusių ADSP (vnt.)



2025 m. 63 proc. duomenų valdytojų apie įvykusį ADSP pranešė ne vėliau kaip per 72 val., 37 proc. – vėliau kaip per 72 val.

Palyginti su ankstesnių metų duomenimis, duomenų valdytojai dažniau teikia pranešimus pavėluotai.

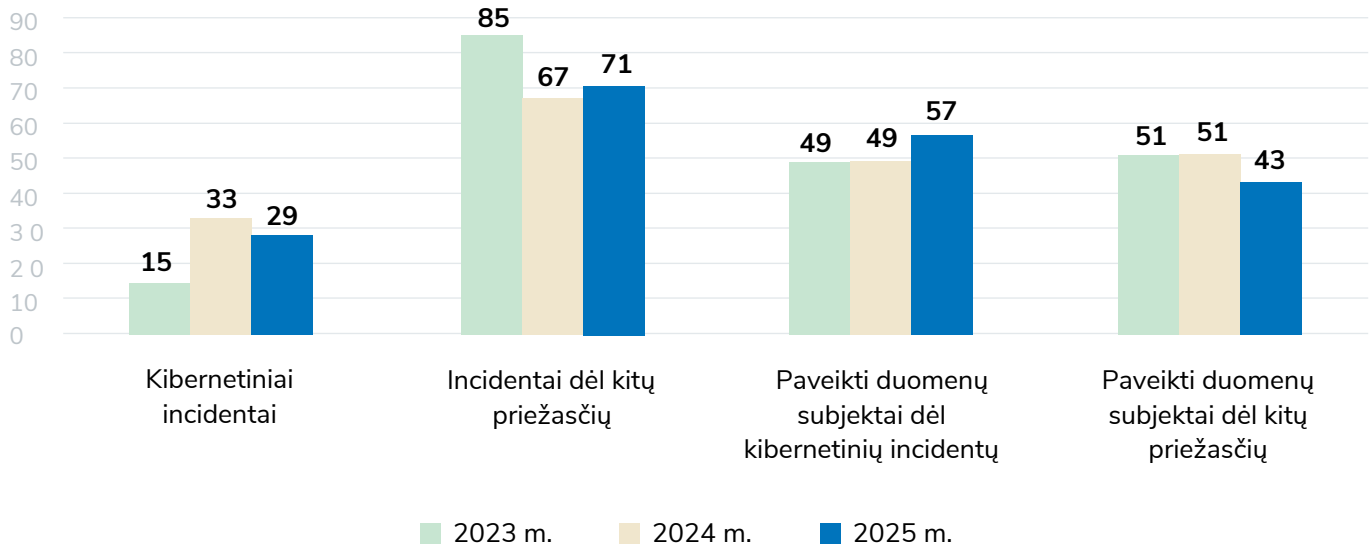
(2024 m. 79 proc. duomenų valdytojų apie įvykusį ADSP pranešė ne vėliau kaip per 72 val., 21 proc. – vėliau kaip per 72 val.), kartais nenurodo vėlavimo priežasčių.

2025 m. VDAI gavo 223 pranešimus apie ADSP, Lietuvoje paveiktų duomenų subjektų skaičius – 1 249 409. Palyginti su ankstesnių metų duomenimis, 2025 m. VDAI gavo mažiau pranešimų apie ADSP negu 2024 m. (2024 m. VDAI gautų pranešimų apie ADSP skaičius – 273). Taip pat beveik 200 tūkst. sumažėjo Lietuvoje paveiktų duomenų subjektų skaičius (2024 m. Lietuvoje paveiktų duomenų subjektų skaičius – 1 467 368).

Pagal ADSP pobūdį Lietuvoje vyrauja konfidencialumo pažeidimai, kurių skaičius per 2025 m. sudarė net 83 proc. visų atvejų (2024 m. sudarė 87 proc.), 6 proc. atvejų sudarė vientisumo pažeidimai (2024 m. sudarė 6 proc.), 10 proc. atvejų – prieinamumo pažeidimai (2024 m. sudarė 6 proc.) ir 1 proc. atvejų incidentas nebuvo laikomas ADSP (neatitiko sąvokos) (2024 m. taip pat sudarė 1 proc.).

4 grafikas

2023–2025 m. su incidentais susijusių duomenų palyginimas, proc.



VDAI, išanalizavusi 2025 m. gautus pranešimus apie ADSP, nustatė, kad 29 proc. (69) ADSP įvyko dėl kibernetinių incidentų, 58 proc. ADSP įvyko dėl žmogiškosios klaidos, 13 proc. dėl kitų priežasčių (dėl įvairių IT sistemų trikdžių, netinkamai atliktų programavimo darbų, neatliktų sistemų testavimo ir kt.).

VDAI, nustačiusi, kad yra netinkamai užtikrinamas duomenų saugumas, 2025 m. teikė 9 nurodymus duomenų valdytojams arba duomenų tvarkytojams suderinti duomenų tvarkymo operacijas su BDAR nuostatomis, 22 rekomendacijas ir skyrė 5 baudas (didžiausia – 9 tūkst. eurų, mažiausia – 3 529 eurai.

1 atvejis

2025 m. sausio mėn. viešajai įstaigai skirta 9 tūkst. eurų baudą. Nustatyta, kad ADSP įvyko dėl įdiegtų duomenų praradimo prevencijos priemonių netinkamo testavimo atlikimo ir daromos nepagrįstos prielaidos, kad scenarijui neatitikus nustatytos taisyklės, priemonė suveiks. Tačiau duomenų praradimo prevencijos priemonė nesuveikė, dėl to 292 asmenims buvo išsiųstas el. laiškas su pridėtu *Excel* dokumentu, kuriame buvo 29 636 duomenų subjektų asmens duomenys, įskaitant specialių kategorijų asmens duomenis.

2 atvejis

2025 m. vasario mėn. viešajai įstaigai skirta 3 529 eurų bauda. Nustatyta, kad įvyko kibernetinė ataka, kurios metu piktavalis įsilaužė į vidinį tinklą ir užšifravo 120 duomenų subjektų duomenis, įskaitant ir specialių kategorijų duomenis. Šiuo atveju duomenų valdytojas nebuvo dokumentavęs ir apibrėžęs vaidmenų ir atsakomybių, neturėjo prieigos valdymo politikos ir tinkamai nevaldė prieigos teisių. Taip pat nebuvo užtikrinta prieigų kontrolė ir autentifikavimas, neįgyvendinta kompiuterinių darbo vietų techninių įrašų registravimo ir stebėsenos sistema, o naudotojams kompiuterinėse darbo vietose buvo suteiktos administratoriaus teisės.

Išankstinės konsultacijos

BDAR numatyta, kad duomenų valdytojas, prieš pradėdamas tvarkyti asmens duomenis, kreipiasi į VDAI išankstinės konsultacijos, kai atliktame poveikio duomenų apsaugai vertinime nurodyta, kad tvarkant asmens duomenis kiltų didelis pavojus fizinių asmenų teisėms ir laisvėms, jei duomenų valdytojas nesiimtų priemonių pavojui sumažinti. Savo apimtimi ši procedūra prilygsta tyrimui, ji gali trukti net iki 12 savaičių.

2025 m. dėl išankstinės konsultacijos suteikimo į VDAI kreipėsi 2 duomenų valdytojai – savivaldybės valdoma viešoji įstaiga ir valstybinė įstaiga. Abiem atvejais kreiptasi dėl planuojamo vykdyti vaizdo ir garso duomenų tvarkymo. Vienu atveju įstaiga ketino įrengti kameras darbuotojų poilsio zonoje remdamasi BDAR 6 str. 1 dalies f punktu, kitu – įstaiga ketino vykdydama jai pavestas viešosios valdžios funkcijas naudoti mobiliąsias vaizdo stebėjimo ir garso įrašymo priemones remdamasi BDAR 6 str. 1 dalies e punktu. VDAI nustačius, kad šiomis duomenų tvarkymo operacijomis gali būti pažeistos BDAR nuostatos, duomenų valdytojams teikti nurodymai ir rekomendacijos. Pirmu atveju rekomenduota atsisakyti kamerų poilsio zonoje ir ieškoti kitų, mažiau darbuotojų privatumą ribojančių turto apsaugos priemonių (pvz.: spintelių užraktų, vidaus taisyklių griežtinimo, darbuotojų sąmoningumo didinimo ir pan.). Antruoju rekomenduota aiškiai ir konkrečiai nustatyti atvejus, kuriems esant patikrinimų metu būtų tvarkomi garso ir (ar) vaizdo duomenys, iš naujo įsivertinti tokio tvarkymo teisėtumą bei proporcingumą ir duomenų saugojimo terminą bei jo pratęsimo aplinkybes nustatyti laikantis duomenų kiekio mažinimo ir saugojimo trukmės apribojimo principų.

Skundų nagrinėjimas

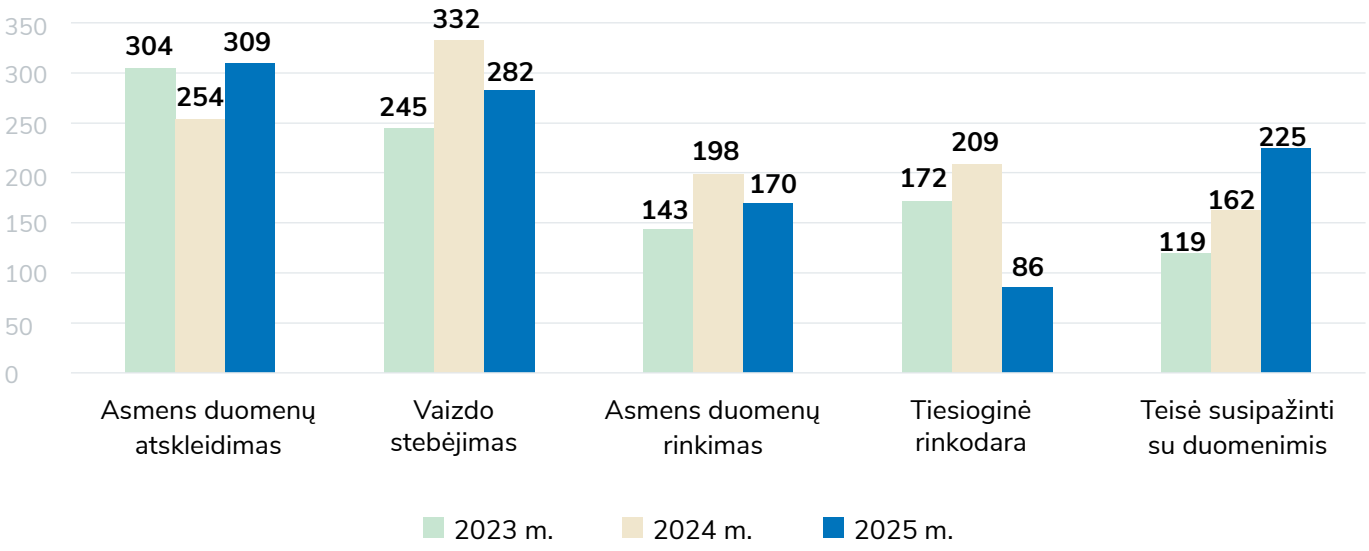
Didelę VDAI veiklos dalį sudaro asmenų skundų nagrinėjimo veikla. 2025 m. gautas 2081 skundas ir, palyginti su 2024 m., kai buvo gauti 1 408 skundai, jų skaičius padidėjo 48 proc.

Skundų skaičius padidėjo 48 proc.

Palyginus trejų metų laikotarpį, matyti, kad gaunamų skundų populiariausios sritys lieka tos pačios: asmens duomenų atskleidimas, vaizdo stebėjimas, tiesioginė rinkodara, asmens duomenų rinkimas, teisė susipažinti su duomenimis. Pastebima tendencija, kad žymiai padaugėjo skundų dėl teisės būti pamirštam – 2025 m. gauti 157 skundai, 2024 m. – 108 (padaugėjo 45 proc.).

5 grafikas

2023–2025 m. sritys, dėl kurių gaunamas didžiausias asmenų skundų skaičius (vnt.)



Daugiausia duomenų subjektų 2025 m. skundėsi dėl asmens duomenų atskleidimo, dėl šios teisės netinkamo įgyvendinimo gauti 309 skundai (2024 m. – 162). Didelę skundų dalį sudarė skundai dėl vaizdo stebėjimo – 282 (2024 m. – 332), asmens duomenų atskleidimo – 309 (2024 m. – 254, teisės susipažinti su duomenimis pažeidimų – 225 (2024 m. – 162).

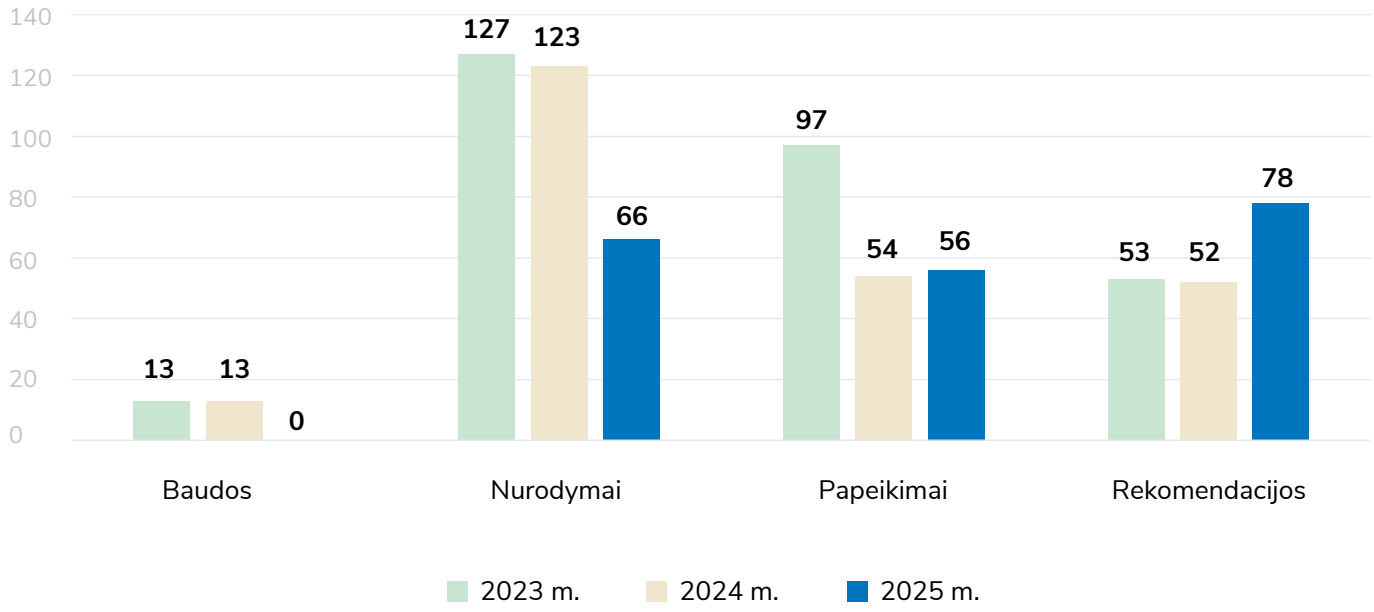
Taikytos poveikio priemonės

VDAI dėl BDAR ir kitų asmens duomenų apsaugos pažeidimų gali imtis įvairių taisomųjų veiksmų, priklausomai nuo konkretaus atvejo aplinkybių, pavyzdžiui, įspėti, pareikšti papeikimą, teikti nurodymus, apriboti arba uždrausti duomenų tvarkymą, skirti administracinę baudą, kuri, priklausomai nuo pažeidimo, gali siekti iki 2 ar 4 proc. ankstesnių finansinių metų bendros metinės pasaulinės apyvartos, arba iki 10 mln. ar 20 mln. EUR. VDAI gali taikyti šias poveikio priemones atlikusi planinį patikrinimą, išnagrinėjusi gautą skundą arba atlikusi tyrimą dėl įvykusio ADSP.

2025 m. VDAI, nustačiusi pažeidimų, organizacijoms teikė 66 nurodymus, 56 papeikimus, 78 rekomendacijas, skyrė 2 įspėjimus. Baudų išnagrinėjus asmenų skundus nebuvo skirta.

6 grafikas

2023–2025 m. taikytų poveikio priemonių skaičius (vnt.)



Reikšmingi VDAI sprendimai

Siekdama veiklos viešumo ir formuojamos praktikos sklaidos, nuo 2025 m. priimtus sprendimus VDAI skelbia interneto svetainėje. Toliau pateikiama keletas išskirtinų atvejų, kai VDAI ėmėsi taisomųjų veiksmų dėl netinkamo asmens duomenų tvarkymo.

1 atvejis

VDAI gavo pareiškėjo skundą dėl Savivaldybės administracijos veiksmų daugetą kartų tikrinant (peržiūrint) pareiškėjui nuosavybės teise priklausantį turtą Nekilnojamojo turto registre (toliau – NTR), nors pareiškėjas su skundžiamu asmeniu jokių sąsajų neturi. Savivaldybės administracija nurodė, kad vykdydama jai priskirtas funkcijas gavo standartinius NTR išrašus, kuriuose pateikti pareiškėjo duomenys jai buvo nereikalingi, todėl jų net neperžiūrėjo.

VDAI padarė išvadą, kad Savivaldybės administracija neįrodė, kad atlikdama daugkartines paieškas NTR ir gaudama NTR išrašus su pareiškėjo asmens duomenimis (vardas ir pavardė, asmens kodas, žemės sklypo (NTR objekto) identifikaciniai duomenys, žemės sklypo adresas, nuosavybės teisės į žemės sklypą dalis ir kt.), pareiškėjo asmens duomenis tvarkė teisėtai, todėl sprendė, kad skundžiamo asmens veiksmai neatitiko nė vienos BDAR 6 str. 1 dalyje nurodytos teisėto tvarkymo sąlygos, atitinkamai skundžiamas asmuo savo veiksmais pažeidė BDAR 5 str. 1 dalies a punkte nustatytą teisėtumo principą. VDAI nevertino skundžiamo asmens veiksmų pagal BDAR 5 str. 1 dalies c punktą, kadangi pati Savivaldybės administracija pripažino, kad vykdant NTR paieškas jos nustatytais tikslais pareiškėjo asmens duomenų tvarkymas jai apskritai nebuvo būtinas.

Savivaldybės administracijai pateiktas nurodymas – užtikrinti, kad vykdant funkcijas, kurių vykdymui yra būtina gauti duomenis iš NTR, tačiau nėra būtina tvarkyti asmens duomenų, asmens duomenys nebūtų tvarkomi, įskaitant asmens duomenų išgavą. Taip pat nuspręsta VĮ Registrų centro atžvilgiu atlikti stebėsenos veiksmus dėl BDAR 25 str. nuostatų įgyvendinimo. Šie veiksmai siejami su sprendime nustatyta aplinkybe, kad duomenų gavėjams pagal sudarytas sutartis teikiami standartiniai NTR išrašai apima ne tik duomenis apie nekilnojamojo turto objektą, bet ir visų daiktinės teisės turėtojų asmens duomenis, nors jie ne visada yra būtini savivaldybių funkcijoms vykdyti. VDAI konstatavo, kad yra būtina įgyvendinti pritaikytosios duomenų apsaugos principą ir sudaryti galimybes gauti tik su nekilnojamojo turto objektu susijusius duomenis (be savininkų asmens duomenų).

2 atvejis

Pareiškėja – transporto priemonės valdytoja – pateikė skundą dėl to, kad Lietuvos techninės apžiūros įmonių asociacija (toliau – Asociacija) pagal duomenų teikimo sutartį trečiajai šaliai perdavė jos automobilio techninės apžiūros ir ridos duomenis, kurie buvo panaudoti mokamoms transporto priemonės istorijos ataskaitoms sudaryti. Pareiškėja nurodė, kad tokie duomenys leidžia ją identifikuoti ir daro poveikį jos interesams.

Asociacija teigė, kad perduodami duomenys nėra asmens duomenys, nes tai tik pseudonimizuotu būdu (VINH) perduodami transporto priemonės techniniai duomenys.

VDAI, remdamasi ES Teisingumo Teismo 2025-09-04 sprendimu byloje Nr. C-413/23, vertino, ar pagal sutartį perduodami transporto priemonės techninės apžiūros ir ridos duomenys laikytini asmens duomenimis. Minėtame sprendime teismas konstatavo, kad jeigu negalima atmesti galimybės, kad tretieji asmenys galės pagrįstai priskirti duomenis, kuriems suteiktas pseudonimas, duomenų subjektui naudodamiesi tokiomis priemonėmis, kaip pavyzdžiui, sutikrindami juos su kitais turimais duomenimis, duomenų subjektas turi būti laikomas asmeniu, kurio tapatybę galima nustatyti, tiek dėl šio perdavimo, tiek dėl bet kokio vėlesnio šių trečiųjų asmenų atliekamo šių duomenų tvarkymo.

Šiuo atveju Asociacija nurodė, kad tvarko vairuotojo pažymėjimo arba asmens tapatybę patvirtinančio dokumento numerį, kas įrodo, kad Asociacija turi papildomos informacijos, leidžiančios su transporto priemone susijusią informaciją priskirti fiziniam asmeniui – transporto priemonės savininkui ar valdytojui. Be to, Asociacija nurodė, kad sutartyje yra nustatyta, kad trečiasis asmuo gautus duomenis naudos tam, kad sudarytų ir pardavinėtų transporto priemonių istorijos ataskaitas savo platformoje; kad šios ataskaitos, be kita ko, gali apimti techninių patikrų istoriją, nuosavybės istoriją, pranešimus apie nelaimingus atsitikimus ar žalą ir kitus atitinkamus istorinius duomenis.

VDAI sprendime pažymėjo, kad pagal identifikatorius, tokius kaip VIN ar asmens dokumento duomenis, transporto priemonė ir jos istorija gali būti priskirti konkrečiam duomenų subjektui, todėl, nepaisant pseudonimizavimo, trečiajai šaliai perduodami duomenys priskirtini asmens duomenų kategorijai.

VDAI konstatavo, kad pareiškėjos asmens duomenų perdavimas trečiajai šaliai buvo neteisėtas ir pažeidė BDAR 5 straipsnio 1 dalies a punkte įtvirtintą teisėtumo principą. Asociacijai teiktas nurodymas nedelsiant nutraukti su pareiškėja siejamų duomenų teikimą bendrovei, iki kol duomenų tvarkymas bus suderintas su BDAR 6 str. 1 dalies reikalavimais.

3 atvejis

Inspekcija gavo pareiškėjų fizinių asmenų skundus dėl draudimo brokerių bendrovės ir dviejų draudimo bendrovių veiksmų tvarkant asmens duomenis, t. y. dėl to, kad draudimo brokerių bendrovė perdavė pareiškėjų asmens duomenis draudimo bendrovėms, kad šios pateiktų draudimo pasiūlymus, o pastarosios tikrino pareiškėjų kredito reitingą trečiosios šalies duomenų bazėje.

Draudimo brokerių bendrovė teigė, kad siekdama tinkamai suteikti paslaugas, privalo perduoti surinktus duomenis draudimo bendrovėms, priešingu atveju ji, kaip draudimo tarpininkas, neturėtų galimybės suteikti paslaugų taip, kaip jos apibrėžtos Draudimo įstatyme. Atsižvelgdama į tai, VDAI vertino, kad draudimo brokerių bendrovė asmens duomenų tvarkymo veiksmus grindžia BDAR 6 str. 1 dalies c punktu (teisine prievole). VDAI nustatė, kad teisės aktai numato draudimo produktų platintojui pareigą informuoti draudėją apie įprastinės draudimo sutarties termino pabaigą ir apie pareigą apdrausti transporto priemonę, tačiau nenustato pareigos rengti, siųsti draudimo bendrovių pasiūlymus ar perduoti draudėjų asmens duomenis draudimo bendrovėms tokiems pasiūlymams teikti. Atitinkamai, VDAI sprendė, kad toks asmens duomenų perdavimas negali būti grindžiamas teisine prievole, t. y. BDAR 6 str. 1 dalies c punkto pagrindu, ir konstatavo BDAR 5 str. 1 dalies a punkte įtvirtinto teisėtumo principo bei BDAR 6 str. 1 dalies nuostatų pažeidimą.

Draudimo bendrovės teigė, kad asmenų kreditingumo reitingą tikrino teisėto intereso pagrindu (BDAR 6 str. 1 dalies f punktas), siekiant nustatyti įprastinės transporto priemonių valdytojų civilinės atsakomybės privalomojo draudimo kainą. VDAI nusprendė, kad nagrinėjamu atveju kredito reitingo duomenų tvarkymas negali būti grindžiamas BDAR 6 str. 1 dalies f punktu, nes nebuvo pateikta duomenų ar objektyvių vertinimų, pagrindžiančių duomenų tvarkymo būtinumą bei teisėtų interesų pusiausvyros egzistavimą.

Viena draudimo bendrovė taip pat nurodė, kad asmenų (draudėjų) kredito reitingo duomenys tvarkomi vadovaujantis BDAR 6 str. 1 dalies b punktu – draudimo sutarties sudarymo (arba pasiūlymo sudaryti sutartį) tikslu. Šiuo atveju VDAI nustatė, kad draudimo bendrovė neturėjo jokių sutarčių su pareiškėjais, taip pat neturėjo pareiškėjų prašymo sudaryti tokią sutartį, todėl BDAR 6 str. 1 dalies b punktas netaikytinas.

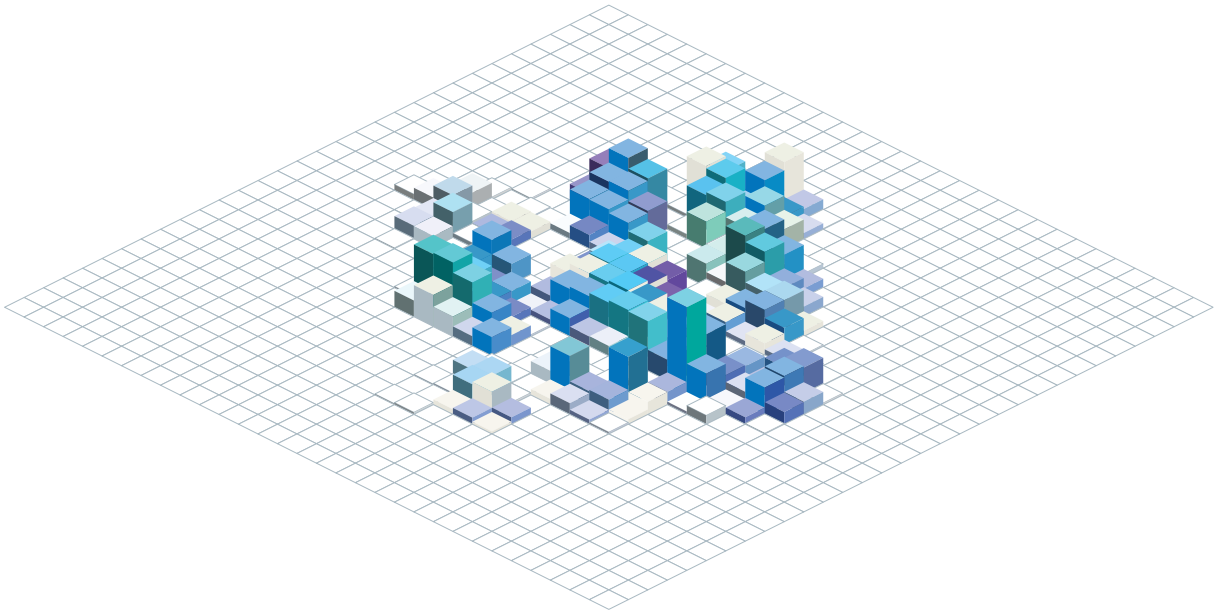
VDAI taip pat konstatavo, kad draudimo bendrovės negali teisėtai tvarkyti asmens duomenų, kurie joms buvo perduoti neteisėtai, net jeigu jų nurodyta teisėto tvarkymo sąlyga būtų hipotetiškai tinkama. Pagal bendrąjį teisės principą iš ne teisės negali atsirasti teisė (lot. *ex injuria jus non oritur*), todėl draudimo bendrovių atliktas pareiškėjų duomenų tikrinimas trečiosios šalies valdomoje duomenų bazėje negali būti laikomas teisėtu jau vien dėl neteisėto duomenų

gavimo iš draudimo brokerių bendrovės. VDAI skundus pripažino pagrįstais bei konstatavo BDAR 5 str. 1 dalies a punkte nustatyto teisėtumo principo ir BDAR 6 str. 1 dalies nuostatų pažeidimus. Draudimo brokerių bendrovei teiktas nurodymas nutraukti duomenų subjektų asmens duomenų teikimą draudimo bendrovėms pasiūlymų inicijavimo tikslu iki kol asmens duomenų tvarkymo operacijos bus suderintos su BDAR 6 str. 1 dalies reikalavimais, o draudimo bendrovėms teikti nurodymai nutraukti duomenų subjektų kredito reitingo duomenų tvarkymą draudimo rizikos vertinimo tikslu.

4 atvejis

VDAI gavo skundą dėl Bendrovės (duomenų valdytojo) ir skolų išieškojimo įmonės galimai neteisėto asmens duomenų tvarkymo. Pareiškėjas nurodė, kad Bendrovė neteisėtai perdavė jo asmens duomenis, susijusius su įsiskolinimu, skolų išieškojimo įmonei.

VDAI nustatė, kad duomenų perdavimas neatitiko BDAR 28 str. 3 dalies reikalavimų. Tokia išvada padaryta nustačius, kad skolų išieškojimo įmonė veikė kaip pagalbinis duomenų tvarkytojas (subtvarkytojas) ir pareiškėjo asmens duomenis gavo iš pirminio duomenų tvarkytojo, nors tarp jų nebuvo sudaryta duomenų tvarkymo sutartis, kaip to reikalauja BDAR 28 str. 3 d. VDAI sprendė, kad tokia neatitiktis savaime nelemia, jog duomenų tvarkymas buvo vykdomas neteisėtai ir pareiškėjo skundą dėl neteisėto asmens duomenų tvarkymo atmetė, tačiau už nustatytus BDAR 28 str. 3 dalies pažeidimus Bendrovei (duomenų valdytojui) ir pirminiam duomenų tvarkytojui teikė nurodymus.

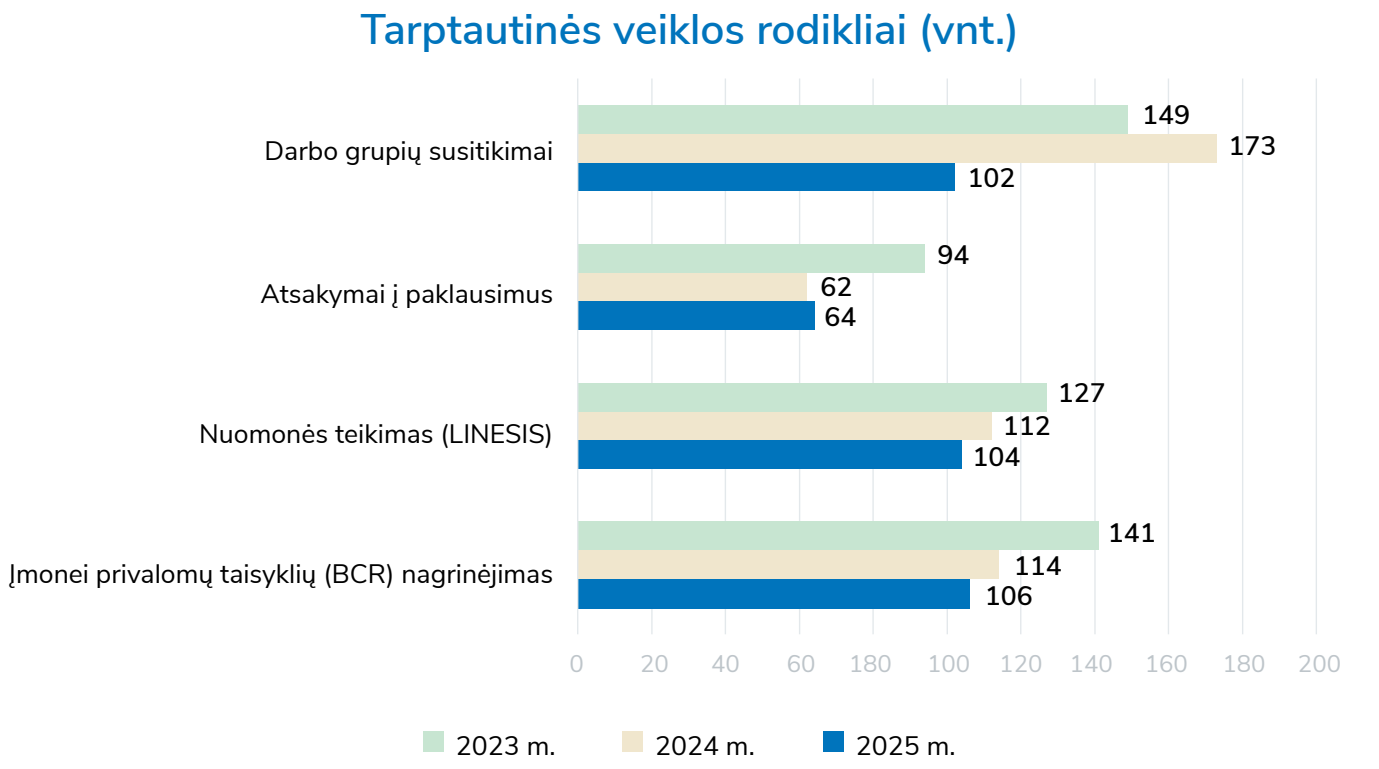


TARPTAUTINĖ VEIKLA

BDAR įtvirtintas nacionalinių priežiūros institucijų privalomas veiklos indėlis EDAV ir jos pogrupiuose, todėl ataskaitiniu laikotarpiu VDAI vykdė aktyvią tarptautinę veiklą šioje srityje bei bendradarbiavo su kitų valstybių narių priežiūros institucijomis. Daugiausiai buvo dalyvauta EDAV pogrupių ir kitų tarptautinių darbo grupių veikloje, kuriuose buvo rengiami ir derinami nuosekliam BDAR taikymui visoje ES svarbūs dokumentai (nuomonės, gairės ir kt.), taip pat buvo keičiamasi nuomonėmis su kitomis ES priežiūros institucijomis įvairiais praktikos formavimo klausimais IMI ar naudojantis vidiniu EDAV įrankiu, skirtu tik valstybių narių priežiūros institucijoms – *Confluence*).

2025 m. VDAI dalyvavo EDAV ir kitų ES institucijų bei tarptautinių organizacijų darbo grupių ir pogrupių iš viso 102 posėdžiuose ir kituose darbiniuose susitikimuose.

7 grafikas



VDAI bendradarbiauja su ES ir Europos ekonominės erdvės valstybių priežiūros institucijomis nagrinėjant skundus taikant nuoseklumo užtikrinimo mechanizmą. Per 2025 m. gauti 34 tarptautiniai skundai, kuriuose VDAI veikia kaip vadovaujanti priežiūros institucija. Per šį laikotarpį veikdama kaip vadovaujanti priežiūros institucija VDAI priėmė 28 sprendimus, kurie buvo derinami su susijusiomis priežiūros institucijomis. VDAI, kaip vadovaujanti priežiūros institucija, 2025 m. pabaigos duomenimis, veikė iš viso 78 tarptautinėse bylose.

Siekiant gilinti bendradarbiavimą ir keistis geriausia praktika, kasmet vyksta Baltijos šalių – Lietuvos, Latvijos ir Estijos – duomenų apsaugos institucijų susitikimai. Tokių kasmetinių susitikimų metu Baltijos šalių duomenų apsaugos institucijų vadovai ir darbuotojai aptaria praėjusių metų veiklos rezultatus ir keičiasi duomenų apsaugos reikalavimų taikymo praktika. 2025 m. rugsėjo 4–5 d. šis susitikimas vyko Vilniuje.

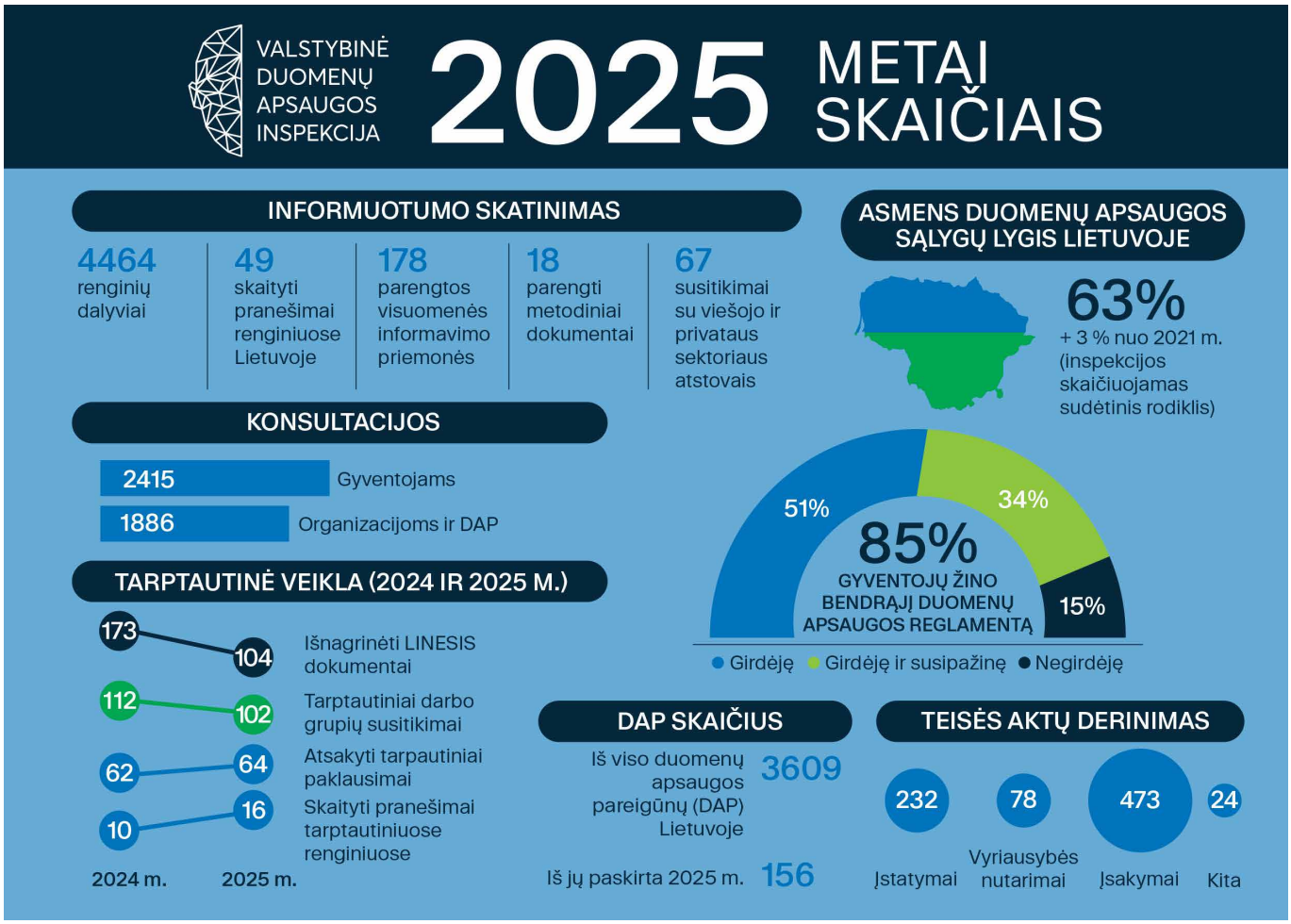
Lietuvos patirtimi dalintasi Tarptautinėje privatumo simpoziumo konferencijoje (angl. P*rivacy Symposium*), vykusioje gegužės mėn. Italijoje. VDAI direktorė Dijana Šinkūnienė diskusijų grupėje tema „Medicininių tyrimų atvėrimas: teisinis antrinio duomenų panaudojimo medicininiuose tyrimuose pagrindas“ pristatė Lietuvos patirtį bei su kitais ES duomenų apsaugos ekspertais diskutavo apie privatumo ir viešojo intereso medicininiuose tyrimuose pusiausvyros užtikrinimą. Diskusijoje taip pat buvo aptarti iššūkiai ir galimybės, kaip suderinti visuomenės interesą pasitelkti sveikatos duomenis moksliniams tyrimams bei inovacijoms ir būtinybę užtikrinti asmens duomenų apsaugą.

Birželio mėn. Vilniuje vykusiame Baltijos šalių privatumo ir inovacijų forume 2025 (*Baltic privacy and innovation summit*) VDAI direktorė Dijana Šinkūnienė su kitais duomenų apsaugos ekspertais diskutavo, kaip išlaikyti pusiausvyrą tarp nuolat tobulėjančių technologijų ir teisinio reglamentavimo. Konferencijoje, kurią organizavo Lietuvos duomenų apsaugos pareigūnų asociacija (LDAPA), taip pat dalyvavo Estijos duomenų apsaugos inspekcijos vadovė Pille Lehis, duomenų apsaugos ekspertai iš kitų valstybinių ir privačių institucijų ir organizacijų bei akademinės visuomenės. Pagrindinės diskusijų ir pranešimų temos buvo DI reguliavimas ir inovacijų skatinimas, duomenų vaidmuo šiuolaikinėse verslo strategijose, asmens duomenų apsaugos sistemos raida, įgyvendinimo tendencijos ir būsimi poreikiai.

VDAI direktorė dalyvavo 2025 m. liepos mėn. Helsinkyje (Suomija) vykusiame aukšto lygio EDAV susitikime. Susitikimo metu ES valstybių narių duomenų apsaugos priežiūros institucijų vadovai, Europos Komisijos, Europos duomenų apsaugos priežiūros pareigūno institucijos atstovai aptarė strategines duomenų apsaugos kryptis: BDAR taikymo supaprastinimas, nuoseklus reglamento įgyvendinimo užtikrinimas bei tarpinstitucinio bendradarbiavimo stiprinimas. Šiems tikslams pasiekti priimtas „Helsinkio pareiškimas dėl aiškumo, pagalbos ir bendradarbiavimo stiprinimo: pagarba pagrindinėms teisėms grįstas požiūris į inovacijas ir konkurencingumą“ (angl. *The Helsinki Statement on Enhanced Clarity, Support and Engagement: A Fundamental Rights Approach to Innovation and Competitiveness*). Helsinkio pareiškime įtvirtintos iniciatyvos, skirtos palengvinti BDAR laikymąsi, ypač labai mažoms, mažoms ir vidutinėms organizacijoms, stiprinti BDAR taikymo nuoseklumą ir skatinti priežiūros institucijų bendradarbiavimą.

VDAI atstovai dalyvavo Europos duomenų apsaugos priežiūros institucijų atstovų 2025 m. Pavasario konferencijoje, kurios metu aptartos aktualios duomenų apsaugos reguliavimo tendencijos ir praktiniai iššūkiai.

VISUOMENĖS INFORMAVIMAS, ŠVIETIMAS IR KONSULTAVIMAS



VDAI, vykdydama vieną iš veiklos prioritetų, didelį dėmesį skiria prevencinei ir šviečiamajai veiklai. Siekiama pasiekti gyventojus ne tik sostinėje, bet ir regionuose.

2 lentelė

VEIKLA	2023 m.	2024 m.	2025 m.
Suteikta konsultacijų	4 163	4334	4301
Parengta visuomenės informavimo priemonių	95	93	178
Parengta metodinių dokumentų	22	25	18
Dalyvauta susitikimuose su viešuoju ir privačiu sektoriais	79	112	67
Dalyvauta renginių	23	18	25
Skaityta pranešimų renginiuose	44	38	49
Renginių dalyvių skaičius	14 731	6288	4464

Konsultacijos

Konsultacijų teikimas yra viena pagrindinių pagalbos priemonių siekiant užtikrinti nuoseklų BDAR taisyklių taikymą. 2025 m. VDAI iš viso suteikė 4 301 konsultaciją, iš jų 1797 duomenų valdytojams, 2415 duomenų subjektams ir 89 DAP. Daugiau konsultacijų suteikta telefonu – 3208 (2024 m. – 3149). Kitais būdais teiktų konsultacijų skaičius išlieka panašus: oficialiu raštu – 234 (2024 m. – 251), elektroniniu paštu – 824 (2024 m. – 902), VDAI patalpose – 35 (2024 m. – 32).

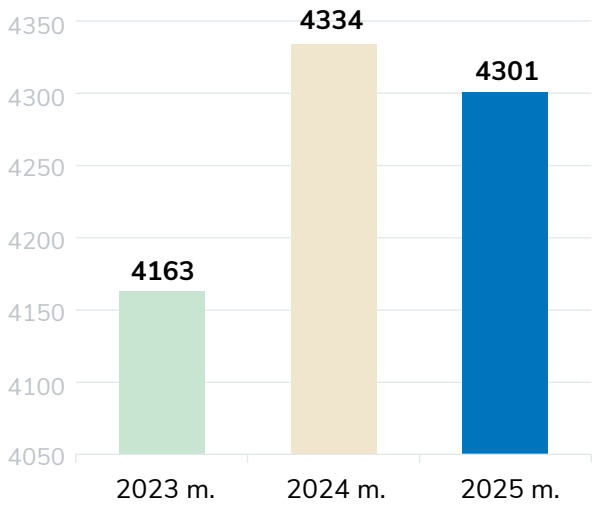
2022– 2024 m. suteikiamų konsultacijų skaičius nuosekliai augo (2022 m. – 3 691, 2023 m. – 4 136, 2024 m. – 4 334).

Stebima tendencija, kad konsultacijų skaičius išlieka panašus.

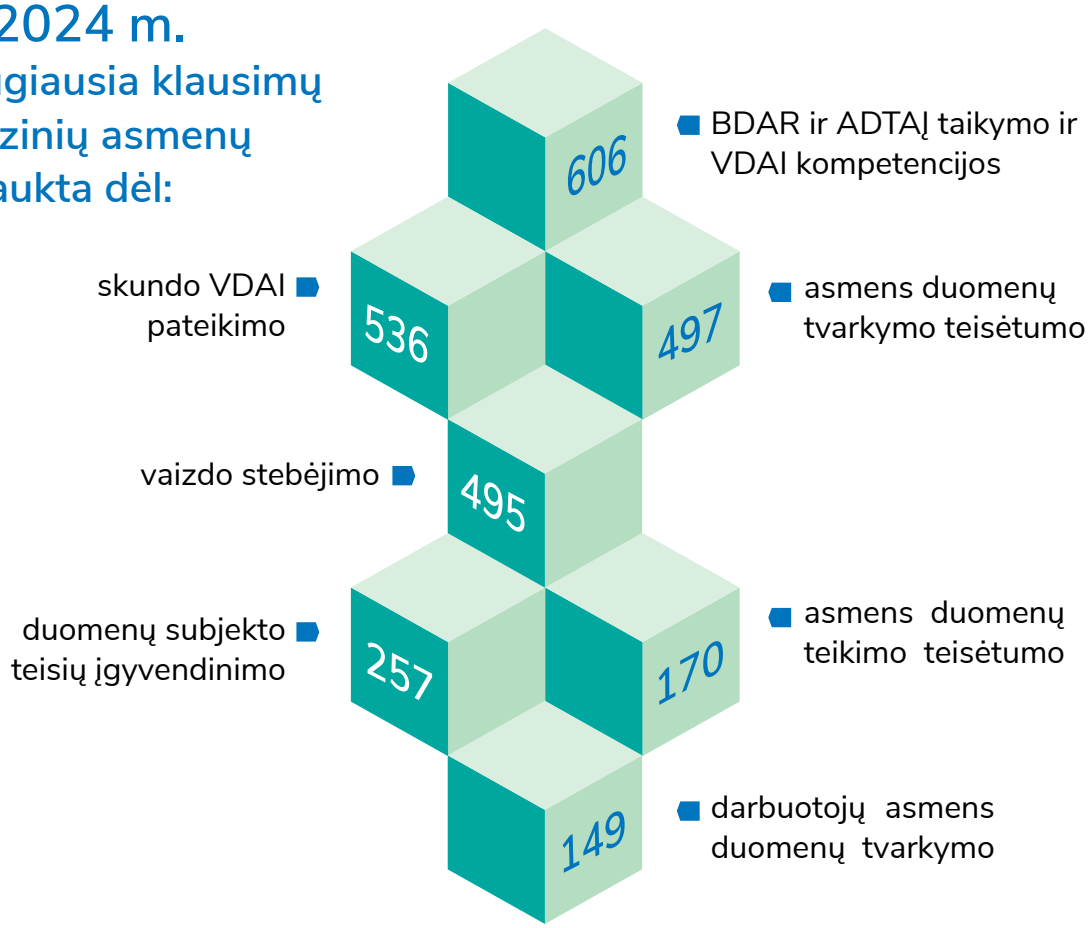
Tam įtakos turi tai, kad VDAI nebeturi galimybių skirti daugiau darbuotojų šiai veiklai vykdyti.

8 grafikas

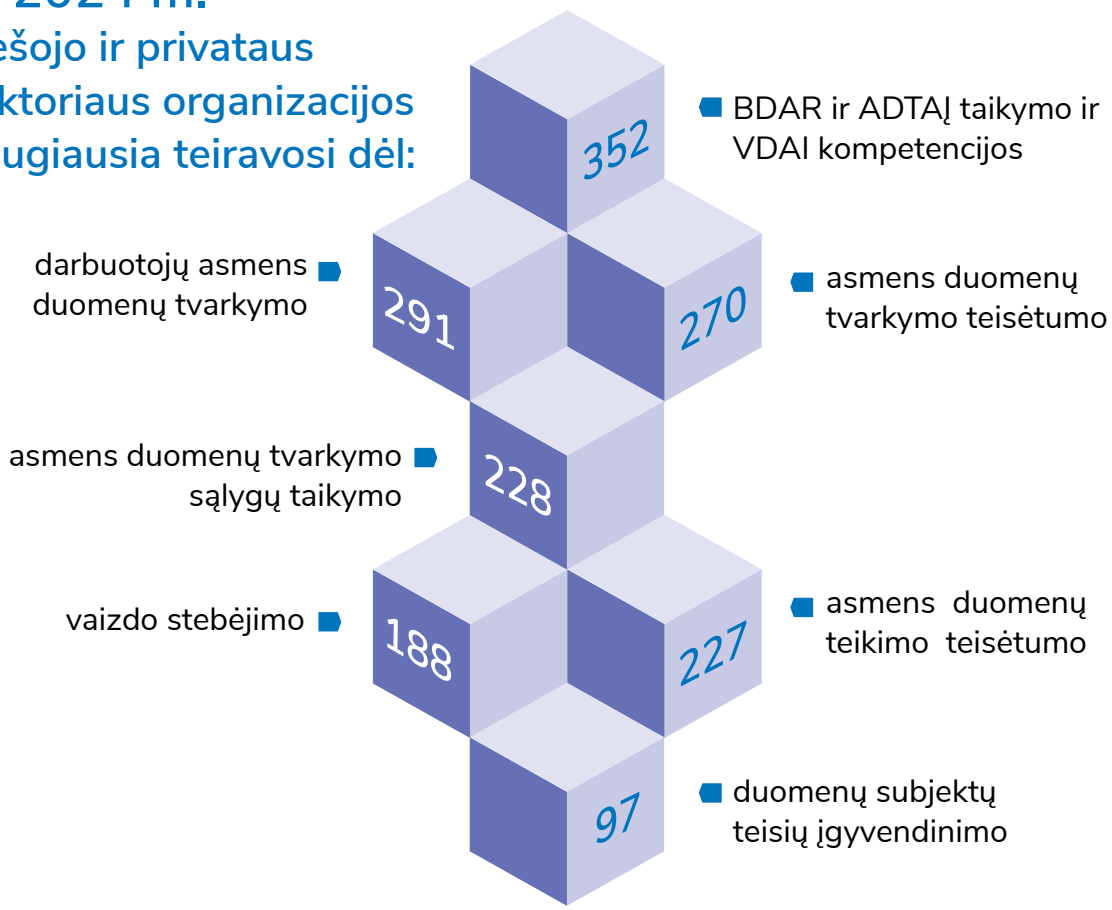
2023–2025 m. suteiktų konsultacijų skaičius (vnt.)



2024 m.
daugiausia klausimų iš fizinių asmenų sulaukta dėl:



2024 m.
viešojo ir privataus sektoriaus organizacijos daugiausia teiravosi dėl:



Metodinė pagalba

VDAI, siekdama pateikti išsamesnės informacijos aktualiais asmens duomenų ir privatumo apsaugos klausimais didesnėms suinteresuotųjų asmenų grupėms, 2025 m. daug dėmesio skyrė metodinės informacijos rengimui, kuri yra naudinga tiek organizacijoms, tiek ir gyventojams. 2025 m. parengta 18 metodinių priemonių: 8 DUK, 4 VDAI apibendrinimai ir 6 rekomendacijos.

„Rekomendacija dėl asmens duomenų apsaugos reikalavimų taikymo teisėkūroje“ skirta viešojo sektoriaus organizacijoms, rengiančioms teisės aktus. Kokybiška teisėkūra itin svarbi užtikrinant pasitikėjimą viešuoju sektoriumi ir jo atliekamu asmens duomenų tvarkymu. Rekomendacijos tikslas – pateikti praktinius patarimus, kurie padėtų teisės aktų rengėjams įgyvendinti pagrindinius asmens duomenų apsaugą reglamentuojančių teisės aktų reikalavimus.

Rekomendaciją „Sekimo pikseliai ir kaip juos blokuoti“ skirta gyventojams. Ji padės asmenims geriau suprasti, kas yra sekimo pikseliai ir kaip jų naudojimą gali blokuoti pats žmogus.

Siekiant atkreipti visuomenės dėmesį į veiksmus, kurių reiktų imtis įvykus kibernetiniam incidentui, kurio metu yra pažeisti asmens duomenys, parengta rekomendacija, kurioje aptarti kibernetinių incidentų tipai; nurodyti veiksmai, kurių turėtų imtis duomenų subjektai įvykus kibernetiniam incidentui; pateikiamos rekomendacijos, kurios padės geriau apsaugoti asmens duomenis.

Parengta rekomendacija organizacijoms dėl DAP. Jos tikslas – padėti organizacijoms suprasti BDAR nustatytus reikalavimus, susijusius su DAP paskyrimu, jo užduotimis, atsakomybe, taip pat atsakyti į klausimus, dėl kurių organizacijos dažniausiai kreipiasi į VDAI konsultacijų.

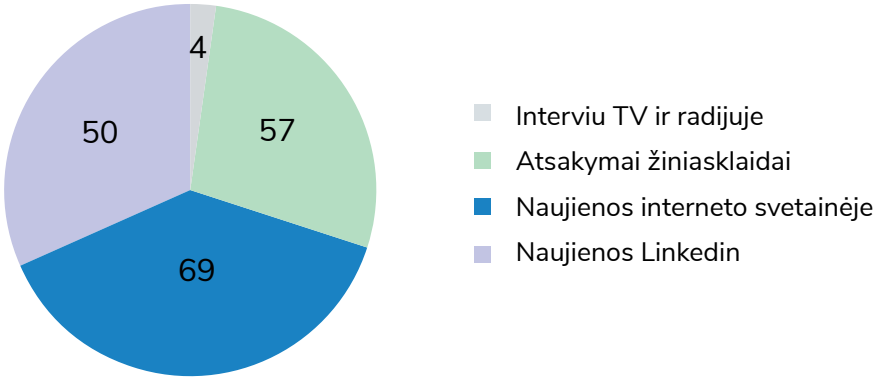
Atsižvelgus į visuomenės poreikius, atnaujintos rekomendacijos dėl ADSP ir dėl prašymų pateikti asmens duomenis. Taip pat parengta metodinė informacija dėl DI sistemų naudojimo, duomenų subjekto teisės susipažinti su duomenimis, asmens tapatybės vagystės rizikų ir kt.

Visuomenės informavimas

VDAI skiria daug dėmesio informacijos sklaidai apie vykdomą veiklą, funkcijas, taip pat teikia komentarus ir patarimus, kaip elgtis organizacijoms ir žmonėms, susidūrusiems su galimais duomenų apsaugos ar saugumo pažeidimais. Šios situacijos aktualios tiek viešajam, tiek privačiajam sektoriams, todėl VDAI 2025 m. rinkosi įvairius visuomenės informavimo kanalus ir priemones: pateikti 57 atsakymai į žiniasklaidos atstovų paklausimus; dalyvauta 4 TV ar radijo laidose, duoti interviu; prevenciniais tikslais paskelbtos 69 naujienos interneto svetainėje bei 50 pranešimų socialiniame tinkle „LinkedIn“.

9 grafikas

2025 m. parengtų informavimo priemonių skaičiaus pasiskirstymas (vnt.)



Renginiai Lietuvoje

2025 m. vykdytos Lietuvos gyventojų apklausos duomenimis, apie BDAR teko girdėti 85 proc. šalies gyventojų. VDAI, siekdama didinti gyventojų informuotumą duomenų apsaugos srityje ir norėdama pasiekti didesnes auditorijas, prioritetą teikė nuotoliniam renginių organizavimo būdui.

Vienas svarbiausių metinių VDAI renginių – duomenų apsaugos dienos konferencija, organizuojama minint Tarptautinę duomenų apsaugos dieną. Konferencijoje „Privatumas skaitmeninėje aplinkoje – iššūkiai ir galimybės“ pranešimus skaitė ir savo įžvalgomis dalijosi VDAI, NKSC, akademinės bendruomenės atstovai. Renginyje dalyvavo 200 dalyvių iš verslo ir viešojo sektoriaus.

Organizacijos, siekdamos kelti darbuotojų kvalifikaciją, neretai pageidauja konsultacijas gauti mokymų (seminarų) forma. Atsižvelgdama į poreikius, VDAI organizavo 3 nuotolinius renginius – sveikatos priežiūros įstaigų, informacinių technologijų specialistams ir DAP.

Seminaro sveikatos priežiūros įstaigų darbuotojams metu pristatyti pagrindiniai BDAR reikalavimai ir jų taikymo aspektai, aptartos duomenų subjektų teisės, pagrindiniai duomenų teikimo, vaizdo stebėjimo sveikatos priežiūros įstaigose reikalavimai, darbuotojų asmens duomenų tvarkymas bei kiti medicinos darbuotojams aktualūs klausimai.

Nuotolinio seminaro „Teisė ir technologijos“ metu dėmesys skirtas kibernetinio saugumo ir asmens duomenų apsaugos temoms.

Kasmetinių nuotolinių DAP mokymų metu apžvelgtos 2025 m. VDAI suteiktos konsultacijos, skundai ir rekomendacijos, pasidalinta metodinės pagalbos patarimais, viešai prieinamais įrankiais BDAR atitikties tikrinimui, aptarti kiti DAP aktualūs klausimai.

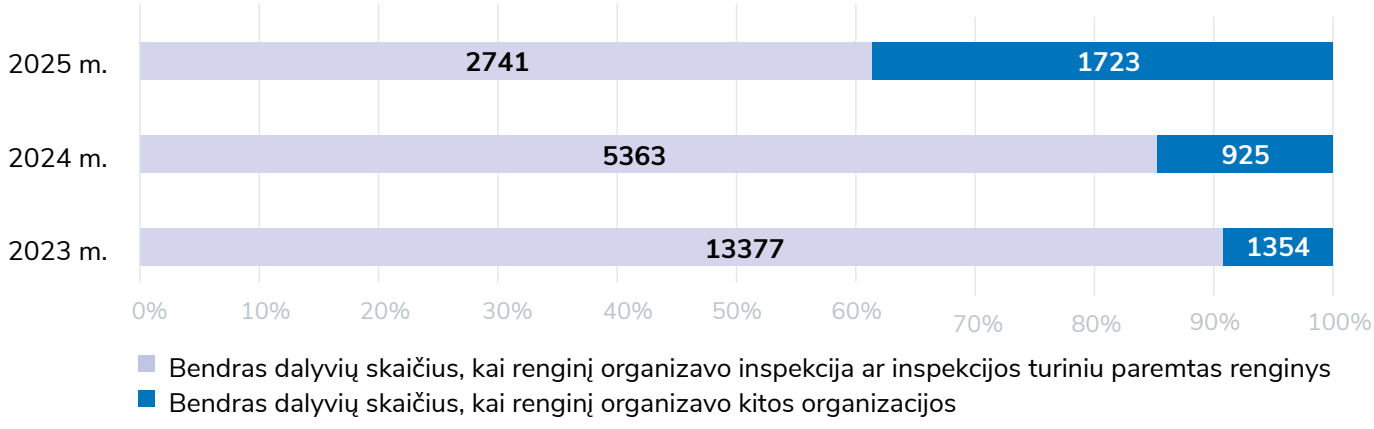
Kartu su Lietuvos bankų asociacija Vilniuje suorganizuota Baltijos šalių bankų sektoriaus konferencija „Duomenų apsauga finansų srityje: tarp BDAR, dirbtinio intelekto ir kibernetinio saugumo iššūkių“ (*Data Protection in Finance: Navigating GDPR, Artificial Intelligence, and Cybersecurity Challenges*). Konferencijoje dalyvavo Europos Komisijos Duomenų apsaugos skyriaus teisės ir politikos atstovė, Lietuvos, Latvijos ir Estijos nacionalinių duomenų apsaugos institucijų vadovai, taip pat visų trijų Baltijos šalių įvairių institucijų, bankų bei technologijų verslo atstovai. Renginio metu ekspertai nagrinėjo DI taikymą finansų sektoriuje, jo galimybes bei etinius ir teisinius aspektus; gilinosi į asmens duomenų tvarkymą pinigų plovimo prevencijos kontekste, diskutavo apie sukčiavimo prevenciją ir balansą tarp privatumo apsaugos ir naujausių saugumo standartų įgyvendinimo, apžvelgė veiksnius, formuojančius finansų sektoriaus ir duomenų apsaugos ateitį Baltijos regione.

Iš viso VDAI atstovai 2025 m. dalyvavo 25 renginiuose Lietuvoje, juose skaitė 49 pranešimus.

- Pranešimai skaityti 5 mokymuose,
- 7 konferencijose,
- dalyvauta 5 diskusijose ir kitokio pobūdžio renginiuose.
- Bendras 2025 m. renginių dalyvių skaičius – 4 464 (2024 m. – 6 288).

10 grafikas

2023–2025 m. renginių dalyvių skaičiaus pasiskirstymas (vnt.)



TEISĖKŪRA ASMENS DUOMENŲ APSAUGOS SRITYJE

VDAI dalyvavimas teisėkūros veikloje 2025 m. užėmė reikšmingą veiklos dalį. Nors 2025 m. gautų derinti teisės aktų projektų skaičius, palyginti su 2024 m., padidėjo nežymiai (2025 gauti 807 teisės aktai, 2024 m. – 768), pastaruosius trejetą metų stebimas teikiamų derinti teisės aktų projektų skaičiaus augimas.

Per ataskaitinį laikotarpį VDAI teikė pastabas ir pasiūlymus

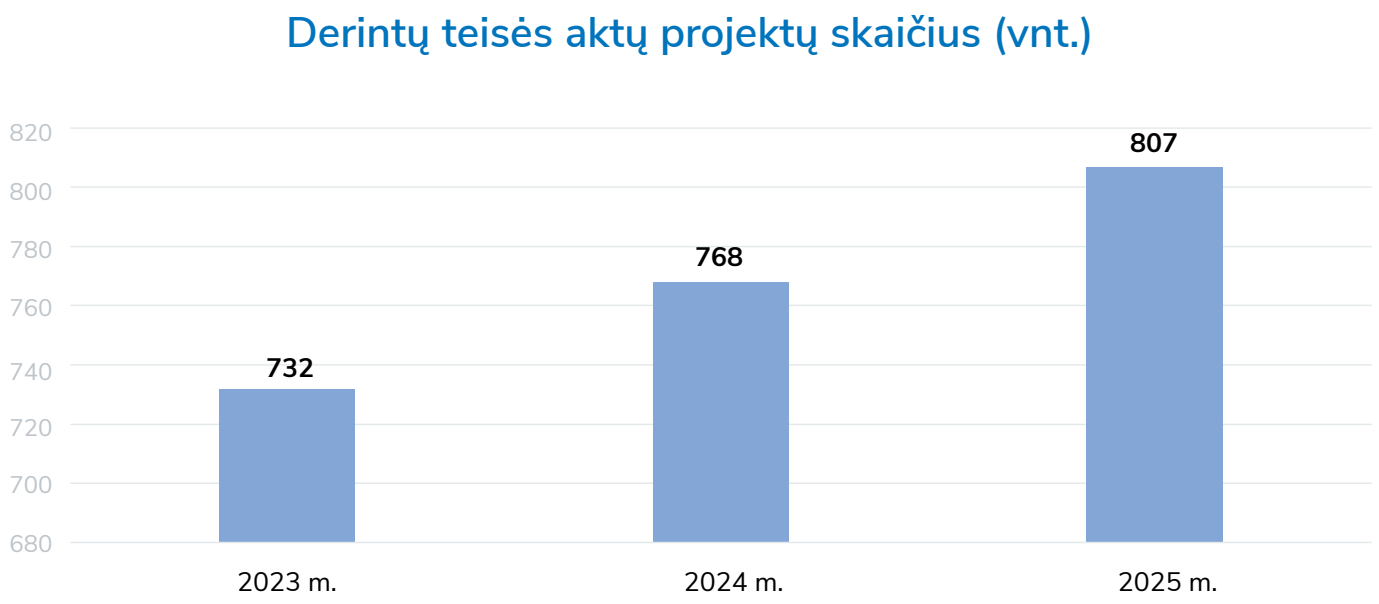
dėl 807

kitų institucijų pateiktų derinti teisės aktų projektų, iš jų:

- **473 įsakymų;**
- **232 įstatymų;**
- **78 Vyriausybės nutarimų;**
- **24 kitų teisės aktų.**

Papildomai pažymėtina, kad organizacijų prašymu VDAI net 94 teisės aktų projektus derino darbine tvarka (į statistiką neįtraukiama), taigi, galima sakyti, kad iš viso 2025 m. suderintas 901 teisės aktas.

11 grafikas



Paminėtini keletas iš 2025 m. pasiūlytu teisiniu reguliavimu visuomenei ar VDAI veiklai reikšmingų pateiktų derinti įstatymų projektų:

1. Lietuvos Respublikos vartojimo kredito įstatymo Nr. XI-1253 pakeitimo įstatymo projektas, kurio tikslas į nacionalinę teisę perkelti 2023 m. spalio 18 d. Europos Parlamento ir Tarybos direktyvos (ES) 2023/2225 dėl vartojimo kredito sutarčių, kuria panaikinama Direktyva 2008/48/EB nuostatas;
2. Lietuvos Respublikos Vyriausiosios tarnybinės etikos komisijos įstatymo Nr. X 1666 18 ir 29 straipsnių pakeitimo įstatymo projektas Nr. XVP-306;
3. Lietuvos Respublikos turizmo įstatymo Nr. VIII-667 2, 5, 6, 7, 9, 10, 11, 12, 13, 14, 15, 19, 20, 21, 24, 28, 31, 33, 34, 36 ir 40 straipsnių pakeitimo įstatymo projektas;
4. Lietuvos Respublikos rinkimų kodekso patvirtinimo, įsigaliojimo ir įgyvendinimo konstitucinio įstatymo Nr. XIV-1381 79 ir 80 straipsnių pakeitimo įstatymo projektas Nr. XIVP-4198 ir Lietuvos Respublikos rinkimų kodekso 33, 75, 78 ir 193 straipsnių pakeitimo konstitucinio įstatymo projektas Nr. XVP-104;
5. ERĮ Nr. IX-2135 81 straipsnio pakeitimo įstatymo projektas;
6. Lietuvos Respublikos žvalgybos įstatymo Nr. VIII-1861 2, 5, 7, 9, 11, 13, 14, 18, 19, 24, 29, 33, 40, 43, 45, 49, 50, 55, 57, 60, 64, 641, 69, 70 ir 71 straipsnių pakeitimo ir papildymo 3 priedu įstatymo projektas.

Vieni pagrindinių iššūkių, su kuriais susiduria teisės aktus teikiančios derinti institucijos, išlieka asmens duomenų tvarkymo, ypač jų viešo skelbimo, nustatymas teisės akte atsižvelgiant į ES ir Lietuvos teismų išaiškinimus bei BDAR 6 str. 3 dalies įgyvendinimas (ypač su būtinų tvarkyti asmens duomenų įvardijimu įstatymus įgyvendinančiuose teisės aktuose, asmens duomenų saugojimo termino trukmės pagrindimu).

Pastebėtina, kad VDAI ne tik derino teisės aktų projektus, bet ir pati, esant poreikiui, juos rengė. Pavyzdžiui, patvirtinti Valstybinės duomenų apsaugos informacinės sistemos ir Valstybinės duomenų apsaugos informacinės sistemos saugos nuostatai, atnaujintas Konsultavimo VDAI tvarkos aprašas, parengtos Vienodos ir kokybiškos asmenų konsultavimo praktikos užtikrinimo gairės ir kt.

Teisėsaugos ADTAĮ įgyvendinimo priežiūra

VDAI be BDAR vykdo ir Teisėsaugos ADTAĮ jos kompetencijai priskirtų nuostatų taikymo priežiūrą. Šis teisės aktas išsiskiria tuo, kad jame yra reglamentuojami su teisėsaugos atliekamu asmens duomenų tvarkymu susiję aspektai.

Svarbu paminėti, kad pastaruoju metu ES yra analizuojamas asmens duomenų apsaugos taisyklių veikimas teisėsaugos srityje. 2025 m. VDAI pildė du klausimynus, pateikdama informaciją apie situaciją Lietuvoje:

2025 m. birželio mėn. VDAI pateikė informaciją klausimynui, susijusiam su 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos direktyvos (ES) 2016/680, kuri perkelta į Teisėsaugos ADTAĮ, taikymo praktika, iššūkiais, įgyta patirtimi ir kitomis įžvalgomis (klausimynas gautas iš Danijos, kaip būsimos ES Tarybai pirmininkausiančios valstybės narės).

2025 m. spalio mėn. pildytas EDAV parengtas klausimynas dėl Direktyvos (ES) 2016/680 taikymo. Kaip rezultatas, 2026 m. sausio 15 d. buvo priimta EDAV ataskaita „EDAV indėlis į Europos Komisijos Duomenų apsaugos teisėsaugos direktyvos („LED“) vertinimą pagal 62 straipsnį“. Kaip ir kitos ES priežiūros institucijos, Inspekcija klausimyne pažymėjo, kad praktinis Direktyvos (ES) 2016/680 taikymas kelia tam tikrų iššūkių ir pateikė apibendrintą informaciją apie Direktyvos (ES) 2016/680 įgyvendinimo praktiką bei taikymo tendencijas, pagrįstą institucijos veiklos patirtimi.

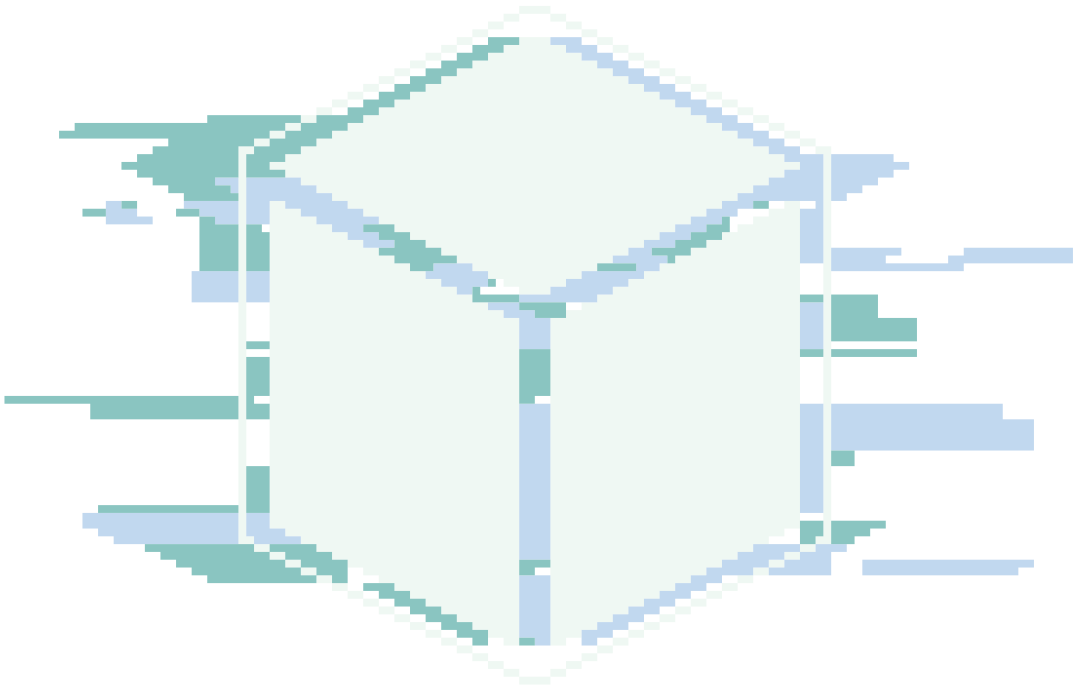
Informacijos pateikimas klausimynams yra svarbus vėliau vertinant asmens duomenų tvarkymo priežiūrą Lietuvos ir ES kontekste.

Pastebėtina, kad fiziniai asmenys itin retai kreipiasi į VDAI dėl teisėsaugos institucijų atliekamo asmens duomenų tvarkymo, kuriam taikomi Teisėsaugos ADTAĮ reikalavimai. Paminėtinas vienas atvejis.

VDAI gavo Pareiškėjo skundą dėl Policijos komisariato veiksmų, kad komisariatas pateikė savivaldybės administracijai informaciją apie jo kreipimusis į policiją, jų skaičių ir priežastis, taip pat perdavė procesinių dokumentų kopijas savivaldybės administracijos atliekamo galimo Pareiškėjo tarnybinio nusižengimo tyrimo tikslu. Pareiškėjas nurodė, kad jo kreipimaisi į policiją buvo nesusiję su darbo pareigų vykdymu.

VDAI padarė išvadą, kad Policijos komisariatas neįvertino prašomų duomenų teikimo teisėtumo, proporcingumo ir konkretaus tikslo, todėl Pareiškėjo asmens duomenų perdavimas savivaldybės administracijai buvo neteisėtas. Tokiu būdu Policijos komisariatas pažeidė Teisėsaugos ADTAĮ 3 str. 1 dalies 1 ir 2 punktus bei 7 str. 2 dalį bei neįrodė, kad toks duomenų teikimas buvo leidžiamas pagal teisės aktus.

Komisariatui pateiktas nurodymas – užtikrinti, kad nusikalstamų veikų prevencijos, tyrimo ar baudžiamojo persekiojimo tikslais surinkti asmens duomenys nebūtų teikiami ir tvarkomi kitais tikslais, jei tai nėra aiškiai leidžiama pagal teisės aktus.



DUOMENŲ APSAUGOS PAREIGŪNŲ SKYRIMAS LIETUVOJE

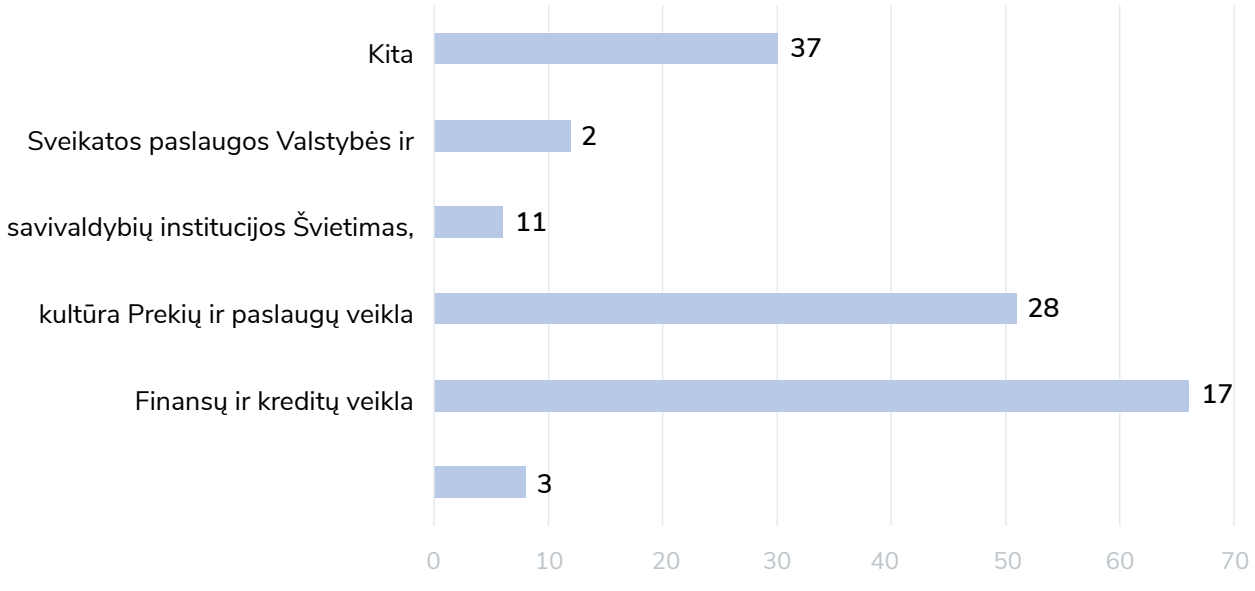
Nuo BDAR taikymo pradžios VDAI iš viso yra pranešta apie 3 609 DAP paskyrimą. 2025 m. Lietuvoje paskirti 156 DAP.

Organizacijos, kaip ir ankstesniais metais, susidūrė su iššūkiais skiriant DAP – išteklių stoka, kandidatų į DAP ekspertinių žinių trūkumu. VDAI, siekdama prisidėti prie DAP kompetencijų ugdymo, praktinių žinių gilinimo, 2025 m. daug dėmesio skyrė būtent šios tikslinės grupės metodinės pagalbos veikloms:

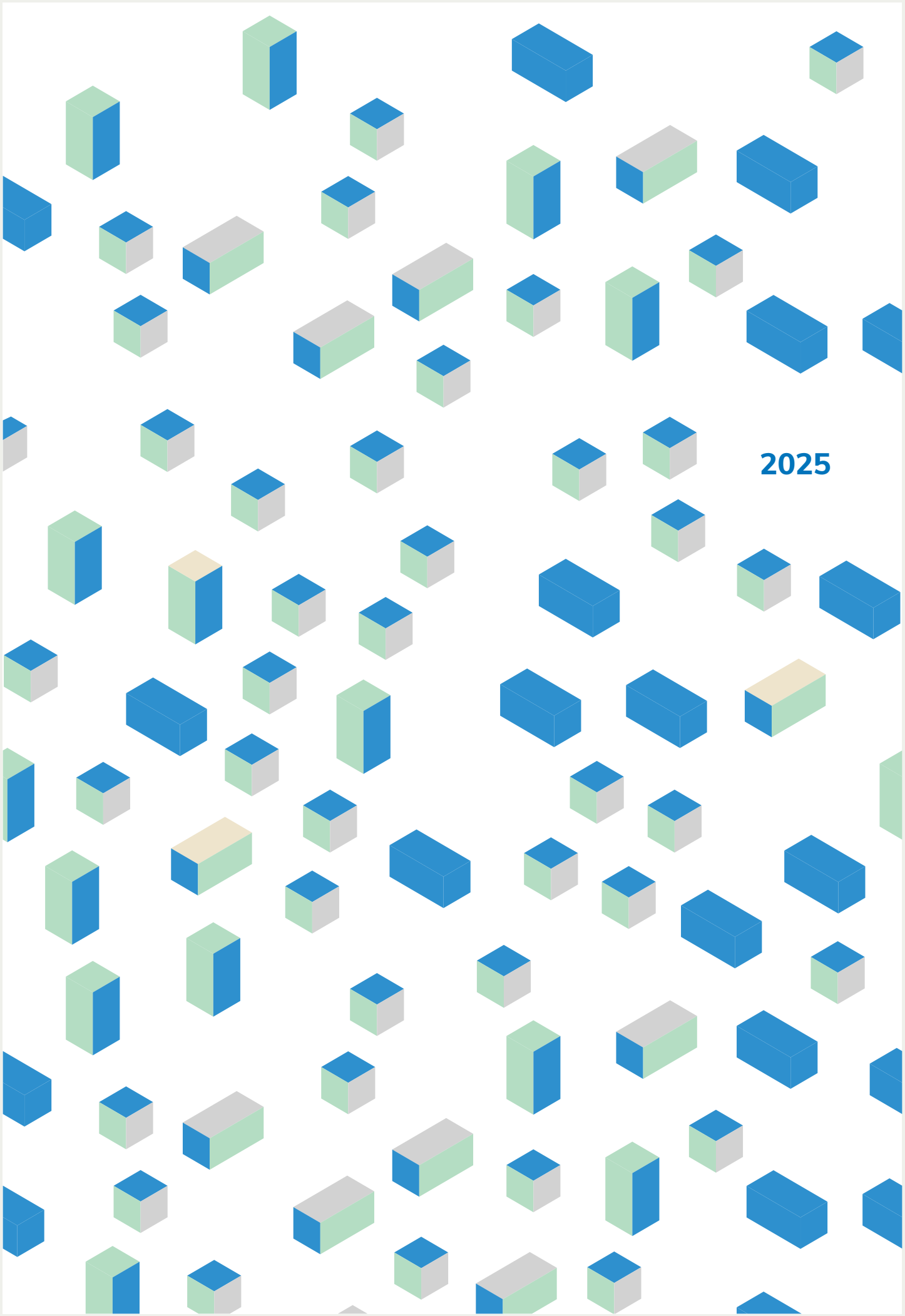
- parengta Rekomendacija dėl DAP, kurios tikslas padėti organizacijoms suprasti BDAR nustatytus reikalavimus, susijusius su DAP paskyrimu, jo užduotimis, atsakomybe;
- surengti kasmetiniai nemokami nuotoliniai DAP mokymai, kurie buvo skirti ne tik Lietuvos DAP, tačiau ir organizacijų vadovams, asmens duomenų apsaugos profesionalams, IT specialistams ir visiems, kam kasdienėje veikloje tenka spręsti su asmens duomenų tvarkymu susijusias situacijas;
- organizuoti susitikimai su Lietuvos duomenų apsaugos pareigūnų asociacija, siekiant padėti spręsti DAP aktualius BDAR taikymo klausimus.

12 grafikas

2025 m. paskirtų DAP pasiskirstymas pagal sritis (proc.)



REVIEW OF PERSONAL DATA PROTECTION SUPERVISION IN LITHUANIA BY THE STATE DATA PROTECTION INSPECTORATE


2025

Dijana Šinkūnienė
Director, State Data Protection Inspectorate

A MESSAGE FROM THE HEAD OF THE STATE DATA PROTECTION INSPECTORATE

The State Data Protection Inspectorate (hereinafter referred to as the SDPI) is an independent data protection supervisory authority, supervising the application of the General Data Protection Regulation (hereinafter referred to as the GDPR) and implementing the tasks set out in other Lithuanian and European Union (hereinafter referred to as the EU) legal acts. The mission of the SDPI as a data protection supervisory authority is to protect the human right to the protection of personal data.

Consistency in the application of personal data protection law depends on the joint efforts of all EU supervisory authorities. in July 2025, the European Data Protection Board (EDPB) adopted the *Helsinki Statement*, which contains measures to strengthen cooperation between authorities, increase clarity on GDPR requirements and provide additional assistance to small and medium-sized organisations. This step contributes to greater consistency in the application of personal data protection requirements across the EU.

In a context of technological developments and a rapidly changing digital environment, the effectiveness of the data protection system increasingly depends on the active involvement of all stakeholders. It is not only the knowledge of institutions that matters, but also that of individuals and organizations, as well as their ability to exercise their rights and fulfil their responsibilities in a responsible manner.

In 2025, the development and publicity of methodological material has been a major focus in order to raise public awareness on the protection of personal data. There has been a marked increase in public interest in this issue, with 48% more complaints and reports than in 2024, reflecting the growing awareness of the public and determination to become more active in defending their rights.

In 2025, confidence in the data protection system grew. A representative survey showed that 58% of residents believe that companies and institutions in Lithuania adequately ensure the protection of personal data, which is an increase of 6 percentage points compared to 2024. In addition, 50% of respondents are convinced that the public is sufficiently informed about personal data protection (4 percentage points more than in the previous year). These indicators show that consistent education and prevention are fostering a more mature data protection culture.

The results achieved in 2025 are the result of the commitment, efforts and responsibility of all SDPI staff members. Looking ahead, we will continue to seek ways to make it even easier for people to exercise their right to personal data protection and to ensure that this right is effectively upheld.

OPERATIONAL PRIORITIES

The data protection supervision system implemented by the SDPI aims to build trust in the processing of personal data by data controllers operating in Lithuania, while at the same time raising public awareness of the risks to the rights and freedoms of natural persons that may arise.

Economic and social life is constantly changing and new technologies are being developed rapidly. With increased digitalisation comes new risks to the right to the protection of personal data and other rights and freedoms, and changes brought about by technological developments should be human-centred and based on trust.

In setting its operational priorities, the SDPI took into account both the aforementioned changes in society and the policy directions outlined in the Programme of the Government of the Republic of Lithuania approved by Resolution No XV-54 „On the Approval of the Programme of the 19th Government of the Republic of Lithuania“ of the Seimas of the Republic of Lithuania of 12 December 2024, which are related to the exploitation of opportunities offered by artificial intelligence, data activation, strengthening the digital skills of the society, creating conditions for the secondary use of data, etc.

In 2025, the SDPI implemented two of its planned operational priorities.

1. To strengthen the prevention of personal data breaches and contribute to building trust in the public sector.

In order to strengthen the prevention of personal data breaches and to build trust in the public sector, the SDPI has focused on educating the actors involved in the processing of personal data in 2025. Only by enhancing the knowledge, competence, and skills of data controllers, data processors and data protection officers is it possible to ensure a higher data protection level (hereinafter referred to as HDPL), and, with greater awareness among data subjects, to achieve effective protection of their rights. While the target was 64% in 2025, the survey data shows that the rate was 63% and has actually increased by 3% since 2021. In 2025, public trust in companies and institutions regarding personal data protection increased. According to the survey,

of residents believe that companies and institutions in Lithuania ensure the right to data protection.

(which is 6 percentage points more than in 2024). Public confidence in data protection awareness also increased, as 50% of respondents state that people are informed about personal data protection (4 percentage points more than in 2024).

Cooperation with other institutions, associations and social partners is crucial for promoting a culture of data protection; therefore, the SDPI is working to establish and maintain various cooperation initiatives. Seminars, training sessions and conferences for target groups were organised together with social partners to discuss IT security, cyber threat prevention, video surveillance, personal data security and other relevant topics. For several years in a row, the SDPI, in cooperation with the National Cyber Security Centre under the Ministry of National Defence (hereinafter referred to as the NCSC) and the Lithuanian Police, has been involved in organising and conducting cyber security exercises. Data Protection Officers (hereinafter referred to as DPO) received their annual free online DPO training, which was aimed not only at Lithuanian DPO, but also at managers of organisations, personal data protection professionals, IT specialists, and anyone who has to deal with situations related to the processing of personal data in their daily work.

This operational priority focuses on the monitoring procedure and the amicable resolution of complaints. While the number of complaints resolved amicably in 2025 has fallen slightly, there has been a 65% increase in the number of such cases since 2022, when the practice started.

In order to strengthen the prevention of breaches and to provide more detailed information on relevant issues related to the protection of personal data and privacy to a wider range of stakeholders, in 2025 the SDPI has focused on the development of methodological information that is useful for both organisations and citizens. A total of 18 methodological tools have been developed: 8 FAQs, 4 Inspectorate summaries and 6 recommendations.

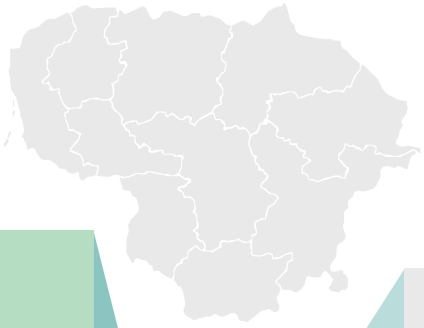
2. To strengthen international cooperation in the field of personal data protection.

In an effort to strengthen international cooperation in the field of personal data protection, the SDPI is actively engaged in international activities and cooperates with supervisory authorities of other Member States. Most of the participation was in the activities of the sub-groups of the European Data Protection Board (hereinafter referred to as the EDPB), where documents important for the consistent application of the GDPR across the EU were drafted and coordinated, and views were exchanged with other EU supervisory authorities on various issues related to the development of best practices. In 2025, the SDPI participated in a total of 102 meetings and other working sessions of working groups and sub-groups of the EDPB, other EU institutions and international organizations. The SDPI cooperates with the supervisory authorities of the EU and European Economic Area countries in the handling of complaints through the consistency mechanism. In 2025, 34 international complaints were received in which the SDPI acts as lead supervisory authority. During this period, acting as the lead supervisory authority, the SDPI adopted 28 decisions which were coordinated with the supervisory authorities concerned.

Data protection authorities from the Baltic states of Lithuania, Latvia and Estonia meet annually to deepen cooperation and exchange best practices.

On 4-5 September 2025, such meeting took place in Vilnius. The meeting discussed the results of the previous year's activities, shared practices and views on the application of data protection requirements, and discussed other relevant cooperation issues.

CONTEXT ANALYSIS



The SDPI is an agency of the Government of the Republic of Lithuania operating in the field of justice. The 2021-2030 National Progress Plan sets out the 8th strategic objective for this area: to increase the effectiveness of the legal system and public administration.

The SDPI contributes to the "Modernize legal protection processes" progress measure of the justice system development programme (hereinafter referred to as the Justice System Development Programme), administered by the Ministry of Justice of the Republic of Lithuania under the 2021–2030 Development Programme, with the aim of achieving the result indicator "Level of personal data protection (%)".

In 2025, the HDPL was 63% and has increased by 3% since 2021.

The objective of the SDPI is to ensure respect for the right of natural persons to the protection of personal data, to ensure the consistent application of the personal data rules, and to contribute to the creation of the conditions for the free movement of personal data.

In pursuit of the objective of the SDPI, the following impact indicator was targeted: “Increase in public trust in state institutions that oversee whether other companies and organizations properly ensure the protection of personal data, %.” In 2025, public trust in companies and institutions regarding personal data protection increased slightly. The expectation was to reach 55% trust, but according to the survey, 56% of residents trust state institutions that oversee whether other companies and institutions properly ensure the protection of personal data, i.e., 2% more than in 2024 (54% in 2024).

The SDPI supervises the application of the GDPR, the Republic of Lithuania Law on the Legal Protection of Personal Data Processed for the Purposes of Prevention, Investigation, Detection or Prosecution of Crimes, Execution of Punishments, or for the Purposes of National Security or Defence (hereinafter referred to as the Law Enforcement LLPPD), the Republic of Lithuania Law on the Legal Protection of Personal Data (hereinafter referred to as the LLPPD), and the provisions of the Republic of Lithuania Law on Electronic Communications (hereinafter referred to as the LEC), which are under the scope of its competence.

The State Progress Strategy ‘Lithuania‘s Vision for the Future ‘Lithuania 2050’’ envisages monitoring future technologies and the changes they will bring as one of the criteria for progress in the civil service. Intelligent technologies and data are expected to be ethically and legally integrated into decision-making processes.

The main objectives of the initiatives adopted by the EU on the Digital Single Market[1] and on the development of Artificial Intelligence (hereinafter referred to as the AI) (e.g. Digital Services Act, Data Act, AI Act) are to create a safer digital space that safeguards the fundamental rights of users of digital services and to establish a level playing field for promoting innovation, growth, and competitiveness.

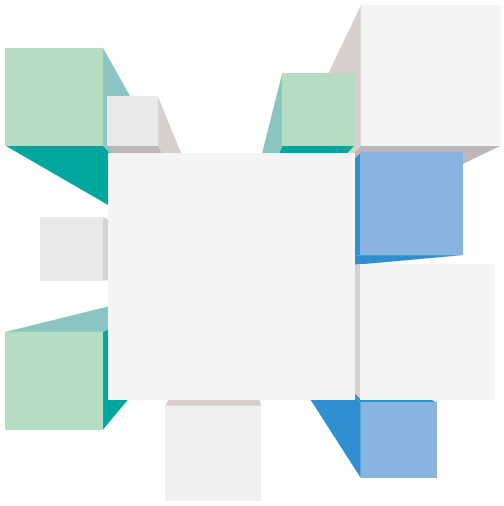
Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on AI and amending certain acts adopted under the Union legislative procedure (AI Act) creates an EU-wide single market for trustworthy and human-centred AI. It aims to booster innovation and the implementation of AI while ensuring a high level of protection of health, safety and fundamental rights, including democracy and the rule of law.

[1] https://www.europarl.europa.eu/factsheets/lt/sheet/43/visur-esanti-bendroji-skaitmenine-rinka#_ftnref1.

It should be noted that in 2025, the European Commission has presented two Omnibus proposals to amend the GDPR and has also presented a proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2024/1689 and (EU) 2018/1139 as regards the simplification of the implementation of harmonised rules on AI (hereinafter referred to as the Omnibus on AI[2]).

It is important to note that the GDPR has become a cornerstone EU law since 2016, strengthening the protection of personal data and trust in cross-border data flows. However, the evolution of EU digital regulation has in recent years highlighted the need to simplify requirements and reduce administrative burdens to make Europe more competitive. The first Omnibus[3] aims to simplify EU rules and reduce administrative burdens by giving more flexibility to choose the most appropriate way to comply with the GDPR. Meanwhile, the second, the Digital Omnibus,[4] not only aims to facilitate compliance with the GDPR, in particular for micro, small and medium-sized organisations, but also to maintain the EU's consistent policy direction: to preserve the core principles of the GDPR, to provide clearer, more practical and risk-based guidance on the application of the Regulation, and to ensure that the level of protection of personal data of the natural person/data subject is not reduced.

The SDPI is also one of the institutions implementing the cybersecurity policy. In implementing this policy, the SDPI participates in the activities of the Cyber Security Council, contributes to cyber security exercises, and, together with other responsible institutions, prepares the annual National Cyber Security Status Report. Cyber security is directly related to ensuring the security of personal data, and the SDPI conducts investigations into personal data breaches (hereinafter referred to as the PDB), cooperating with the NCSC as necessary during such investigations.



[2] Proposal of the European Commission for a Regulation of the European Parliament and of the Council of 19 November 2025 amending Regulations (EU) 2024/1689 and (EU) 2018/1139 as regards the simplification of the implementation of harmonised rules on artificial intelligence (hereinafter referred to as the Omnibus on AI).

[3] Proposal of the European Commission for a Regulation of the European Parliament and of the Council of 21 May 2025 amending Regulations (EU) 2016/679, (EU) 2016/1036, (EU) 2016/1037, (EU) 2017/1129, (EU) 2023/1542 and (EU) 2024/573 as regards the extension of certain mitigating measures available for small and medium sized enterprises to small mid-cap enterprises and further simplification measures (hereinafter referred to as Ominbus I)

[4] Proposal of the European Commission for a Regulation of the European Parliament and of the Council of 19 November 2025 amending Regulations (EU) 2016/679 (General Data Protection Regulation / GDPR), (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 (Data Act) and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Open Data Directive) (Digital Omnibus) (hereinafter referred to as the Digital Ominbus).

BUDGET ALLOCATIONS AND STAFFING ISSUES

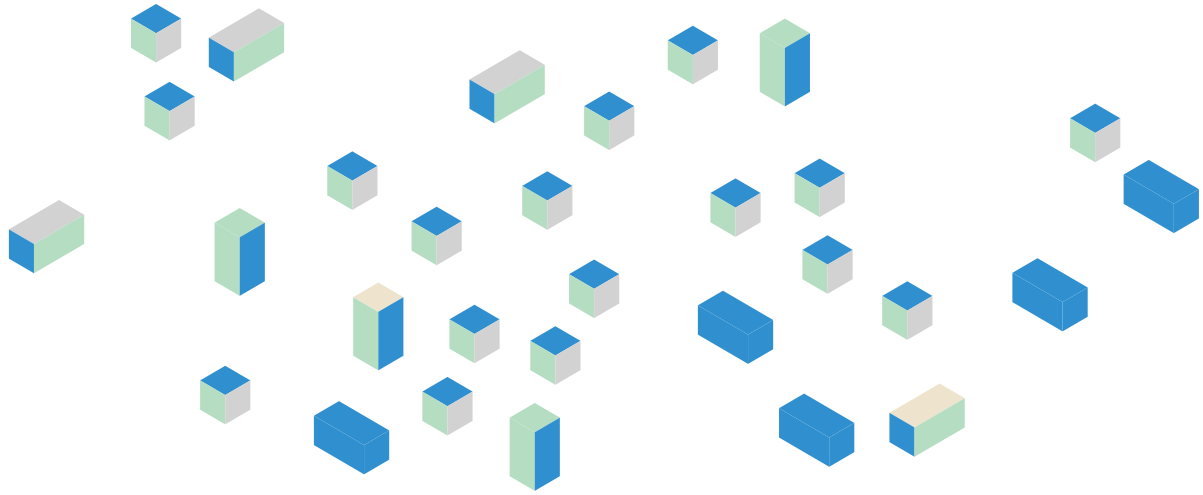
The SDPI is an attractive employer that offers the opportunity to acquire high-level qualifications in a promising field, but it faces greater challenges in recruiting staff than is typical for other public institutions. The prospect of acquiring high-level qualifications is insufficient to attract new employees; a competitive labour remuneration system must also be in place. Given the budget of the SDPI, this need can only be partially met, even with the implementation of additional incentive measures.

Table 1

Finance and human resources in 2023–2025

ACTIVITIES	2023 m.	2024 m.	2025 m.
Budget (thousand EUR)	1 592,0	1 727,0	2 198,0
of which remuneration (thousand EUR)	1 318,0	1 463,0	1 892,0
Number of positions	52	46	54*

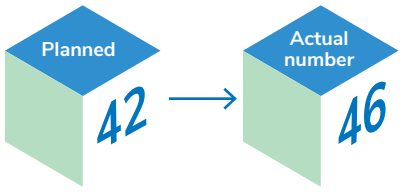
*In light of the additional financial resources received, the number of positions was increased in 2025



In 2025, 32 competitions were announced for vacant career civil service positions, of which 16 were held. Particular attention was paid to attracting new employees, and recruitment efforts were expanded: potential candidates who could join the team through internal transfers were sought; five open house events were organized; information about the competitions is published not only on the website and social media but also on job vacancy portals and sent to higher education institutions.

In order to not only attract but also retain professional specialists, significant attention is paid to improving employee qualifications.

The planned 2025 evaluation criterion for SDPI employees who participated in refresher courses and training was 42; the actual number was 46.



Employees participated in events designed to enhance their communication skills and deepen their knowledge of professional ethics, corruption prevention, digital literacy, and cyber security. Specialists also learned about effective communication with customers, managing complex service situations, and the psychological aspects of customer service.

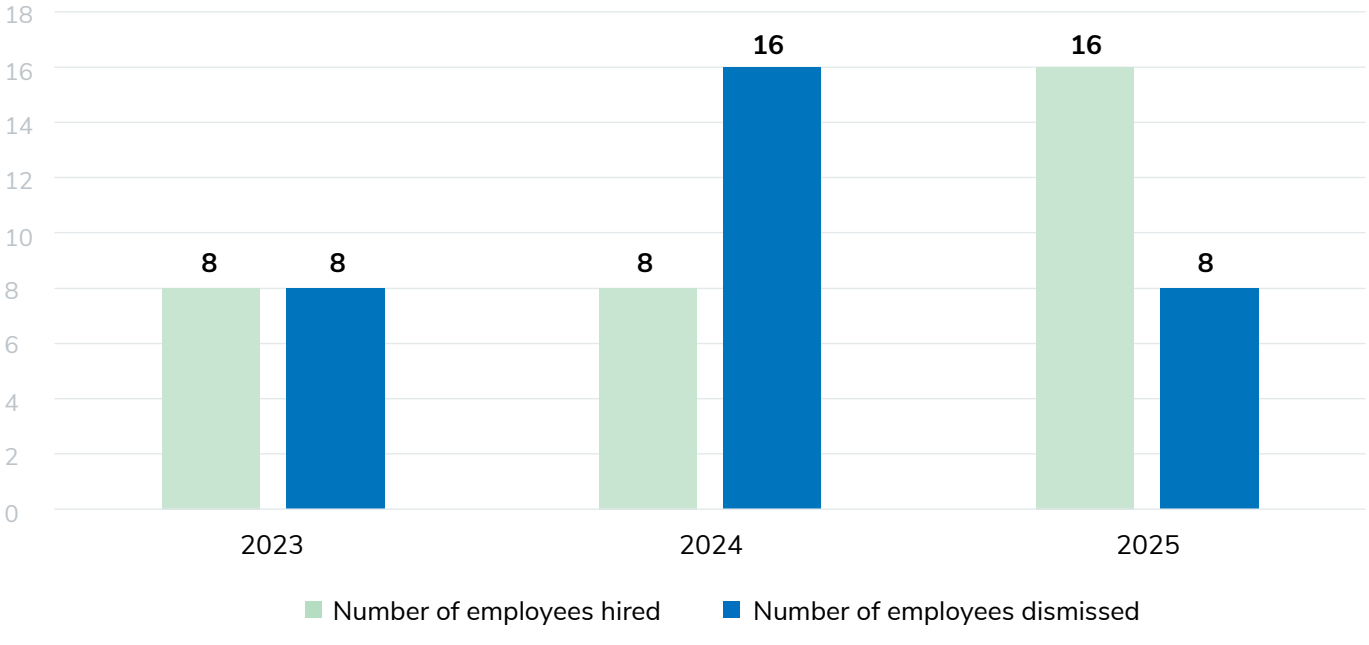
In order to improve staff competences in the field of personal data protection and to share best practices with other EU countries, two employees from Germany were accepted for a four-week internship program in 2025. The aim of the programme is to strengthen data protection skills and improve the implementation and enforcement of the GDPR, with a view to developing these skills through practical experience.

Labor market trends indicate that data protection specialists remain in high demand. For this reason, the risk of staff turnover remains high.

In 2025, a total of 14 civil servants and 2 employees working under employment contracts were hired. 8 civil servants were dismissed.

Chart 1

Change in the number of employees in 2023–2025 (numbers)



SUPERVISION OF ECONOMIC OPERATORS AND OTHER DATA CONTROLLERS

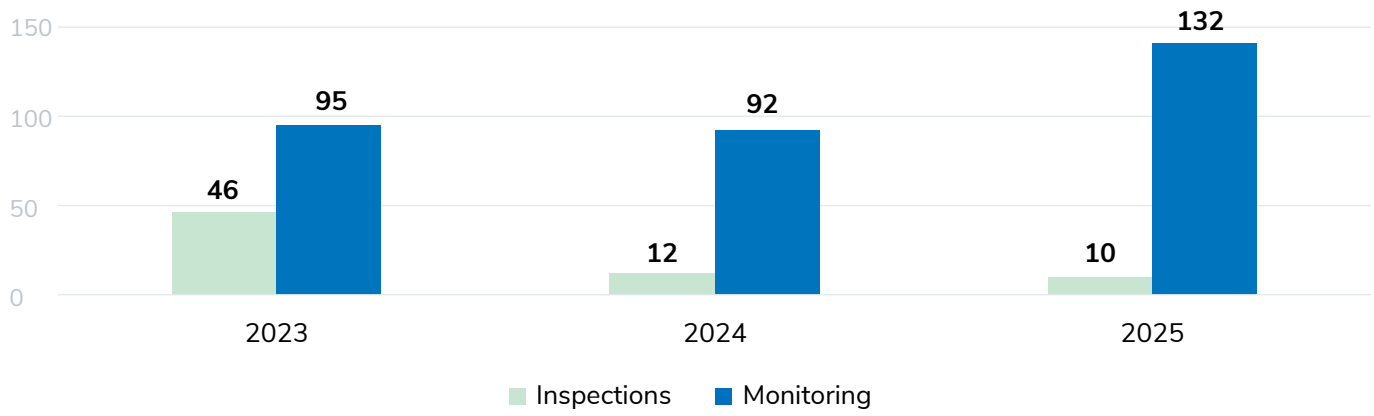
Inspections and monitoring

In 2025, 16 scheduled inspections were carried out by the SDPI (12 in 2024 and 46 in 2023). There were also cases where unscheduled inspections had to be carried out - a total of 10 were conducted.

In 2025, unscheduled inspections were initiated upon receiving information about potential PDBs in order to promptly assess potential risks and ensure lawful and secure data processing.

Chart 2

Breakdown of the number of inspections and monitoring activities in 2023–2025 (numbers)



Pursuant to Article 57(1)(a) of the GDPR, the SDPI has the authority to monitor compliance with the GDPR. This involves conducting an initial analysis of specific personal data processing operations and providing observations and recommendations on the proper implementation of legal requirements.

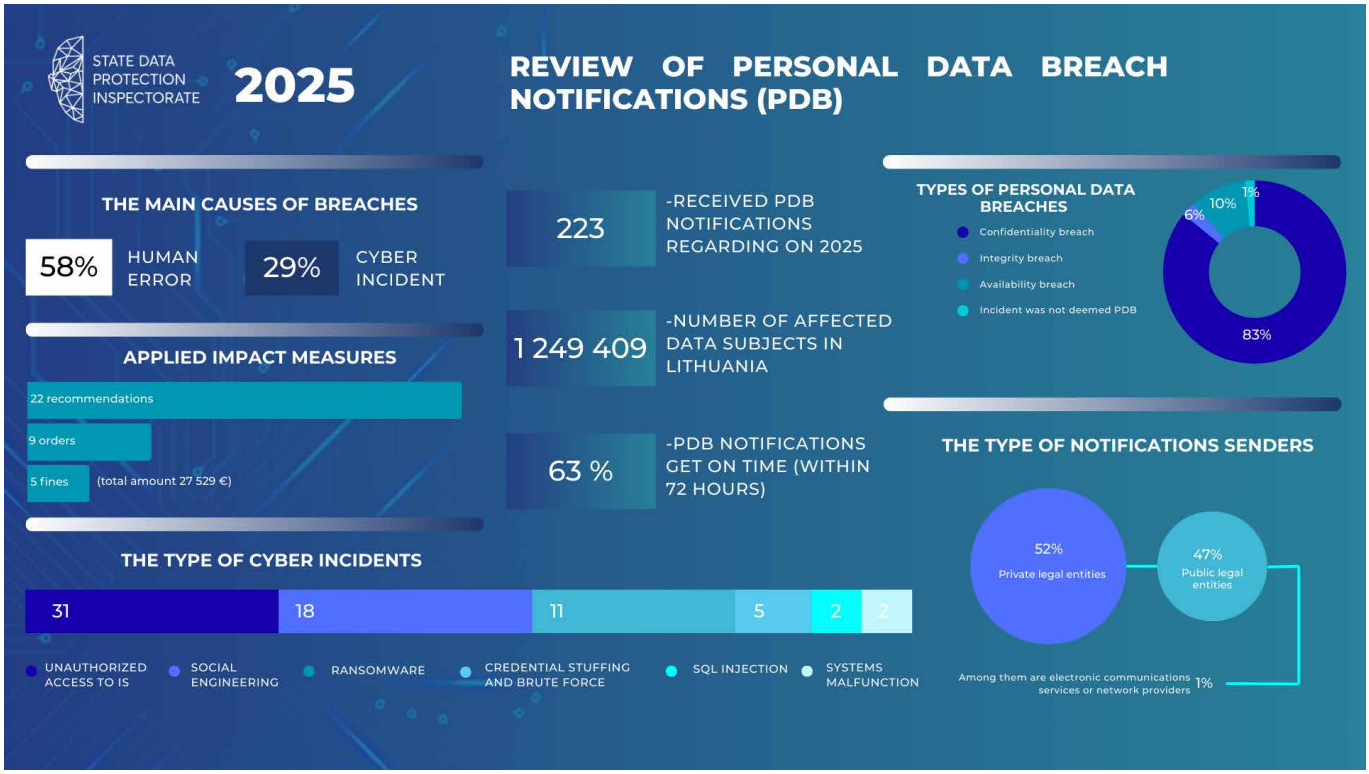
2022

This activity began in 2022 and makes it easier to respond to potential PDBs.

If, following monitoring activities, it becomes apparent that organisations have not voluntarily rectified operational shortcomings and GDPR breaches may still exist, the SDPI may initiate an inspection on its own initiative and apply enforcement measures.

In 2025, monitoring actions were applied in 132 cases. Monitoring most frequently concerned potential breaches in the area of direct marketing and its implementation methods (use of e-mail, tracking pixels, cookies), potential PDBs, and video surveillance. In isolated cases, inquiries were made regarding potential excessive data collection, data security, the processing of personal identification numbers and copies of identity documents, and the scope of data obtained from registers.

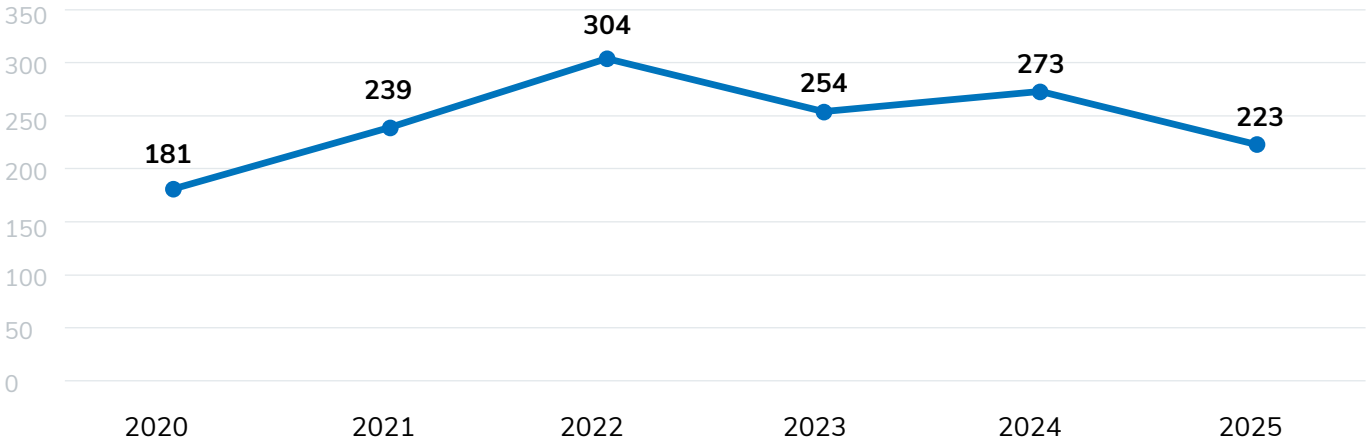
Personal data breaches



When PDB occurs, organisations must take steps to manage the breach, as well as implement measures to stop the breach and ensure that such breaches do not recur in the future. In all cases, organisations must investigate and document such breaches and comply with other procedures established by the GDPR. If it is determined that the breach poses a risk to the rights and freedoms of natural persons, the SDPI must be notified within 72 hours. The SDPI shall evaluate the PDB reports received and, if necessary, carry out an investigation.

Chart 3

Notifications received regarding ADSPs that occurred in 2020–2025 (pcs.)



In 2025, 63% of data controllers reported an PDB within 72 hours, while 37% reported it later than 72 hours.

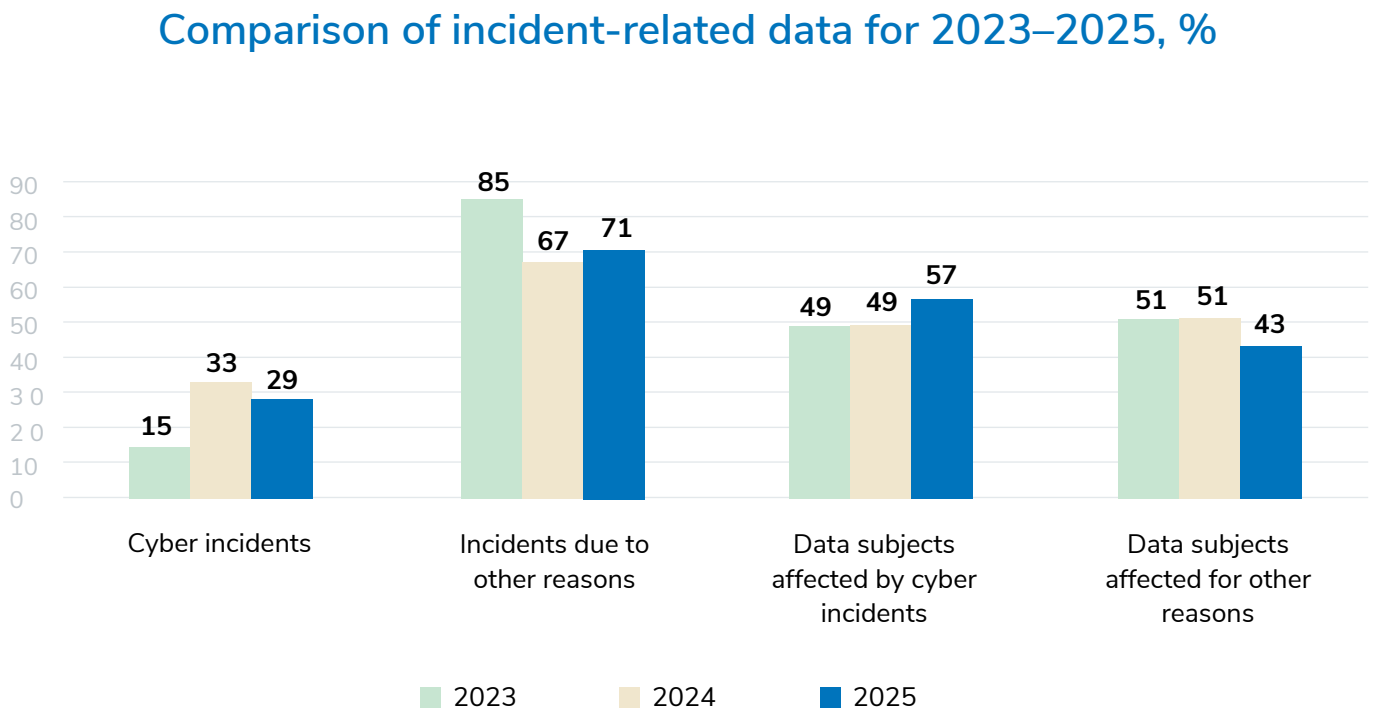
Compared to data from previous years, data controllers are more likely to submit reports late.

(in 2024, 79% of data controllers reported PDB within 72 hours, while 21% reported it later than 72 hours), and sometimes do not specify the reasons for the delay.

In 2025, the SDPI received 223 reports of PDB, and the number of data subjects affected in Lithuania was 1,249,409. Compared to data from previous years, the SDPI received fewer reports of PDB in 2025 than in 2024 (the number of PDB reports received by the SDPI in 2024 was 273). The number of data subjects affected in Lithuania also decreased by nearly 200,000 (in 2024, the number of data subjects affected in Lithuania was 1,467,368).

In terms of the nature of PDBs in Lithuania, confidentiality breaches predominate, accounting for as much as 83% of all cases in 2025 (87% in 2024); integrity breaches accounted for 6% of cases (6% in 2024); 10% of cases were availability breaches (6% in 2024), and 1% of cases were not classified as PDB (did not meet the definition) (1% in 2024 as well).

Chart 4



After analysing PDB reports in 2025, the Inspectorate found that 29% (69) of PDBs were caused by cyber incidents, 58% of PDBs were caused by human error, and 13% by other reasons (various IT system malfunctions, improperly performed programming work, failure to test systems, etc.).

Having determined that data security was not adequately ensured, in 2025 the SDPI issued 9 instructions to data controllers or processors to bring data processing operations into compliance with the provisions of the GDPR, also issued 22 recommendations, and imposed 5 fines (the highest being EUR 9,000 and the lowest – EUR 3,529).

Case 1

In January 2025, a public institution was fined EUR 9,000. It was established that the PDB occurred due to inadequate testing of the data loss prevention measures in place, and to unreasonable assumptions that a scenario not meeting the defined rule would trigger the measure to work. However, the data loss prevention measure did not work, resulting in an e-mail sent to 292 individuals with an attached Excel document containing personal data of 29 636 data subjects, including special categories of personal data.

Case 2

In February 2025, a public body was fined EUR 3,529. It was established that a cyberattack has occurred, during which a malicious actor hacked into the internal network and encrypted the data of 120 data subjects, including special categories of data. In this case, the controller has not documented or defined roles and responsibilities, did not have an access management policy and did not manage access rights properly. Furthermore, access control and authentication were not ensured, a system for logging and monitoring computer workstations had not been implemented, and users were granted administrator rights on their computer workstations.

Prior consultations

The GDPR provides that the controller shall consult the SDPI prior to processing where a data protection impact assessment indicates that the processing would result in a high risk to the rights and freedoms of natural persons in the absence of measures taken by the controller to mitigate the risk. In scope, this procedure is equivalent to an investigation and may last up to 12 weeks.

In 2025, two data controllers, viz. a municipal public institution and a state institution, contacted the SDPI for prior consultation. In both cases, the requests concerned the planned processing of video and audio data. In one case, the institution intended to install cameras in the staff lounge area on the basis of Article 6(1)(f) of the GDPR, and in the other case, the institution intended to use mobile video surveillance and sound recording devices in the exercise of its public authority functions on the basis of Article 6(1)(e) of the GDPR. After the SDPI determined that these data processing operations could breach the provisions of the GDPR, it issued instructions and recommendations to the data controllers. In the first case, it was recommended to remove cameras from the lounge area and seek other property protection measures that less restrict employee privacy (e.g. locker locks, stricter internal rules, raising employee awareness, etc.). In the second case, it was recommended to clearly and specifically define the circumstances under which audio and/or video data would be processed during inspections, to reassess the lawfulness and proportionality of such processing, and to determine the data storage period and the circumstances for its extension in accordance with the principles of data minimization and storage limitation.

Handling complaints

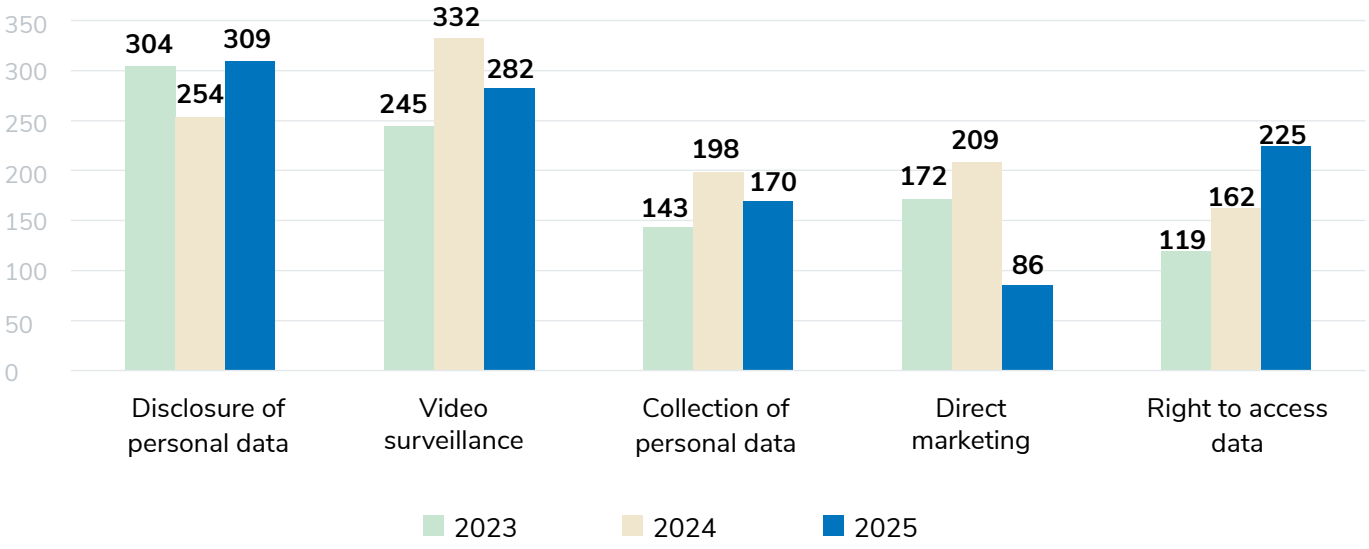
A significant portion of the activities of the SDPI involves handling complaints from the public. In 2025, 2,081 complaints were received, representing a 48% increase compared to 2024, when 1,408 complaints were received.

Complaints were received, representing a 48%.

A comparison of the three-year period shows that the most common areas of complaints remain the same, viz. disclosure of personal data, video surveillance, direct marketing, collection of personal data, and the right of access to data. There is a noticeable trend of a significant increase in complaints regarding the right to be forgotten, with 157 complaints received in 2025, compared to 108 received in 2024 (an increase of 45%).

Chart 5

Areas receiving the largest number of complaints from individuals in 2023–2025 (pcs.)



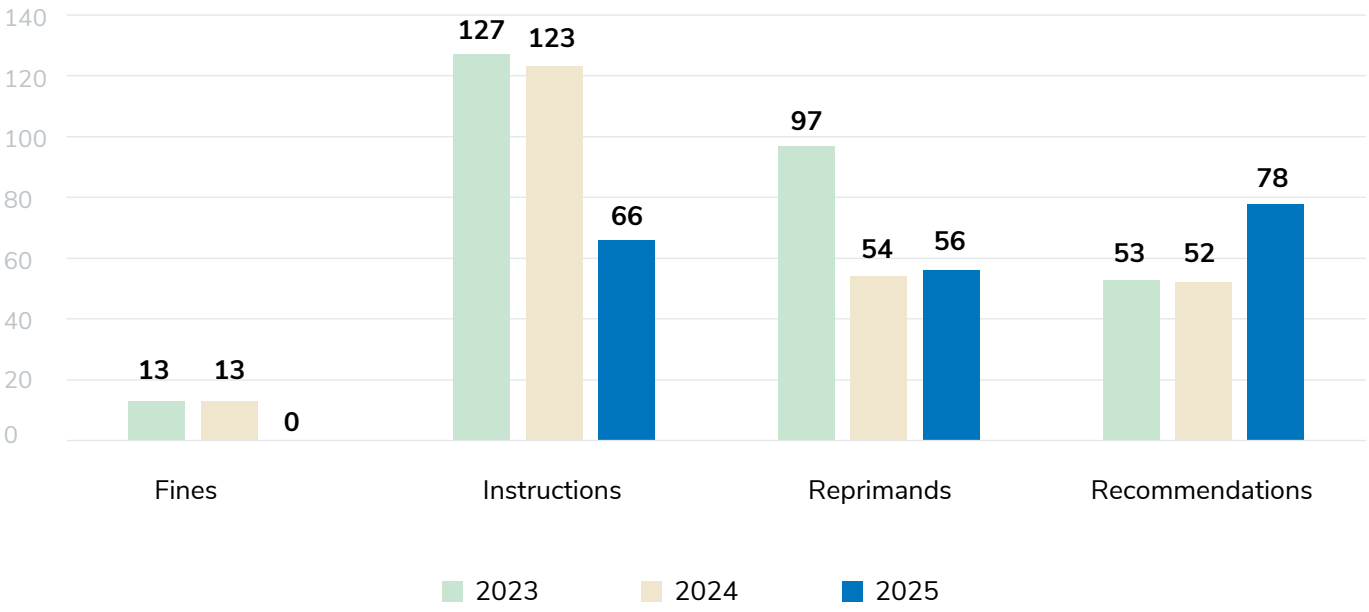
In 2025, the majority of data subjects filed complaints regarding the disclosure of personal data, with 309 complaints received about the inadequate exercise of this right (162 in 2024). A large proportion of the complaints concerned video surveillance – 282 (332 in 2024), disclosure of personal data – 309 (254 in 2024), and breaches of the right of access to data – 225 (162 in 2024).

Measures imposed

The SDPI can take a variety of remedial actions for breaches of the GDPR and other data protection breaches, depending on the circumstances of the case, such as warnings, reprimands, instructions, restriction or prohibition of processing, administrative fines, which can amount to up to 2% or 4% of the total annual worldwide turnover of the previous financial year, or up to EUR 10 million or EUR 20 million, depending on the breach. The SDPI may impose these measures after conducting a scheduled inspection, reviewing a complaint received, or conducting an investigation into a PDB. In 2025, the SDPI issued 66 instructions, 56 reprimands, 78 recommendations, and 2 warnings to organisations following findings of breaches. No fines were imposed following the review of complaints filed by individuals.

Chart 6

Number of impact measures applied in 2023–2025 (pcs.)



Significant decisions of the SDPI

In order to ensure transparency and promote best practices, the SDPI has been publishing its decisions on its website since 2025. Below are a few notable cases in which the SDPI took remedial action regarding the improper processing of personal data.

Case 1

The Inspectorate received a complaint from the complainant regarding the actions of the Municipality Administration in checking (reviewing) the property owned by the complainant in the Real Property Register (hereinafter referred to as the RPR) on numerous occasions, although the complainant is not related to the person complained against. The Municipality Administration stated that, in the exercise of its functions, it had received standard extracts from the RPR containing the complainant's data, which were unnecessary for its purposes, and therefore did not even review them.

The Inspectorate concluded that the Municipality Administration did not prove that by performing multiple searches in the RPR and obtaining extracts from the RPR containing the complainant's personal data(name and surname, personal identification number, identification data of the land plot (RPR object), address of the land plot, parts of the ownership right to the land plot, etc.), it has lawfully processed the complainant's personal data and, therefore, concluded that the actions of the person complained against did not comply with any of the conditions for lawful processing set out in Article 6(1) of the GDPR, and that, accordingly, the person complained against breached the principle of lawfulness set out in Article 5(1)(a) of the GDPR. The Inspectorate did not assess the actions of the person complained against under Article 5(1)(c) of the GDPR, since the Municipality Administration itself acknowledged

that, when conducting RPR searches for the purposes it had established, the processing of the complainant's personal data was not necessary for it at all.

The Municipality Administration was instructed to ensure that, when performing functions for which it is necessary to obtain data from the RPR but not to process personal data, personal data is not processed, including the extraction of personal data. It was also decided to conduct monitoring activities regarding the State Enterprise Centre of Registers concerning the implementation of the provisions of Article 25 of the GDPR. These actions are linked to the finding in the decision that the standard extracts from the RPR provided to data recipients under the concluded contracts include not only data on the real property object but also the personal data of all holders of rights in rem, even though such data is not always necessary for the performance of the functions of municipalities. The Inspectorate stated that it is necessary to implement the principle of data protection by design and to allow access only to the data related to the immovable property (without the owners' personal data).

Case 2

The complainant, a vehicle owner, filed a complaint alleging that the Lithuanian Association of Technical Inspection Companies (hereinafter referred to as the Association) has transferred her vehicle's technical inspection and mileage data to a third party under a data provision agreement, which was used to compile paid vehicle history reports. The complainant argued that such data allows her to be identified and affects her interests.

The Association argued that the data transmitted is not personal data as it is only the technical data of the vehicle transmitted in a pseudonymised form (VINH).

The Inspectorate, relying on the judgment of the Court of Justice of the European Union of 4 September 2025 in case No. C-413/23, assessed whether the vehicle technical inspection and mileage data transferred under the agreement should be considered personal data. In that judgment, the Court held that, if it cannot be excluded that third parties will be able to reasonably attribute the pseudonymised data to the data subject by means such as, for example, by cross-checking it with other data in their possession, the data subject must be considered to be an identifiable person, both with regard to that transmission and to any subsequent processing of those data by those third parties.

In this case, the Association stated that it processes the number of a driver's license or an identity document, which proves that the Association has additional information allowing it to link vehicle-related information to a natural person – the owner or operator of the vehicle. Furthermore, the Association stated that the agreement provides that the third party will use the data received to compile and sell vehicle history reports on its platform; that these reports may include, inter alia, technical inspection history, ownership history, accident or damage reports and other relevant historical data.

The Inspectorate noted in its decision that identifiers, such as the VIN or the identity document, can be used to link a vehicle and its history to a specific data subject and that, therefore, despite pseudonymisation, the data transmitted to a third party falls within the category of personal data.

The Inspectorate found that the transfer of the complainant's personal data to the third party was unlawful and breached the principle of lawfulness enshrined in Article 5(1)(a) of the GDPR. The Association has been instructed to immediately cease providing the company with data relating to the complainant until the processing of the data complies with the requirements of Article 6(1) of the GDPR.

Case 3

The Inspectorate received complaints from the complainants, who are natural persons, regarding the actions of an insurance brokerage company and two insurance companies in processing personal data, viz. that the insurance brokerage company has transferred the complainants' personal data to the insurance companies so that they could provide insurance offers, and that the latter have checked the complainants' credit ratings in a third-party database.

The insurance brokerage company argued that in order to provide a proper service, it had to pass on the collected data to the insurance companies, otherwise it would not be able to provide the service as defined in the Law on Insurance. In view of the above, the Inspectorate assessed that the insurance brokerage company based the processing of personal data on Article 6(1)(c) of the GDPR (legal obligation). The Inspectorate found that the legislation imposes an obligation on the distributor of insurance products to inform the policyholder of the expiry of the term of a regular insurance contract and of the obligation to insure the vehicle, but does not impose an obligation to prepare, send offers from insurance companies or to transmit the personal data of policyholders to the insurance companies for the purpose of making such offers. Accordingly, the Inspectorate decided that such a transfer of personal data could not be based on a legal obligation, i.e. on the basis of Article 6(1)(c) of the GDPR, and found a breach of the principle of lawfulness enshrined in Article 5(1)(a) of the GDPR and of the provisions of Article 6(1) of the GDPR.

The insurance companies argued that they had a legitimate interest (Article 6(1)(f) of the GDPR) in checking the credit rating of individuals in order to determine the standard price of compulsory civil liability insurance for vehicle operators. The Inspectorate concluded that, in this case, the processing of credit rating data could not be based on Article 6(1)(f) of the GDPR, as no data or objective assessments had been provided to justify the necessity of the processing and the existence of a balance of legitimate interests.

One insurance company also indicated that credit rating data of individuals (policyholders) are processed in accordance with Article 6(1)(b) of the GDPR for the purpose of entering (or offering to enter) into an insurance contract. In this case, the Inspectorate found that the insurance company did not have any contract with the complainants, nor did it have a request from the complainants to enter into such a contract, and therefore Article 6(1)(b) of the GDPR is not applicable.

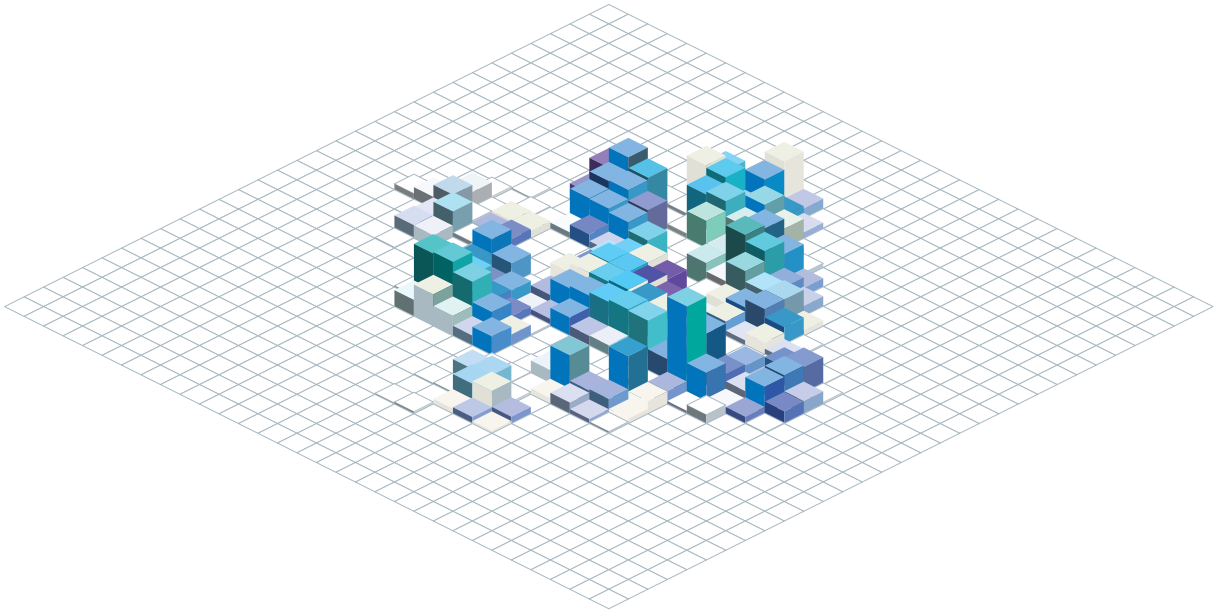
The Inspectorate also stated that insurance companies cannot lawfully process personal data which have been unlawfully transferred to them, even if the condition for lawful processing they claim is hypothetically appropriate. According to the general principle of law stating that

law does not arise from injustice *(ex injuria jus non oritur)*, the insurance companies' checking of the complainants' data in a database operated by a third party cannot be considered lawful on the sole ground of the unlawful receipt of the data from the insurance brokerage company. The Inspectorate found the complaints to be justified and found a breach of the principle of lawfulness enshrined in Article 5(1)(a) of the GDPR and of the provisions of Article 6(1) of the GDPR. An instruction was issued to the insurance brokerage company to cease providing data subjects' personal data to insurance companies for the purpose of initiating offers until the processing of personal data is in line with the requirements of Article 6(1) of the GDPR, and instructions were issued to insurance companies to cease processing data subjects' credit rating data for the purpose of insurance risk assessment.

Case 4

The Inspectorate has received a complaint about the possible unlawful processing of personal data by the Company (data controller) and a debt collection company. The complainant submitted that the Company has unlawfully transferred his personal data relating to a debt to a debt collection company.

The Inspectorate found that the data transfer did not comply with the requirements of Article 28(3) GDPR. Such conclusion was reached when it was established that the debt collection company acted as an ancillary processor (sub-processor) and received the complainant's personal data from the initial processor, even though there was no data processing agreement between them, as required by Article 28(3) of the GDPR. The Inspectorate decided that such a discrepancy did not in itself lead to unlawful processing and rejected the complainant's complaint for unlawful processing of personal data; however, it issued instructions to the Company (data controller) and the initial processor for the established breach of Article 28(3) of the GDPR.

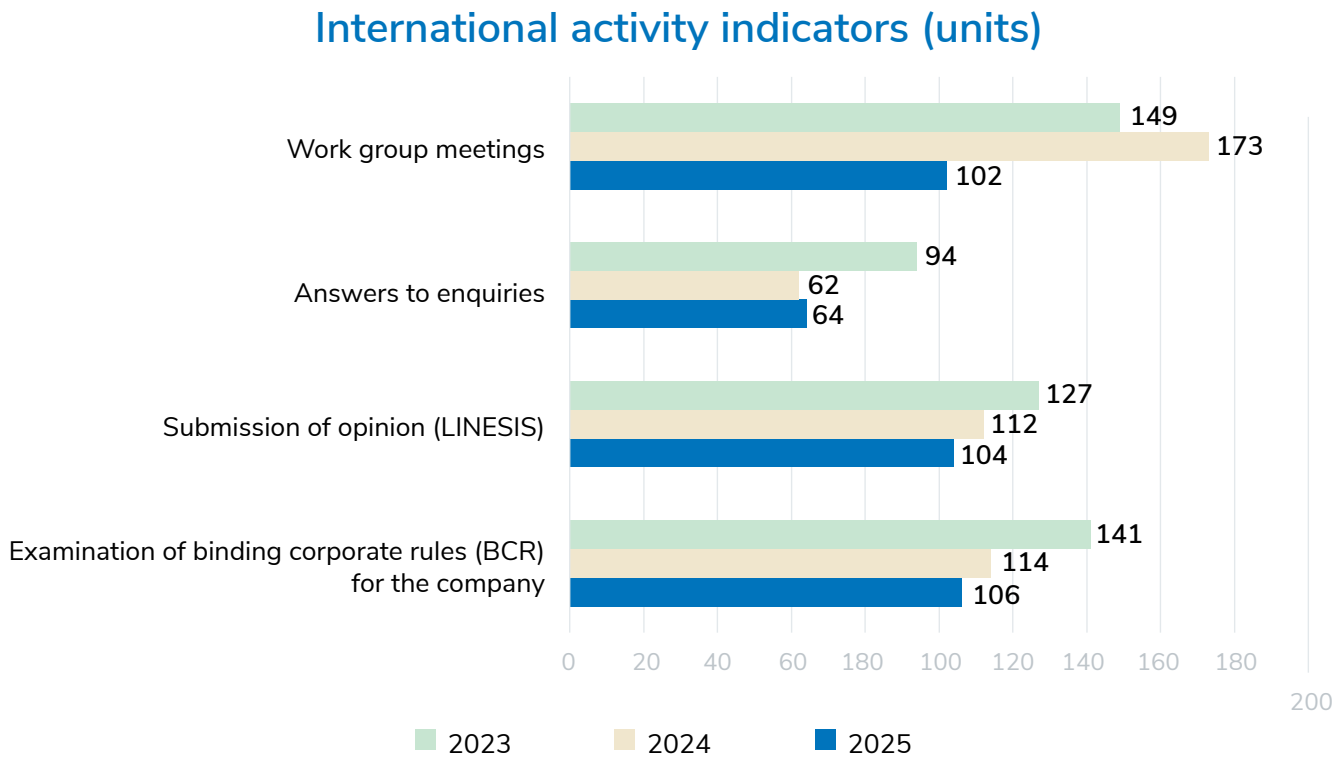


INTERNATIONAL ACTIVITIES

The GDPR establishes a mandatory role for national supervisory authorities within the EDPB and its sub-groups; therefore, during the reporting period, the SDPI was actively engaged in international activities in this area and cooperated with supervisory authorities from other Member States. Participation was primarily focused on the activities of EDPB sub-groups and other international working groups, where documents (opinions, guidelines, etc.) important for the consistent application of the GDPR across the EU were drafted and coordinated; views were also exchanged with other EU supervisory authorities on various issues related to the development of best practices via IMI or using the internal EDPB tool, viz. *Confluence*, intended solely for supervisory authorities of Member States.

In 2025, the Inspectorate participated in a total of 102 meetings and other working sessions of working groups and sub-groups of the EDPB, other EU institutions and international organizations.

Chart 7



The SDPI cooperates with the supervisory authorities of the EU and European Economic Area countries in the handling of complaints through the consistency mechanism. In 2025, 34 international complaints were received in which the SDPI acts as lead supervisory authority. During this period, acting as the lead supervisory authority, the SDPI adopted 28 decisions which were coordinated with the supervisory authorities concerned. As of the end of 2025, the SDPI, as the lead supervisory authority, has handled a total of 78 international cases.

Data protection authorities from the Baltic states of Lithuania, Latvia and Estonia meet annually to deepen cooperation and exchange best practices. During these annual meetings, the heads and staff of the data protection authorities from the Baltic states discuss the results of the previous year's activities and exchange practices on the application of data protection requirements. On 4-5 September 2025, such meeting took place in Vilnius.

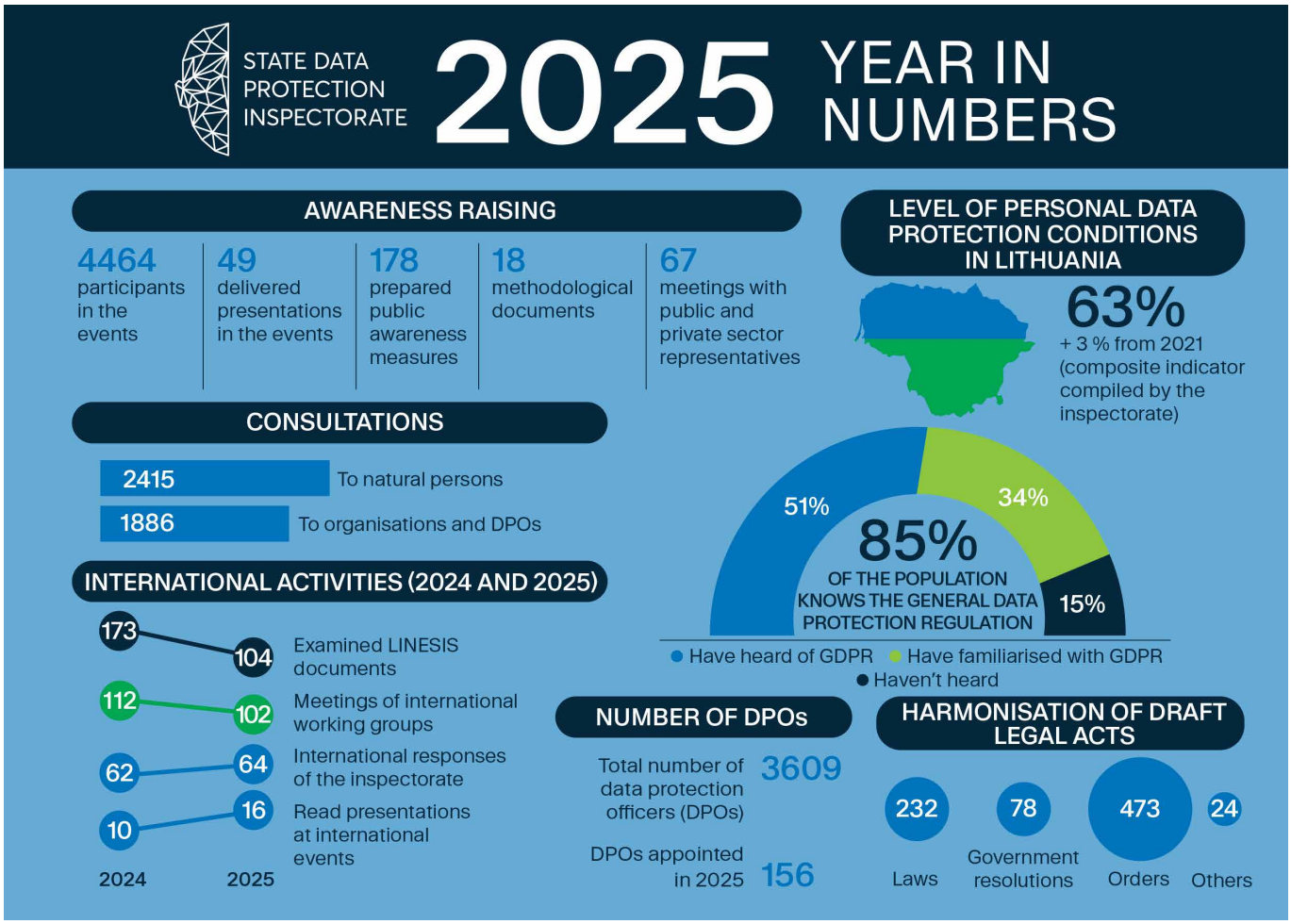
Lithuania shared its experience at the International Privacy Symposium, held in Italy in May. Dijana Šinkūnienė, Director of the SDPI, presented Lithuania's experience in a panel discussion on the topic „Opening up medical research: the legal basis for the secondary use of data in medical research", and discussed with other EU data protection experts how to ensure a balance between privacy and public interest in medical research. The discussion also addressed the challenges and opportunities of reconciling the public interest in using health data for scientific research and innovation with the need to ensure the protection of personal data.

At the Baltic Privacy and Innovation Summit 2025 held in Vilnius in June, Dijana Šinkūnienė, Director of the SDPI, discussed with other data protection experts how to balance the constantly evolving technology and legal regulation. The conference, organised by the Lithuanian Data Protection Officers Association (LDPOA), was also attended by Pille Lehis, Head of the Estonian Data Protection Inspectorate, as well as data protection experts from other public and private institutions and organisations, and the academic community. The main topics of discussions and presentations were the regulation of the AI and the promotion of innovation, the role of data in modern business strategies, the evolution of the personal data protection system, implementation trends and future needs.

The Director of the SDPI attended the high-level EDPB meeting held in Helsinki, Finland, in July 2025. During the meeting, the heads of the data protection supervisory authorities of the EU Member States, representatives of the European Commission and the European Data Protection Supervisor (EDPS) discussed strategic directions for data protection: simplifying the application of the GDPR, ensuring consistent implementation of the Regulation and strengthening inter-institutional cooperation. To achieve these objectives, *the Helsinki Statement on Enhanced Clarity, Support and Engagement: A Fundamental Rights Approach to Innovation and Competitiveness* was adopted. The Helsinki Statement sets out initiatives to facilitate compliance with the GDPR, in particular for micro, small and medium-sized organisations, to enhance consistency in the application of the GDPR and to promote cooperation between supervisory authorities.

Representatives of the Inspectorate participated in the Spring Conference of European Data Protection Supervisors 2025, which discussed current trends and practical challenges in data protection regulation.

PUBLIC INFORMATION, EDUCATION AND CONSULTATION



As one of its priorities, the SDPI focuses on prevention and education. The aim is to reach people not only in the capital city but also in the regions.

Table 2

ACTIVITIES	2023	2024	2025
Consultations provided	4 163	4334	4301
Public information materials prepared	95	93	178
Methodological documents prepared	22	25	18
Participation in meetings with the public and private sectors	79	112	67
Participation in events	23	18	25
Presentations given at events	44	38	49
Number of event participants	14 731	6288	4464

Consultations

Providing consultations is one of the key measures for ensuring the consistent application of GDPR rules. In 2025, the SDPI provided a total of 4,301 consultations, of which 1,797 were to data controllers, 2,415 to data subjects, and 89 to DPOs. More consultations were provided by phone, viz. 3,208 (3,149 in 2024). The number of consultations provided by other means remains similar: 234 by an official letter (251 in 2024), 824 by e-mail (902 in 2024), 35 on the premises of the SDPI (32 in 2024).

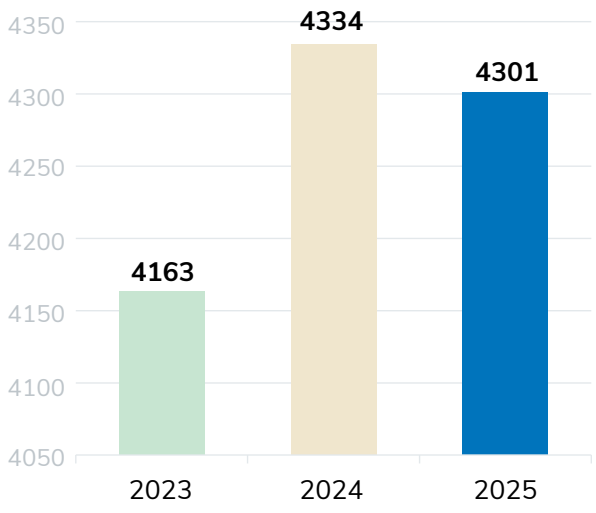
The number of consultations provided in 2022-2024 has increased steadily (3,691 in 2022, 4,136 in 2023, 4,334 in 2024);

The current trend shows that the number remains similar.

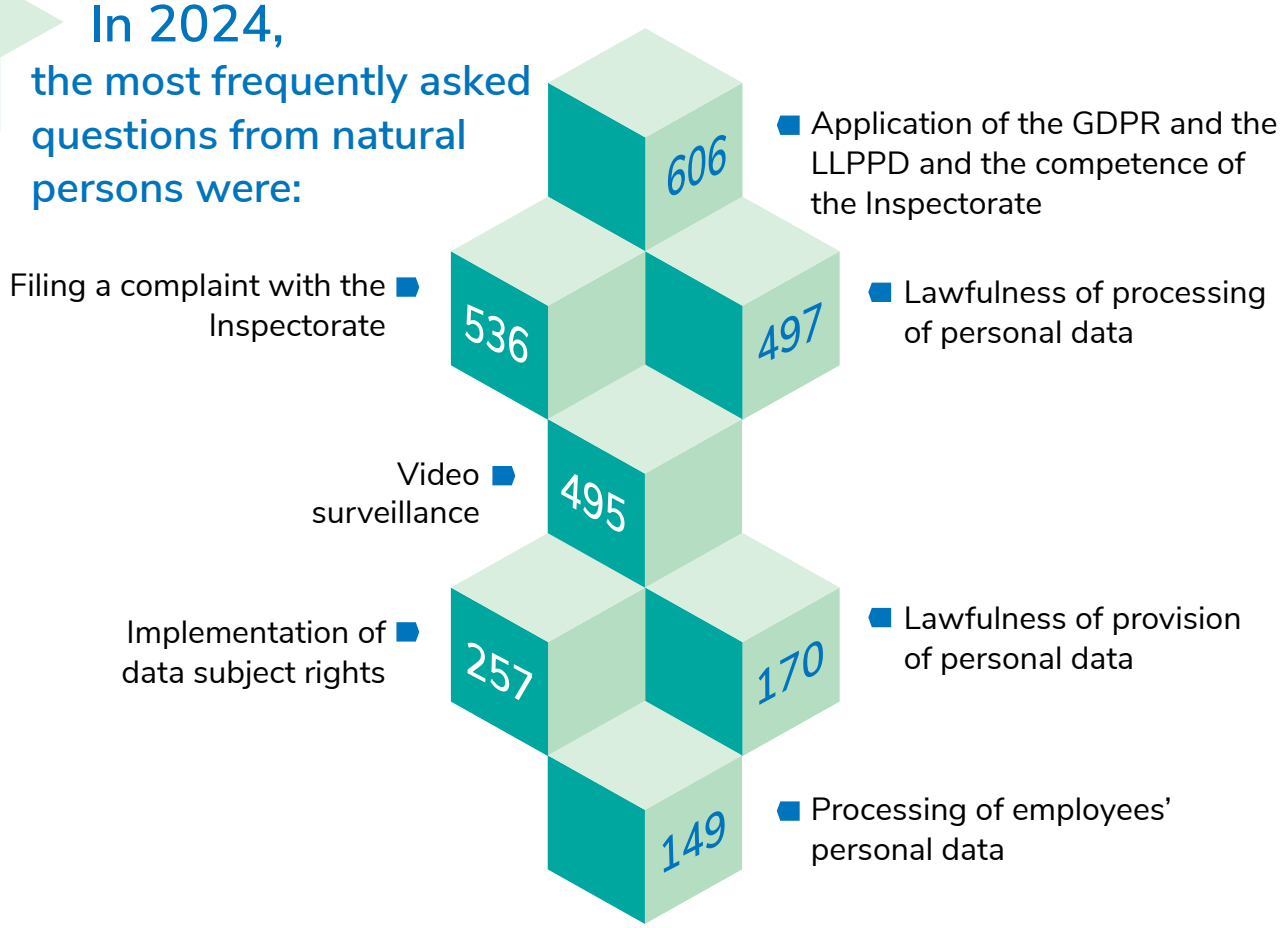
This is influenced by the fact that the SDPI no longer has the capacity to allocate more staff to carry out this activity.

Chart 8

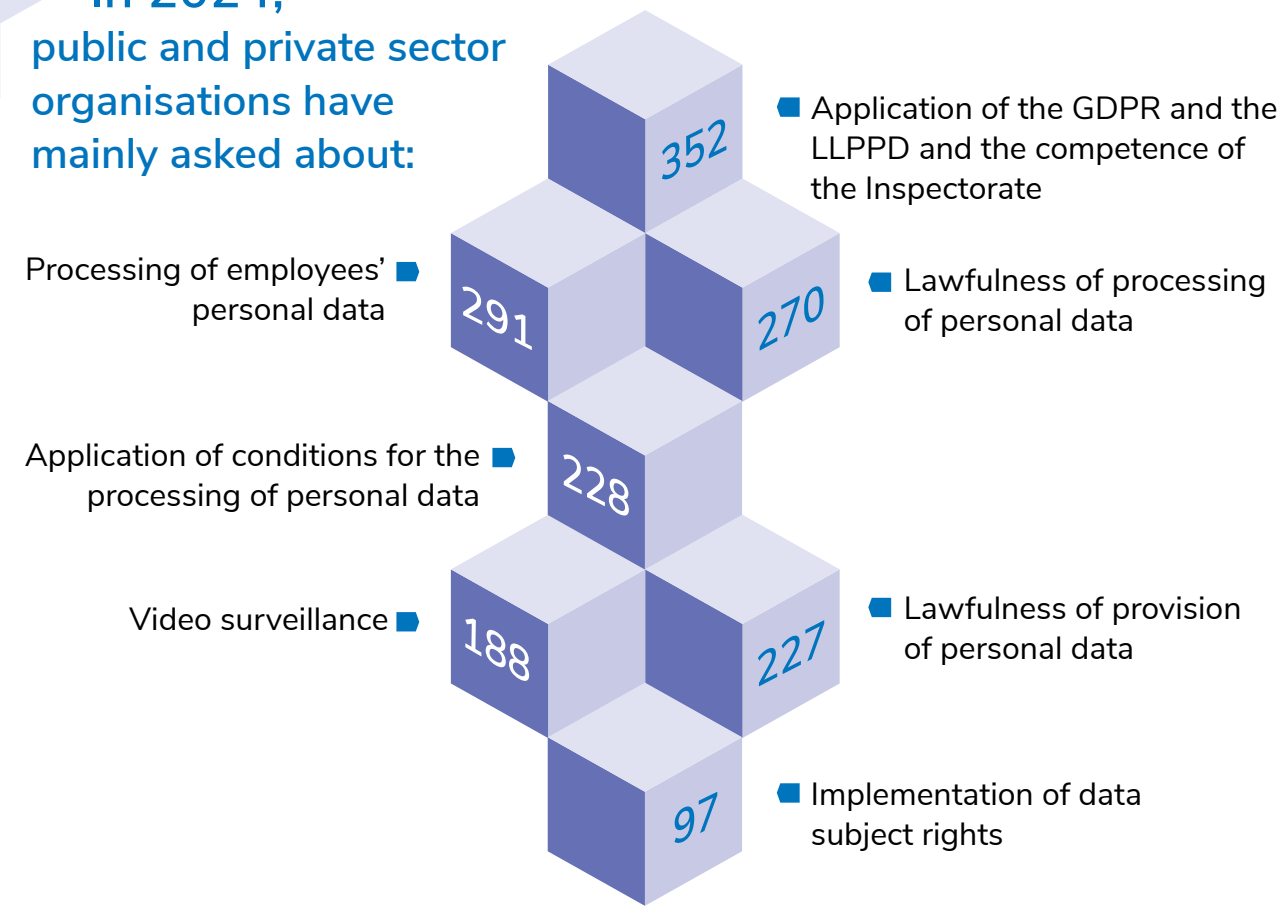
Number of consultations provided in 2023–2025 (pcs.)



In 2024,
the most frequently asked questions from natural persons were:



In 2024,
public and private sector organisations have mainly asked about:



Methodological support

In order to provide more detailed information on relevant issues related to the protection of personal data and privacy to a wider range of stakeholders, in 2025 the SDPI has focused on the development of methodological information that is useful for both organisations and citizens. 18 methodological tools have been developed in 2025: 8 FAQs, 4 Inspectorate summaries and 6 recommendations.

"Recommendation on the Application of Personal Data Protection Requirements" in Legilation is intended for public sector organisations involved in drafting legal acts. Quality legislation is essential to ensure trust in the public sector and its processing of personal data. The purpose of the recommendation is to provide practical advice to help legislators implement the key requirements of the legal acts on the protection of personal data.

Recommendation "Tracking Pixels and How to Block Them" is intended for the general public. It will help people better understand what tracking pixels are and how their use can be blocked by the individual.

In order to raise public awareness of the steps that should be taken in the event of a cyber incident involving personal data, a recommendation has been drafted to address the types of cyber incidents, stating the steps that should be taken by data subjects in the event of a cyber incident, and providing recommendations that will help better protect personal data.

A recommendation for organisations regarding the DPO has been prepared. Its purpose is to help organisations understand the requirements set forth in the GDPR regarding the appointment of a DPO, his duties, and responsibilities, as well as address the questions organisations most frequently raise when seeking consultation from the SDPI.

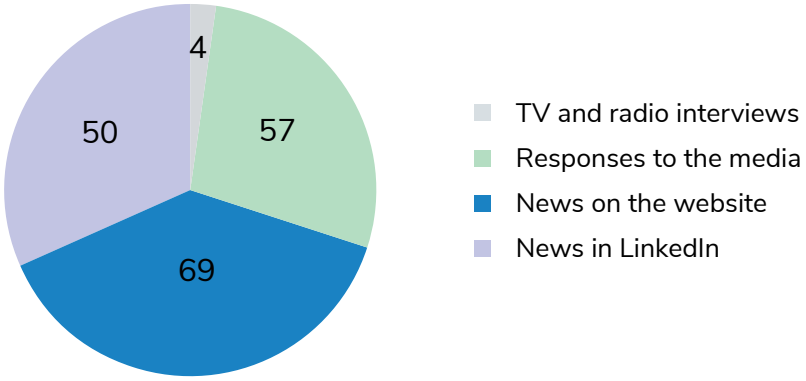
In response to public needs, recommendations on PDB and on requests for personal data have been updated. Methodological information has also been developed on the use of artificial intelligence (AI) systems, the data subject's right of access to data, risks of identity theft, etc.

Public information

The SDPI focuses on disseminating information about its activities and functions, as well as providing commentary and advice on how to deal with organisations and individuals who are confronted with potential data protection or security breaches. These situations are relevant for both the public and private sectors, and the SDPI has therefore chosen to use a variety of public information channels and tools in 2025: provided 57 responses to media inquiries; participated in four TV or radio programmes and gave interviews; published 69 news items on its website and 50 posts on the social network LinkedIn for preventive purposes.

Chart 9

Breakdown of the number of informational materials prepared in 2025 (numbers)



Events in Lithuania

According to a survey of Lithuanian residents conducted in 2025, 85% of the country's population has heard of the GDPR. In an effort to raise public awareness of data protection and reach a wider audience, the SDPI prioritized the online format for organizing events.

One of the most important annual events of the SDPI is the Data Protection Day Conference, organised to mark the International Data Protection Day. Representatives of the Inspectorate, the NCSC and the academic community gave presentations and shared their insights at the conference „Privacy in the Digital Environment: Challenges and Opportunities". The event was attended by 200 participants from business and the public sector.

Organisations seeking to improve their employees' qualifications often prefer to receive guidance in the form of training sessions (seminars). In response to the needs, the SDPI organised 3 online events – for health care institutions, IT professionals and DPOs.

During the seminar for employees of health care institutions, the key requirements of the GDPR and aspects of their application were presented, the rights of data subjects, key requirements for data provision and video surveillance in health care institutions, the processing of employees' personal data, and other issues relevant to medical staff were discussed.

Webinar „Law and Technology" focused on cyber security and personal data protection.

The annual DPO online training reviewed the consultations, complaints and recommendations provided by the SDPI in 2025, shared methodological support tips, publicly available tools for verifying compliance with the GDPR, and discussed other issues of interest to DPOs.

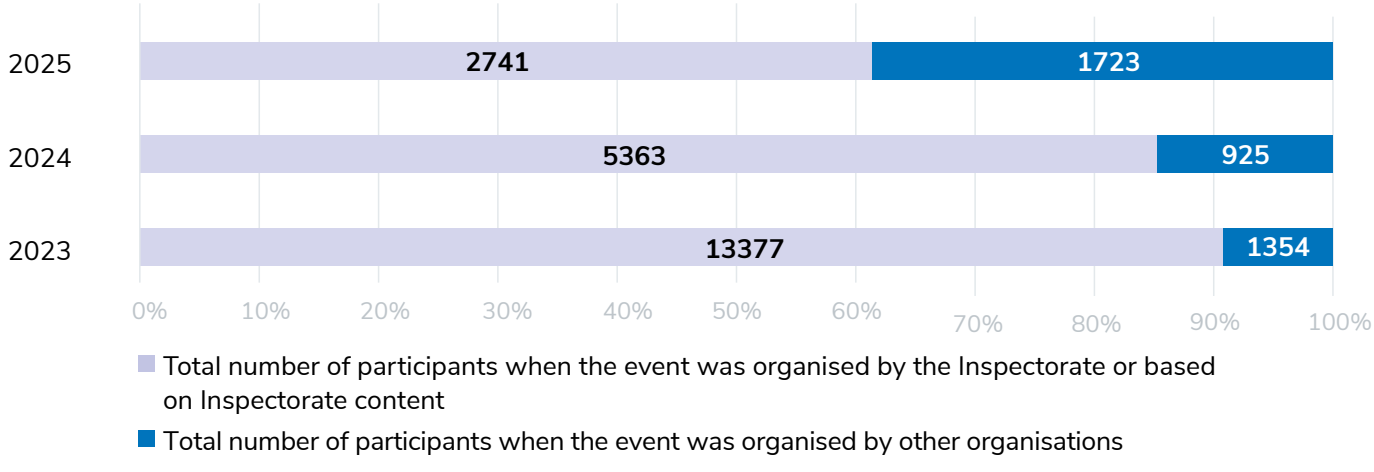
In collaboration with the Lithuanian Banking Association, a conference for the Baltic banking sector titled “Data Protection in Finance: Navigating GDPR, Artificial Intelligence, and Cybersecurity Challenges” was organized in Vilnius. The conference was attended by a representative of the Data Protection Law and Policy Unit of the European Commission, heads of the national data protection authorities of Lithuania, Latvia and Estonia, as well as representatives of various institutions, banks and technology businesses from all three Baltic states. During the event, experts explored the application of AI in the financial sector, its potential and ethical and legal aspects; delved into the processing of personal data in the context of anti-money laundering, discussed fraud prevention and the balance between privacy protection and the implementation of state-of-the-art security standards, and reviewed the factors shaping the future of the financial sector and data protection in the Baltic region.

In total, SDPI representatives participated in 25 events in Lithuania in 2025, delivering 49 presentations.

- Presentations were delivered at 5 trainings,
- 7 conferences,
- the SDPI representatives participated in 5 discussions and other types of events.
- In 2025, the total number of participants in the events was 4,464 (6,288 in 2024).

Chart 10

2023–2025 m. Number of event participants distribution (units)



LEGISLATION ON PERSONAL DATA PROTECTION

The involvement of the SDPI in legislative activities was a significant part of its activities in 2025. Although the number of draft legal acts received for coordination in 2025 increased slightly compared to 2024 (807 legal acts received in 2025, compared to 768 received in 2024), an increase in the number of draft legal acts submitted for coordination has been observed over the past three years.

During the reporting period, the SDPI provided comments and suggestions

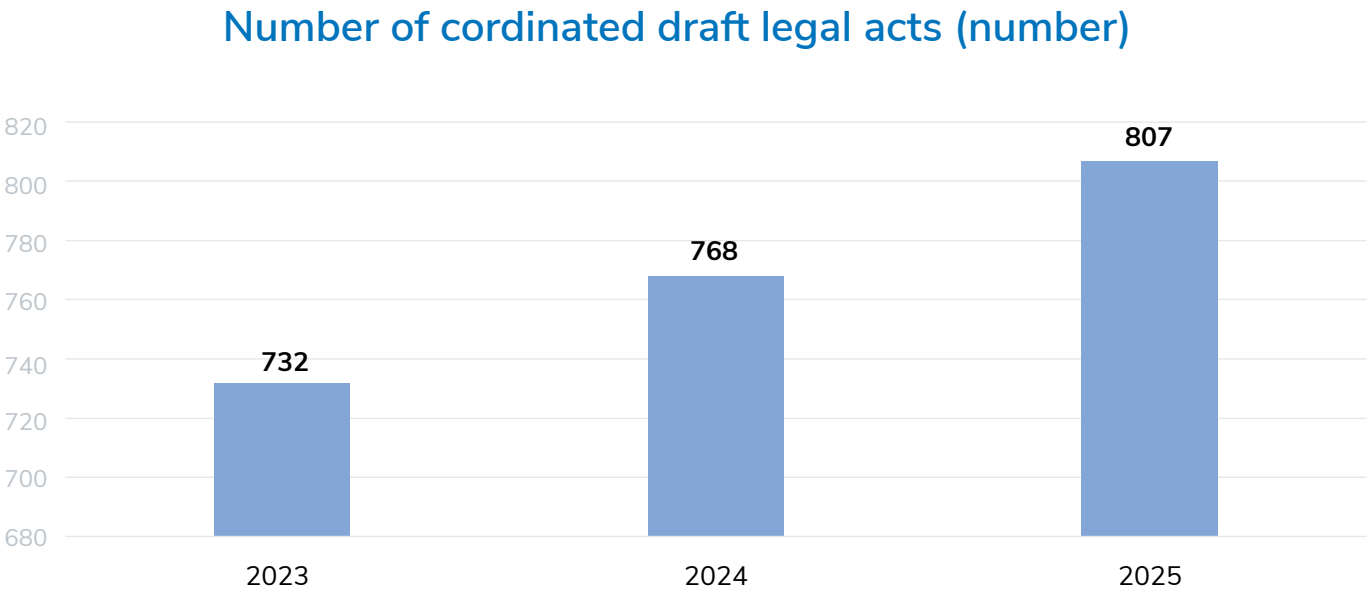
on 807

draft legal acts submitted by other institutions for coordination, including:

- **473 orders;**
- **232 laws;**
- **78 Government decisions;**
- **24 other legal acts.**

In addition, it should be noted that at the request of organisations, the SDPI has co-ordinated as many as 94 draft legal acts on a working basis (not included in the statistics), which means that a total of 901 legal acts have been coordinated in 2025.

Chart 11



It is worth noting several of the draft laws submitted for coordination in 2025 that are significant for the public or the activities of the State Data Protection Inspectorate:

1. Draft law amending Law No XI-1253 amending the Republic of Lithuania Law on Consumer Credit, aimed at transposing the provisions of Directive (EU) 2023/2225 of the European Parliament and of the Council of 18 October 2023 on credit agreements for consumers and repealing Directive 2008/48/EC into national law;
2. Draft Law No XVP-306 amening Articles 18 and 29 of Republic of Lithuania Law No X-1666 on the Chief Official Ethics Commission;
3. Draft law amending Articles 2, 5, 6, 7, 9, 10, 11, 12, 13, 14, 15, 19, 20, 21, 24, 28, 31, 33, 34, 36 and 40 of Republic of Lithuania Law No VIII-667 on Tourism;
4. Draft Law No XIVP-4198 amending Articles 79 and 80 of Constitutional Law No XIV-1381 on the Approval, Entry into Force and Implementation of the Electoral Code of the Republic of Lithuania, and Draft Constitutional Law No XVP-104 amending Articles 33, 75, 78 and 193 of the Electoral Code of the Republic of Lithuania;
5. Draft law amending Article 81 of Law No IX-2135 on Electronic Communications;
6. Draft law amending Articles 2, 5, 7, 9, 11, 13, 14, 18, 19, 24, 29, 33, 40, 43, 45, 49, 50, 55, 57, 60, 64, 641, 69, 70 and 71 of Republic of Lithuania Law No VIII-1861 on Intelligence.

One of the main challenges faced by the institutions submitting legal acts for coordination is the definition of the processing of personal data, in particular their public disclosure, in the legal act in the light of the interpretations of the EU and Lithuanian courts and the implementation of Article 6(3) of the GDPR (in particular, the identification of the personal data to be processed in the implementing legislation, the justification of the duration of the retention of personal data).

It should be noted that the SDPI not only coordinated the draft legal acts, but also drafted them itself when necessary. For example, the Security Regulations of the State Data Protection Information System and the State Data Protection Information System have been approved, the Description of the Procedures for Consultation with the SDPI has been updated, the Guidelines for Ensuring Uniform and Quality Consultation Practices with Individuals have been prepared, etc.

Oversight of the implementation of the Law Enforcement LLPPD

In addition to the GDPR, the SDPI also oversees the application of the provisions of the Law Enforcement LLPPD that fall within its competence. This legal act is unique in that it regulates aspects related to the processing of personal data by law enforcement agencies.

It is important to note that the EU has recently been analysing the functioning of the rules on personal data protection in the field of law enforcement. in 2025, the SDPI completed two questionnaires providing information on the situation in Lithuania:

in June 2025, the SDPI provided information for a questionnaire on the practices, challenges, lessons learned and other insights on the application of Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016, as transposed into the Law Enforcement LLPPD (the questionnaire was received from Denmark, as the Member State that will hold the upcoming EU Council Presidency).

In October 2025, a questionnaire prepared by the EDPB regarding the application of Directive (EU) 2016/680 was completed. As a result, the EDPS report "Contribution of the EDPB to the European Commission's evaluation of the Data Protection Law Enforcement Directive ("LED") under Article 62 LED" was adopted on 15 January 2026. In line with other EU supervisory authorities, the Inspectorate noted in the questionnaire that the practical application of Directive (EU) 2016/680 poses certain challenges, and provided summary information on the implementation practices and trends in the application of Directive (EU) 2016/680, based on the operational experience of the authority.

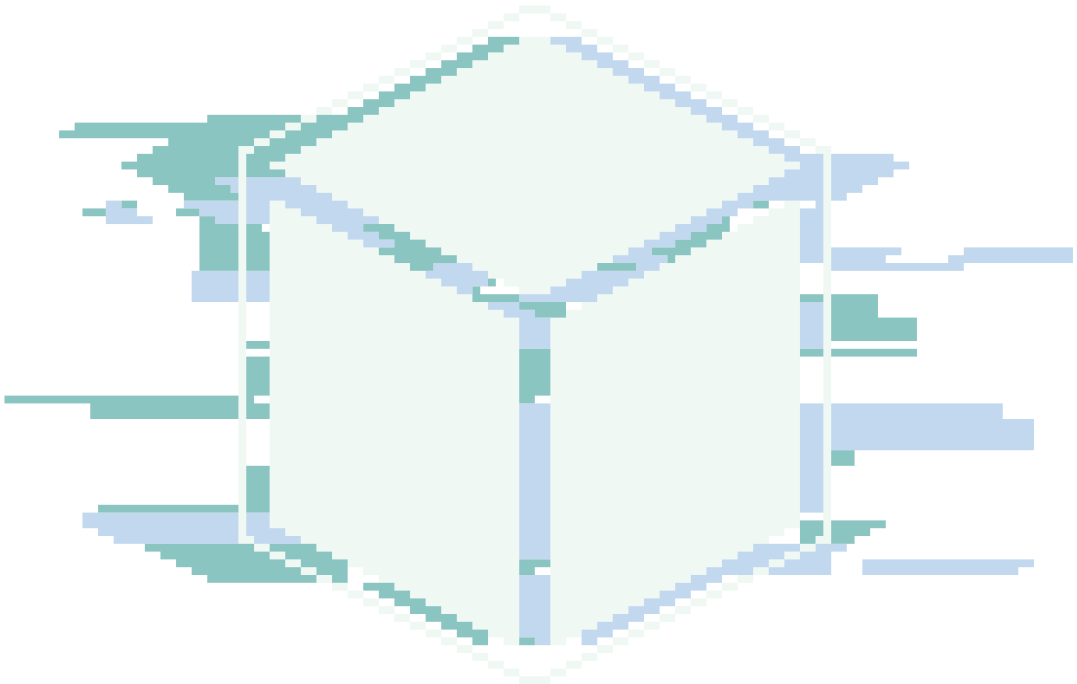
The provision of information for the questionnaires is important for the subsequent assessment of the supervision of the processing of personal data in the Lithuanian and EU context.

It should be noted that it is extremely rare for natural persons to contact the SDPI in relation to the processing of personal data by law enforcement authorities, which is subject to the requirements of the Law Enforcement LLPPD. One case is worth mentioning.

The SDPI received a complaint from the Complainant regarding the actions of the Police Commissioner's Office alleging that the Police Commissioner's Office has provided the Municipality Administration with information about his reports to the police, their number and reasons, and has also forwarded copies of procedural documents for the purpose of a potential investigation into the Complainant's misconduct being conducted by the Municipality Administration. The Complainant stated that his calls to the police were not related to the performance of his duties.

The SDPI concluded that the Police Commissioner's Office failed to assess the lawfulness, proportionality and the specific purpose of the provision of the requested data, therefore the transfer of the Complainant's personal data to the Municipality Administration was unlawful. Thus, the Police Commissioner's Office violated Article 3(1)(1) and (2) and Article 7(2) of the Law Enforcement LLPPD and failed to prove that such provision of data was permitted by law.

The Police Commissioner's Office was instructed is to ensure that personal data collected for the purposes of the prevention, investigation or prosecution of criminal offences are not disclosed and processed for other purposes, unless expressly permitted by law.



APPOINTMENT OF DATA PROTECTION OFFICERS IN LITHUANIA

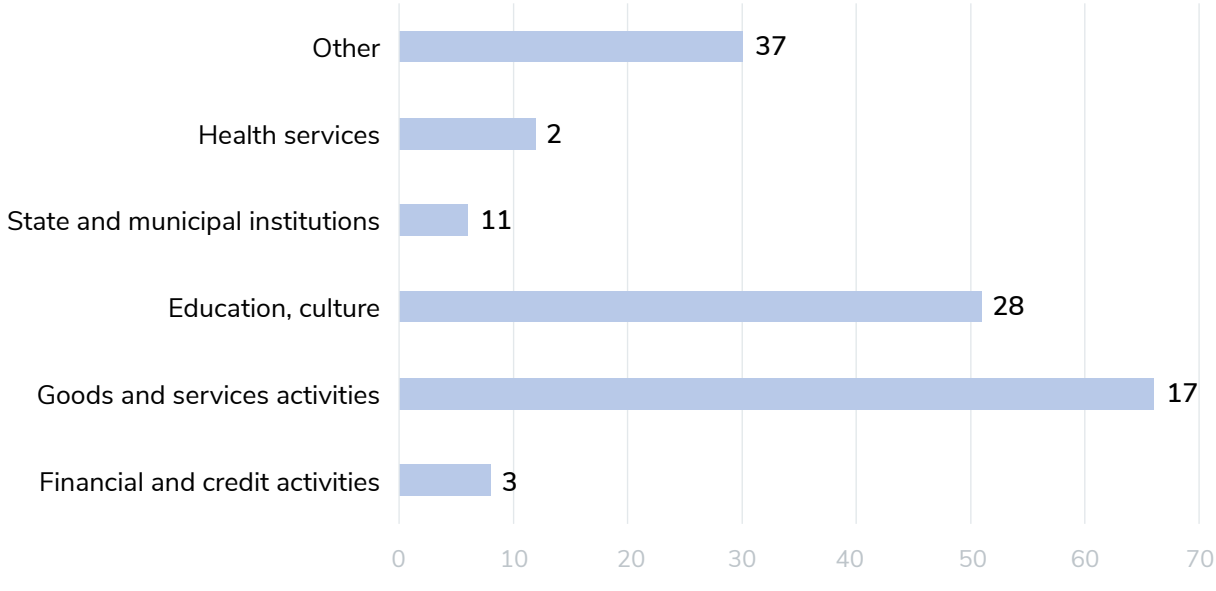
Since the introduction of the GDPR, a total of 3 609 DPO appointments have been notified to the SDPI. In 2025, 156 DPOs were appointed in Lithuania.

As in previous years, organisations faced challenges in appointing DPOs, viz. lack of resources, lack of expertise of DPO candidates. In order to contribute to the development of the competences and practical knowledge of DPOs, the SDPI has focused on methodological support activities for this target group in 2025:

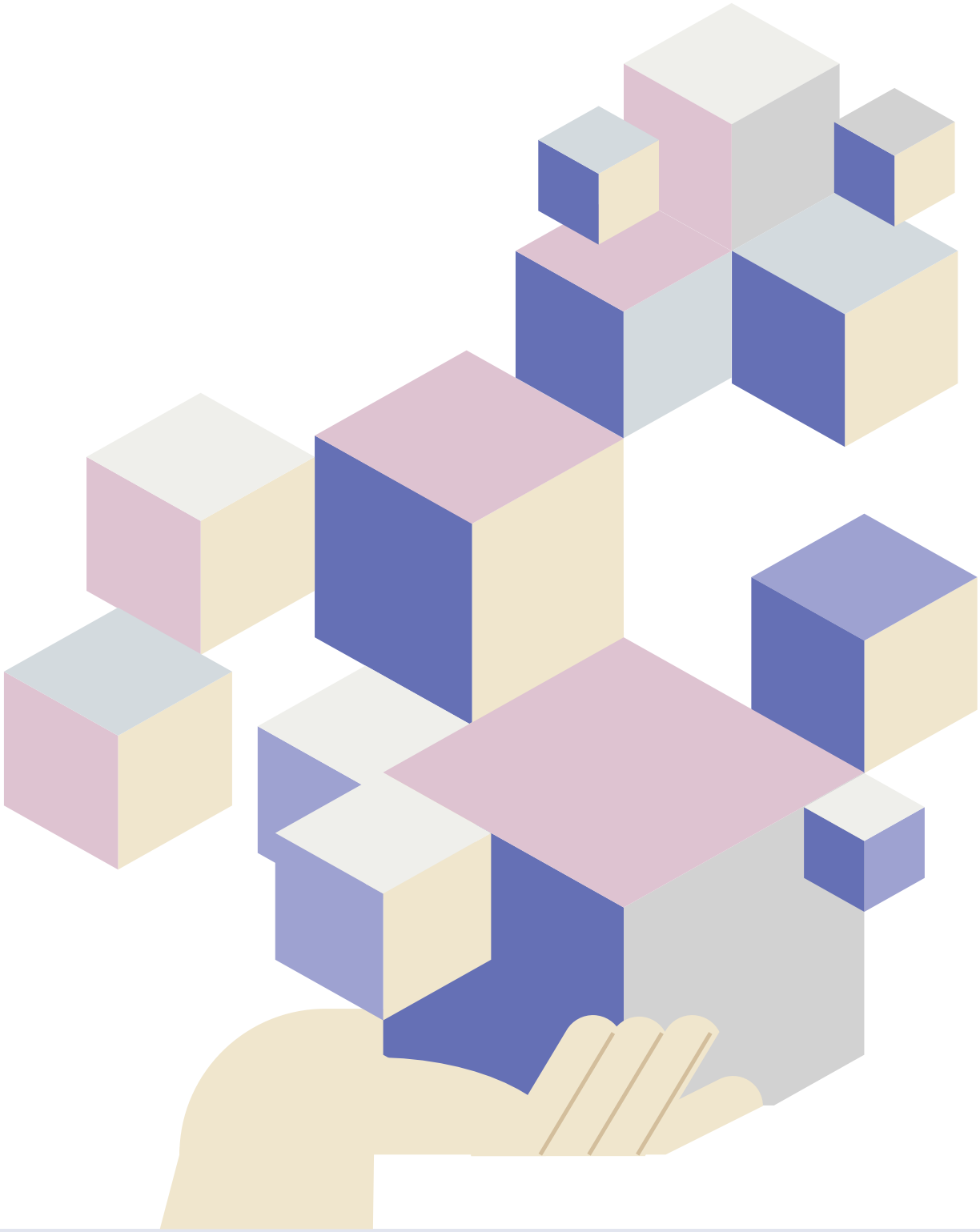
- Recommendation on DPO has been drafted, with the aim of helping organisations understand the requirements set forth in the GDPR regarding the appointment of a DPO, his duties, and responsibilities;
- Annual free online DPO training was organised, which was aimed not only at Lithuanian DPO, but also at managers of organisations, personal data protection professionals, IT specialists, and anyone who has to deal with situations related to the processing of personal data in their daily work;
- Meetings with the Lithuanian Association of Data Protection Officers were organised to help the DPOs address relevant issues regarding the application of the GDPR.

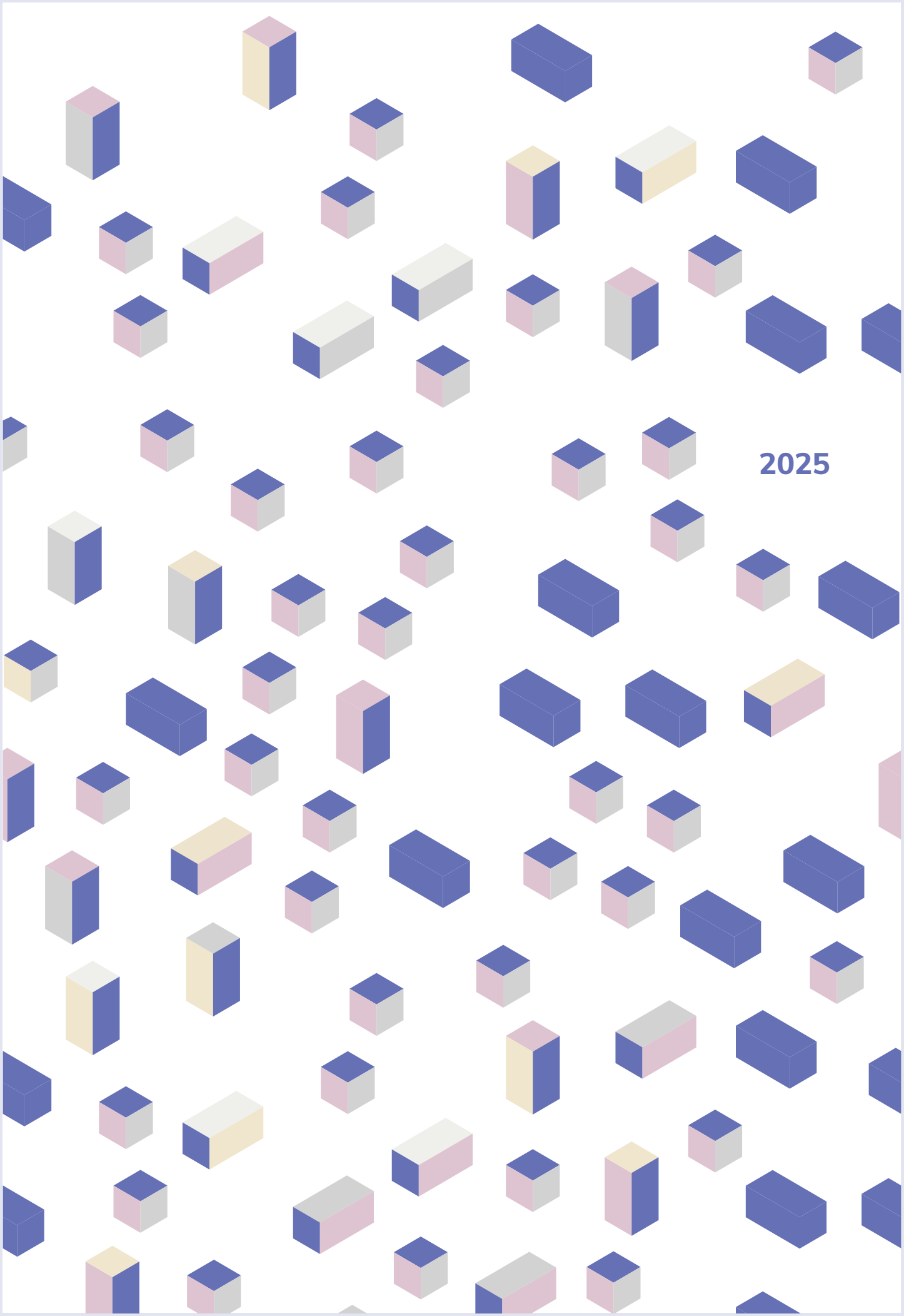
Chart 12

Distribution of appointed DPOs by sectors in 2025 (per cent)



ŽURNALISTŲ ETIKOS INSPEKTORIAUS TARNYBOS ASMENS DUOMENŲ APSAUGOS PRIEŽIŪROS LIETUVOJE APŽVALGA




2025

ŽURNALISTŲ ETIKOS INSPEKTORIAUS ŽODIS

Dainius Radzevičius
Žurnalistų etikos inspektorius

Bendrojo duomenų apsaugos reglamento (toliau – Reglamentas) santykis su viešosios informacijos rengėjais ir skleidėjais, o ypatingai su žurnalistais yra nuolatinių viešų diskusijų objektas. Žurnalistų etikos inspektoriaus tarnyboje nuolat gaunama paklausimų dėl Reglamento apimčių ir išimčių žurnalistikos tikslais taikymo. Vis dažniau kreipiasi žiniasklaidos atstovai prašydami ekspertinės tarnybos darbuotojų nuomonės, kuomet valstybės ar savivaldos institucijose atsisakoma teikti informaciją naudojantis Reglamento nuostatomis. Kita vertus, gausėja skundų dėl viešoje erdvėje ir ypatingai tarptautinėse algoritmų platformose skleidžiamų privačių asmens duomenų. Žurnalistų etikos inspektoriaus tarnyba yra asmens teisių gynėjas medijose, todėl tarnybos darbuotojai privalo užtikrinti, kad visuomenės informavimo srityje būtų ginamos žmogaus teisės. Dažniausiai tenka nagrinėti asmenų skundus dėl pažeistos žmonių garbės ir orumo ar teisės į privatumą, taip pat duomenų subjektų pagal Reglamentą pateiktus skundus. Teisė būti pamirštam tampa vis dažnesniu klausimu ir reikalauja nuolat vertinti tokių duomenų buvimo viešoje erdvėje pagrįstumą, o žiniasklaidos archyvuose skelbiamai informacijai svarbus ir žurnalistikos tikslų argumentas.

Tarnyba yra viena iš dviejų Reglamento priežiūros institucijų Lietuvoje, todėl glaudus bendradarbiavimas su Valstybine duomenų apsaugos inspekcija padeda efektyviai koordinuotis veiklą.

Tarnyba skiria ir planuoja ateityje dar daugiau dėmesio skirti konsultacijoms ir mokymams. Nors šiai funkcijai vykdyti nėra skirta pakankamai finansinių ar žmogiškųjų resursų, tačiau glaudus bendradarbiavimas su kitomis institucijomis, asocijuotomis struktūromis bei žiniasklaida leidžia efektyviai skleisti svarbią informaciją tikslinei auditorijai.

Lietuva yra sukūrusi išskirtines sąlygas žurnalistams nemokamai gauti duomenis, taip pat ir apie privačius asmenis, iš valstybės valdomų registrų ir informacinių sistemų, todėl viešosios informacijos rengėjų ir skleidėjų bei žurnalistų statusas tampa vis aktualesne tema, o atskiri skundai rodo, jog šiai sričiai gali tekti inicijuoti papildomus teisės aktų pakeitimus, dėl kurių šiuo metu diskusijos vyksta Medijų taryboje, veikiančioje prie Kultūros ministerijos. Ši tema reikalauja ypatingo jautrumo ir dėmesio, nes bet koks naujas reguliavimas gali būti siejamas su žiniasklaidos laisvėmis bei jų atspindžiu tarptautiniuose spaudos laisvės indeksuose.

ŽURNALISTŲ ETIKOS INSPEKTORIAUS MANDATAS

Žurnalistų etikos inspektorius yra nepriklausomas, Seimui atskaitingas valstybės pareigūnas, kuris prižiūri, kaip įgyvendinamos Visuomenės informavimo, Nepilnamečių apsaugos nuo neigiamo viešosios informacijos poveikio įstatymų nuostatos. Jam taip pat suteikti priežiūros institucijos įgaliojimai asmens duomenų apsaugos srityje – kai duomenys tvarkomi žurnalistikos tikslais ir akademinės, meninės ar literatūrinės saviraiškos tikslais, žurnalistų etikos inspektorius stebi, kaip taikomas Asmens duomenų teisinės apsaugos įstatymas, vykdo 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 – Reglamentas) ir 1981 m. sausio 28 d. Strasbūre sudarytos Konvencijos dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (ETS Nr. 108) ir jos protokolų priežiūros institucijos Lietuvos Respublikoje funkcijas.

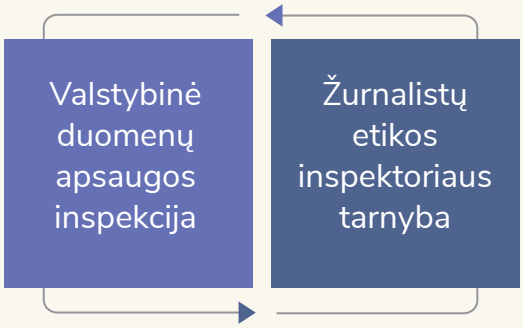
Viena iš svarbiausių Žurnalistų etikos inspektoriaus tarnybos (toliau – Tarnyba) veiklos krypčių yra institucijai pavesto draudžiamos informacijos internete priežiūros mandato įgyvendinimas. Pagal Informacinės visuomenės paslaugų įstatymą, kuris įgyvendina 2022 m. spalio 19 d. Europos Parlamento ir Tarybos Reglamentą (ES) 2022/2065 dėl bendrosios skaitmeninių paslaugų rinkos, kuriuo iš dalies keičiama Direktyva 2000/31/EB, Tarnyba yra paskirta kaip viena iš kompetentingų institucijų ir jai suteikti įgaliojimai užtikrinti šio reglamento vykdymą Tarnybos kompetencijos ribose.

Pagrindinė žurnalistų etikos inspektoriaus funkcija yra nagrinėti suinteresuotų asmenų skundus dėl visuomenės informavimo priemonėse pažeistos jų garbės ir orumo, teisės į privataus gyvenimo apsaugą, taip pat duomenų subjektų pagal Reglamentą pateiktus skundus dėl asmens duomenų tvarkymo žurnalistikos, akademinės, meninės ar literatūrinės saviraiškos tikslais. Pažymėtina, kad nepaisant to, jog pagrindinė žurnalistų etikos inspektoriaus funkcija yra suinteresuotų asmenų skundų nagrinėjimas, šią funkciją jis atlieka atsižvelgdamas į Visuomenės informavimo įstatyme numatytą jo, kaip žmogaus teisių visuomenės informavimo srityje užtikrinimo garantijos, paskirtį, t. y. užtikrindamas viešojo intereso – žodžio ir spaudos laisvės, visuomenės informavimo – tinkamą įgyvendinimą.

Šalia pagrindinės skundų nagrinėjimo ir pažeidimų tyrimo funkcijos, žurnalistų etikos inspektorius vykdo ir eilę kitų funkcijų: vertina, kaip informuojant visuomenę yra laikomasi pagrindinių visuomenės informavimo principų, atlieka viešosios informacijos visuomenės informavimo priemonėse (išskyrus radiją ir televiziją) stebėseną, ekspertinį paskelbtos viešosios informacijos vertinimą dėl nesantaikos skatinimo įvairiais pagrindais, priskiria visuomenės informavimo priemones ar jų turinį erotinio, pornografinio ir (ar) smurtinio pobūdžio informacijos kategorijoms, teikia Seimui ir kitoms valstybės institucijoms siūlymus dėl visuomenės informavimą reglamentuojančių įstatymų bei teisės aktų tobulinimo ir įgyvendinimo, bendradarbiauja su Europos Sąjungos ir kitų šalių analogiškomis institucijomis, pagal savo kompetenciją atstovauja Lietuvos Respublikai tarptautinėse organizacijose.

Žurnalistų etikos inspektoriaus funkcijose metodinės pagalbos visuomenės informavimo klausimais teikimas ir švietėjiška veikla nėra numatyti. Vis dėlto inspektorius ir Tarnybos atstovai, atsižvelgdami į turimas galimybes, organizuoja mokymus, seminarus bei skaito pranešimus žmogaus teisių užtikrinimo žiniasklaidoje, asmens duomenų teisinės apsaugos žiniasklaidoje ir kovos su neteisėtu visuomenės informavimo priemonių turiniu temomis. Siekdamas prisidėti prie geresnio žiniasklaidos sritį reglamentuojančių teisės aktų nuostatų supratimo, žurnalistų etikos inspektorius ir Tarnybos specialistai teikia konsultacijas bei informaciją visiems suinteresuotiems asmenims Tarnybos kompetencijai priskirtais klausimais.

Pagal įtvirtintą teisinį reguliavimą Reglamento ir Asmens duomenų teisinės apsaugos įstatymo taikymo priežiūrą Lietuvoje atlieka du subjektai – Žurnalistų etikos inspektoriaus tarnyba ir Valstybinė duomenų apsaugos inspekcija (toliau – VDAI).



Siekiant efektyviai įgyvendinti asmens duomenų apsaugą, būtina užtikrinti sklandų šių dviejų institucijų bendradarbiavimą. Ataskaitiniu laikotarpiu buvo organizuojami tarpinstituciniai susitikimai, diskutuojama aktualiais veiklos klausimais, keičiamasi patirtimi ir turima informacija. Žurnalistų etikos inspektorius arba Tarnybos atstovai buvo kviečiami ir dalyvavo įvairiuose renginiuose, konferencijose, mokymuose, kur kartu su VDAI atstovais dalijosi sukauptomis žiniomis bei informacija asmens duomenų apsaugos ir teisės į privataus gyvenimo apsaugą temomis.

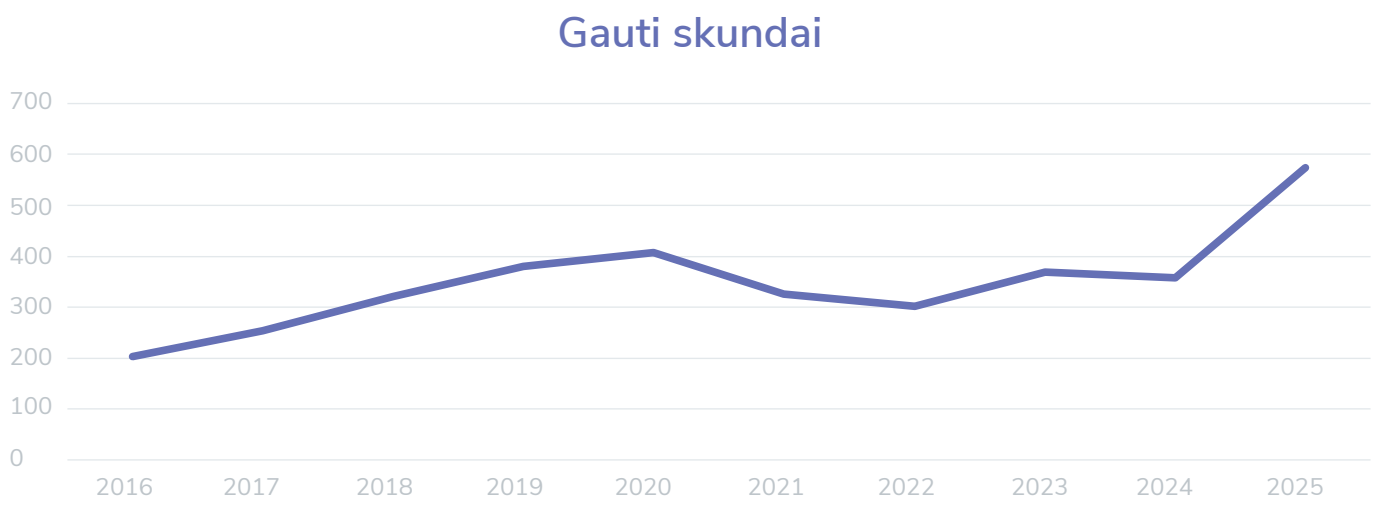
Bendradarbiavimo su Valstybine duomenų apsaugos inspekcija poreikis nuosekliai auga, nes praktinės situacijos tampa vis sudėtingesnės, o dviejų priežiūros institucijų kompetencijų atskyrimas ir aiškus apibrėžimas kelia papildomų iššūkių. Vis dažniau atsiranda būtinybė derinti institucijų pozicijas, siekiant užtikrinti vienodą Reglamento nuostatų aiškinimą ir taikymą, tinkamą ataskaitų teikimą, operatyvų keitimąsi aktualia informacija bei konstruktyvias diskusijas dėl svarbiausių Reglamento įgyvendinimo priežiūros klausimų. Taip pat ieškoma suderintų veikimo mechanizmų, leidžiančių užtikrinti veiksmingą ir nuoseklią priežiūrą, pasiruošimą Asmens duomenų teisinės apsaugos įstatymo numatytam ex post vertinimui.

Pagal Reglamentą, kiekviena asmens duomenų priežiūros institucija parengia metinę savo veiklos ataskaitą, kurią pateikia Europos duomenų apsaugos valdybai, Europos Komisijai ir visuomenei. Bendradarbiaujant su VDAI, Tarnyba savo ataskaitą apie duomenų tvarkymo priežiūrą pateikia kartu viename bendrame dokumente.

BENDRA SKUNDŲ IR SPRENDIMŲ STATISTIKA

Ataskaitiniu laikotarpiu Tarnyba iš viso gavo 574 skundus (2024 metais – 358) (žr. 1 diagramą). Tai rodo reikšmingą kreipimųsi dėl galimų pažeidimų visuomenės informavimo srityje augimą. Analizuojant gautus skundus matyti, kad vis didesnė jų dalis yra susijusi su socialiniuose tinkluose skelbiamu turiniu. Socialiniuose tinkluose skelbiama informacija yra lengvai prieinama ir greitai pasiekia plačią auditoriją, dažnai ginčams būdingas tiesioginis bendravimas, todėl galimi asmens teisių pažeidimai šioje viešosios informacijos sklaidos aplinkoje dažniau pastebimi ir identifikuojami kaip pažeidimai. Ši aplinkybė gali būti viena iš tikėtinų priežasčių, lemiančių bendrą Tarnybai teikiamų skundų skaičiaus augimą.

1 diagrama



Dalis skundų Tarnybai persiųsti kitų institucijų pagal kompetenciją, ženkliai padidėjo ir iš VDAI persiunčiamų skundų dėl galimų asmens duomenų pažeidimų skaičius. Dideliu aktyvumu išsiskyrė įvairūs šalies policijos komisariatai, kurie pagal kompetenciją persiuntė nagrinėti Tarnybai priskirtinus atvejus.

Skundų analizė leidžia identifikuoti pagrindines konfliktines situacijas ir problemas visuomenės informavimo srityje, tačiau išsamesnį šių tendencijų vertinimą suteikia priimtų sprendimų analizė.

Žurnalistų etikos inspektoriaus sprendimai atskleidžia, kaip konkrečiose situacijose taikomos Visuomenės informavimo įstatymo ir kitų teisės aktų nuostatos, taip pat leidžia įvertinti formuojamą praktikos kryptį ginant asmens neturtines teises. Sprendimų analizė suteikia galimybę įvertinti ne tik nustatytų pažeidimų pobūdį, bet ir tai, kokie kriterijai taikomi derinant saviraiškos laisvę su asmens garbės bei orumo, dalykinės reputacijos, privataus gyvenimo ir asmens duomenų apsauga bei pagrindinių visuomenės informavimo principų laikymusi.

2025 m. žurnalistų etikos inspektorius iš viso priėmė 435 sprendimus (žr. 2 diagramą), kuriuose vertinti galimi Visuomenės informavimo įstatymo ir kitų visuomenės informavimo sritį reglamentuojančių teisės aktų pažeidimai. Nagrinėjant skundus kiekvienu atveju vertinama, ar nepažeista pusiausvyra tarp konkuruojančių konstitucinių vertybių – saviraiškos laisvės ir asmens garbės ir orumo, dalykinės reputacijos, privataus gyvenimo bei asmens duomenų apsaugos. Sprendimuose analizuojamas ne tik paskelbtos informacijos turinys, bet ir jos pateikimo kontekstas, tikslas bei ryšys su viešuoju interesu.

Šie sprendimai atspindi ne tik individualių skundų nagrinėjimo rezultatus, bet ir Tarnybos formuojamos praktikos kryptis, susijusias su saviraiškos laisvės ir asmens neturtinių teisių apsaugos derinimu.

2 diagrama

Iš visų 2025 m. išnagrinėtų skundų 109 pripažinti nepagrįstais. Tokie sprendimai dažniausiai siejami su situacijomis, kai ginčijama informacija susijusi su viešojo intereso klausimais arba kai pareiškėjai laikytini viešaisiais asmenimis, kurių atžvilgiu leistinos kritikos ribos yra platesnės. Kartu sprendimuose pabrėžiama, kad saviraiškos laisvė nėra absoliuti ir negali pateisinti nepagrįstos ar faktais neparemtos informacijos sklaidos.

Ataskaitiniu laikotarpiu dalis tyrimų nutraukti (56), įskaitant atvejus, kai ginčas išspręstas taikiai taikant mediacijos procedūrą (22). Toks sprendimo būdas taikomas situacijose, kai viešosios informacijos rengėjas (skleidėjas) pašalina nustatytus pažeidimus, o pareiškėjas atsiima skundą. Dalis skundų nenagrinėjami dėl Visuomenės informavimo įstatyme ir Asmens duomenų teisinės apsaugos įstatyme nustatytų pagrindų, pavyzdžiui, kai skundas nepatenka į inspektoriaus kompetenciją, trūksta duomenų tyrimui pradėti ar yra suėjęs skundo pateikimo senaties terminas.

ASMENS DUOMENŲ APSAUGOS PRAKTIKA VISUOMENĖS INFORMAVIMO SRITYJE

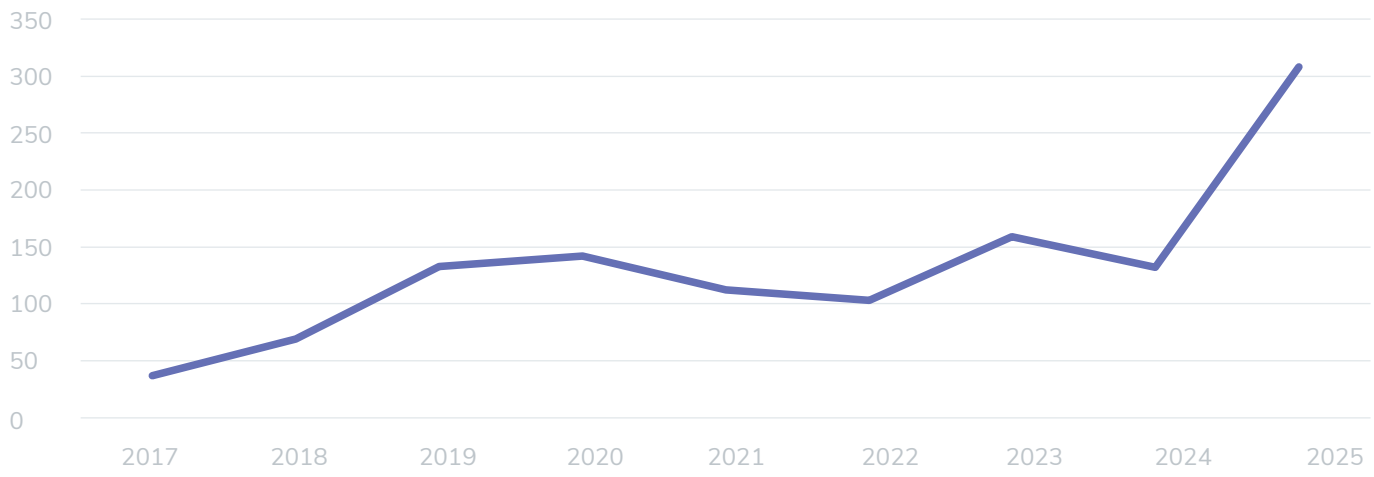
2025 metų duomenys patvirtina reikšmingą skundų dėl teisės į asmens duomenų apsaugą gausėjimą. 2025 metais gauti 308 skundai (53 proc. visų skundų) (žr. 3 diagramą), t. y. palyginti su 2024 metais, šis rodiklis išaugo daugiau nei du kartus, kai buvo gauti 132 tokie skundai. Svarbus ne tik absoliutus šių skundų augimas, bet ir santykinės dalies pokytis bendrame skundų kontekste: 2024 metais jie sudarė 37 proc., o 2025 metais jų dalis padidėjo iki 53 proc. ■

Daugiau nei pusė Tarnybai teiktų skundų susiję su asmens duomenų apsauga.

Ši dinamika atspindi ne tik didėjantį duomenų subjektų aktyvumą ir sąmoningumą įgyvendinant Reglamento nuostatomis grindžiamas teises, bet ir augantį asmens duomenų apsaugos klausimų aktualumą šiuolaikinėje informacinėje aplinkoje. Kartu šis pokytis leidžia konstatuoti, kad asmens duomenų apsaugos klausimai tampa viena dominuojančių Tarnybos nagrinėjamų skundų sričių, o šios kategorijos skundai praktikoje įgauna vis didesnį reikšmingumą. Dėl to kyla poreikis ne tik užtikrinti efektyvų individualių skundų nagrinėjimą, bet ir nuosekliai stiprinti prevencines bei metodines priemones, orientuotas į asmens duomenų apsaugos reikalavimų įgyvendinimą skaitmeninėje aplinkoje.

3 diagrama

Skundai dėl asmens duomenų apsaugos



Ataskaitinių metų skundų nagrinėjimo praktika patvirtino, kad asmens duomenų apsaugos reikalavimų taikymas neišvengiamai susijęs su interesų pusiausvyros tarp teisės į asmens duomenų apsaugą ir saviraiškos laisvės vertinimu, ypač tais atvejais, kai asmens duomenys tvarkomi žurnalistikos tikslais ar siekiant įgyvendinti viešąjį interesą. Nors žurnalistinė veikla nepanaikina pareigos laikytis Reglamento reikalavimų, tačiau duomenų apsauga negali būti taikoma taip, kad neproporcingai ribotų visuomenės teisę gauti informaciją. Žurnalistiniais tikslais tvarkomiems duomenims taikomos tam tikros duomenų apsaugos išimtys ir nukrypti leidžiančios nuostatos, tačiau jos turi būti taikomos vadovaujantis proporcingumo ir būtinybės principais. Atsižvelgiant į tai, toliau pateikiama 2025 metais gautų skundų analizė, atskleidžianti vyraujančias duomenų tvarkymo situacijas, dažniausiai ginčijamus sklaidos kanalus bei pagrindinius iššūkius, su kuriais susiduriama taikant asmens duomenų apsaugos reikalavimus.

Vyraujanti skundų kategorija – asmens duomenų viešinimas socialiniuose tinkluose

Kaip jau minėta, 2025 metais fiksuotas reikšmingas skundų dėl galimų asmens duomenų apsaugos pažeidimų skaičiaus augimas, kuris daugiausia siejamas su informacijos viešinimu socialiniuose tinkluose. Pastebėta, jog tradicinėse visuomenės informavimo priemonėse (interneto portaluose, spaudoje, radijuje, televizijoje) skelbiamos informacijos atžvilgiu skundų dinamika išlieka santykinai stabili. Tai patvirtina, kad teisės į asmens duomenų apsaugą pažeidimų problematika vis labiau koncentruojasi socialinių tinklų erdvėje, kur informacijos sklaida vyksta greitai ir plačiu mastu, o turinį daugiausia formuoja bei viešina patys naudotojai.

4 diagrama

Kaip ir ankstesniais metais, dažnu atveju asmenys kreipiasi dėl teisės į asmens duomenų apsaugą gynimo situacijose, kai duomenų tvarkymą vykdo socialinių tinklų paskyrų valdytojai, kurie nėra profesionalūs žurnalistai. Akcentuotina, kad didžioji dalis tokių skundų kyla privačių asmenų tarpusavio konfliktų kontekste, kai siekiama viešai paskleisti informaciją apie kitą asmenį, jo elgesį ar tariamą nepatikimumą, taip pat paviešinti subjektyvaus pobūdžio asmenines istorijas. Ypač dažnai skunduose minimos situacijos, kai socialiniuose tinkluose informacija apie kitą asmenį pateikiama konfliktiniame ar žeminančiame kontekste. Pavyzdžiui, fiksuotas atvejis, kai socialiniame tinkle *Facebook* paviešintos šeimos nuotraukos, siekiant viešai eskaluoti tarpasmeninį ginčą, tai rodo, jog viešinimo praktika neretai peržengia teisėto tikslo ribas ir tampa privataus konflikto perkėlimu į viešąją erdvę.

Vienas dažniausių skunduose įžvelgiamų pažeidimų socialiniuose tinkluose yra asmens duomenų viešinimas siekiant viešai įvardyti kitą asmenį „nesąžiningu“, „aferistu“ ar „apgaviku“. Tokiose situacijose be sutikimo skelbiami vardai, pavardės, nuotraukos ir telefono numeriai, o įrašai dažnai pateikiami kaip bendruomeninis „įspėjimas“. Pavyzdžiui, ne vienu atveju *Facebook* paskyroje asmuo viešai įvardytas „aferistu“, kartu paviešinant jo telefono numerį bei nuotrauką. Analogiškai, *Facebook* grupėse „AFERISTAI!!! SUKČIAI!!! APGAVIKAI!!!“ fiksuoti atvejai, kai net ir ginčui išsisprendus (grąžinus pinigus), įrašai nepašalinami, o asmens duomenų viešinimas įgauna tęstinį pobūdį. Pastebima, kad socialiniuose tinkluose informacija apie galimai nesąžiningus asmenis (nepatikimus nuominikus, meistrus, skolininkus) vis dažniau skelbiama ne tik specialiai tam sukurtose grupėse, bet ir siekiant didesnio informacijos paplitimo masto – konkrečių miestų skelbimų, turgelių bei kitose teminėse grupėse. Kartu pažymėtina, kad nors uždarose grupėse skelbiamai informacijai dažnu atveju taikoma namų ūkio išimtis, 2025 m. vertintas atvejis, kai ginčo informacija paskelbta uždaros grupės viršelio nuotraukoje, kurios turinys buvo matomas ir prieinamas bet kuriam socialinio tinklo vartotojui.

Reikšminga dalis skundų susijusi su gyvenamosios vietos adreso ar privataus namo nuotraukų paskelbimu socialiniuose tinkluose. Gyvenamosios vietos adreso atskleidimas laikytinas viena jautriausių asmens duomenų viešinimo formų, nes tokia informacija tam tikrais atvejais gali sudaryti prielaidas identifikuoti konkretų asmenį ir, kaip pažymima skunduose, padidinti papildomų saugumo bei privatumo pažeidimų riziką. Skunduose dažnai akcentuojama, kad adresas arba konkrečios gyvenamosios aplinkos detalės viešinamos tarpasmeninių nesutarimų kontekste – siekiant viešai eskaluoti ginčus, stigmatizuoti kitą asmenį ar siekiant paveikti asmens vertinimą bendruomenėje. Tokie atvejai rodo, kad gyvenamosios vietos duomenys socialinių tinklų erdvėje neretai tampa sąmoningo privataus identifikavimo viešinimo forma, sukelianti papildomas privatumo rizikas. Tipinis atvejis fiksuotas socialiniame tinkle *Facebook*, kai pareiškėjas skundėsi dėl to, jog paviešintas gyvenamosios vietos adresas, siekiant nesutarimus tarp kaimynų perkelti į viešąją erdvę.

Socialiniai tinklai tampa erdve, kurioje duomenų subjektai susiduria su viešu „įvardijimu“ ar identifikavimu bendruomeninėse grupėse. Praktikoje pasitaiko atvejų, kai asmuo nufotografuojamas viešoje vietoje ir jo atvaizdas skelbiamas socialinių tinklų grupėje kartu su menkinančiais komentarais ar kaltinimais. Vienu atveju gautas skundas dėl nepilnamečio vaiko nuotraukų publikavimo *Facebook* grupėse, kai vaikas identifikuotas ir aptariamas suaugusių asmenų diskusijose. Tokie atvejai atskleidžia, kad socialinių tinklų grupės neretai tampa neformalia viešo neigiamo vertinimo erdve, kurioje privatumo ribos lengvai peržengiamos.

2025 metai išsiskyrė skundų dėl nepilnamečių asmens duomenų gausa, ypač jų atvaizdų, viešinimo socialiniuose tinkluose augimu. Tai itin jautri ir didelės rizikos asmens duomenų apsaugos pažeidimų sritis. Skunduose pateikti atvejai rodo, kad vaiko atvaizdas, vardas ar kiti identifikaciniai duomenys neretai viešinami be teisėto pagrindo, dažnai konfliktiniame kontekste, nesuvokiant tokios informacijos sklaidos galimų ilgalaikių pasekmių vaikui. Vienas dažniausiai pasitaikančių scenarijų – nepilnamečių atvaizdo publikavimas socialinių tinklų grupėse ar paskyrose, kai vaikas tampa diskusijų ar nesutarimų objektas, nors pats nėra susijęs su viešinamos informacijos turiniu. Pavyzdžiui, gautas skundas dėl nepilnamečių vaikų atvaizdų, kai vieno iš mokinių mama atvykusi filmavo klasę, šaukė ant mokytojos, o vaizdo įrašą su matomais nepilnamečių vaikų atvaizdais paskelbė savo *Facebook* paskyroje, kurioje vaikai identifikuojami tiesiogiai su jais nesusijusiame kontekste. Tokie atvejai atskleidžia, kad vaiko atvaizdas socialiniuose tinkluose gali būti panaudojamas kaip priemonė suaugusiųjų tarpusavio ginčuose, o vaiko privatumo interesas lieka neapsaugotas. Praktikoje pasitaiko ir itin jautrių situacijų, kai nepilnamečių nuotraukos viešinamos kartu su žeminančiais komentarais ar neigiamais vertinimais. Vienu atveju pareiškėjas kreipėsi dėl to, kad jo nepilnametės dukros nuotraukos paviešintos *Facebook* grupės pokalbių kanale kartu su neigiamomis ir žeminančiomis pastabomis. Tokie atvejai kelia ypatingą pavojų nepilnamečių privatumo apsaugai. Skundų praktikoje taip pat fiksuojami atvejai, kai nepilnamečių duomenys viešinami instituciniame ar bendruomeniniame kontekste, pavyzdžiui, mokyklų renginiuose ar susitikimuose. Kitu atveju skųstasi, kad susitikimų metu filmuojami ir fotografuojami mokiniai, o vėliau ši medžiaga viešinta socialiniuose tinkluose be aiškaus sutikimo. Tokios situacijos rodo, kad praktikoje vis dar stinga aiškaus supratimo apie nepilnamečių duomenų apsaugos reikalavimus ir pareigą užtikrinti jų privatumo apsaugą skaitmeninėje erdvėje.

Papildomą problemos mastą atskleidžia ir atvejai, kai viešojo asmens – Seimo nario – socialinio tinklo paskyroje buvo paviešinti nepilnamečių asmens duomenys – ketinusių vykti į protestą mokinių sąrašai su vardais ir pavardėmis. Šie duomenys paskelbti viešoje socialinių tinklų erdvėje su-

sieti su tam tikrais procesais ar aplinkybėmis, neturinčiomis savarankiško viešojo intereso nepilnamečių identifikavimo požiūriu. Be to, mokiniai apibūdinti baubikais, kitais neigiamais epitetais. Šiuo atveju nepilnamečiai tapo viešos diskusijos objektas vien dėl to, kad jų duomenys įtraukti į politinio ar visuomeninio pobūdžio komunikaciją. Tokia praktika ypač problemiška, nes nepilnamečių vardų ir pavardžių viešinimas leidžia juos tiesiogiai identifikuoti, o duomenų subjektai neturi realių galimybių kontroliuoti informacijos sklaidos. Svarbu paminėti, kad viešinimas vykdomas asmens, turinčio padidintą viešosios komunikacijos poveikį ir auditorijos pasiekiamumą, todėl informacijos sklaidos mastas ir galimas poveikis nepilnamečių privatumui objektyviai didesnis nei įprastų socialinių tinklų naudotojų atveju. Be to, tokia komunikacija gali sudaryti prielaidas nepilnamečių stigmatizacijai, nepageidaujamam dėmesiui ar neigiamam vertinimui jų socialinėje aplinkoje. Šis atvejis atskleidė reikšmingą praktinę problemą – nepilnamečių asmens duomenų naudojimą viešojoje ir politinėje komunikacijoje, nepakankamai įvertinant jų ypatingą teisinį statusą ir padidintą apsaugos poreikį. Tarnybos praktika patvirtina, kad net ir siekiant viešai aptarti aktualius visuomeninius klausimus, nepilnamečių identifikuojančių duomenų viešinimas negali būti laikomas proporcinga ar būtina priemone.

Ataskaitiniais metais gauta skundų dėl socialiniuose tinkluose viešinamų jautrių sveikatos duomenų, kurie, nors ir nesudaro reikšmingos bendro skundų skaičiaus dalies, išsiskiria dėl tvarkomų duomenų pobūdžio. Vienu atveju kreiptasi dėl socialiniame tinkle *Tik Tok* viešai demonstruoto kito asmens sveikatos išrašo, kuris pateiktas per klaidą, tačiau jame nurodyti itin jautrūs duomenys apie asmens sveikatos būklę, leidžiantys tiesiogiai identifikuoti duomenų subjektą. Akivaizdu, kad net ir netyčinis tokios informacijos paskelbimas sudaro prielaidas itin plataus masto duomenų sklaidai, atsižvelgiant į socialinių tinklų turinio plitimo ypatumus. Kitu atveju skundas pateiktas dėl socialinio tinklo *Facebook* įrašo komentarų, kuriuose gydytoja paviešino asmens psichinės sveikatos būklę, pasisakydama apie asmens galėjimą eiti tam tikras pareigas. Tokia informacija atskleista be sutikimo, todėl spręstas klausimas dėl teisėto pagrindo duomenų tvarkymui buvimo ir proporcingumo. Gautas skundas dėl socialiniame tinkle paviešintos asmens ŽIV diagnozės, kai itin jautri sveikatos informacija paskelbta nurodant asmenį identifikuojančius duomenis. Tokie skundai išryškino reikšmingas asmens duomenų apsaugos rizikas dėl itin jautraus tvarkomų duomenų pobūdžio. Šie atvejai patvirtina, kad net ir netyčinis ar riboto masto sveikatos informacijos atskleidimas socialinių tinklų aplinkoje gali turėti neproporcingą poveikį asmens privatumui ir kelia poreikį ypatingai atsakingai vertinti tokios informacijos viešinimo teisėtumą.

2025 metų skundų analizė leidžia nustatyti reikšmingą tendenciją – asmens duomenų viešinimo socialiniuose tinkluose praktinį įsigalėjimą, kai asmens tapatybę atskleidžiantys duomenys vis dažniau suvokiami kaip priimtina socialinės komunikacijos priemonė. Tokiais atvejais viešinimas neretai grindžiamas subjektyviu siekiu „įspėti“, „apsiginti“ ar išsakyti nuomonę, nors objektyviai

tokia praktika neatitinka proporcingumo ir būtinybės kriterijų, keliamų asmens duomenų tvarkymui. Ši tendencija ypač ryški įvairiose bendruomeninėse socialinių tinklų grupėse, kur asmens duomenų atskleidimas tampa socialinio spaudimo ar neigiamo vertinimo formavimo instrumentu. Tokiose situacijose privatumo ribos palaipsniui silpnėja, o duomenų subjektai faktiškai praranda galimybę kontroliuoti informacijos sklaidą. Skundų analizė taip pat rodo, kad socialinių tinklų paskyrų valdytojai dažnai nesuvokia, jog jų vykdomas asmens duomenų viešinimas patenka į Reglamento taikymo sritį, nepriklausomai nuo to, ar jie laikytini profesionaliais viešosios informacijos rengėjais ir skleidėjais.

Remiantis teismų formuojama ir Tarnybos plėtojama praktika, viešas asmens duomenų skelbimas, kai jis nėra grindžiamas teisėtu tikslu, pavyzdžiui, viešojo intereso įgyvendinimu, gali būti vertinamas kaip neteisėtas asmens duomenų tvarkymas ir sukelti teisinę atsakomybę.

Tai ypač aktualu socialinių tinklų aplinkoje, kur informacijos sklaida yra greita, auditorija plati, o galimos neigiamos pasekmės duomenų subjektui – sunkiai kontroliuojamos ir sudėtingai pašalinamos.

Kaip ir ankstesniais metais, dalis gautų skundų susiję su informacijos skleidimu uždarose ar pusiau uždarose socialinių tinklų erdvėse, pavyzdžiui, privačiose paskyrose, riboto prieinamumo grupėse ar kitose virtualiose platformose, kuriose turinys prieinamas tik tam tikrais kriterijais apibrėžtam asmenų ratui. Tokiais atvejais ypač aktualus Reglamento 2 straipsnio 2 dalies c punkte įtvirtintos vadinamosios „namų ūkio išimties“ taikymas, pagal kurią Reglamento nuostatos netaikomos, kai asmens duomenų tvarkymas vykdomas išimtinai asmeniniais ar namų ūkio poreikiais. Praktika patvirtino, kad informacijos skleidimo uždarose ar riboto prieinamumo skaitmeninėse erdvėse atvejai reikalauja itin kruopštaus faktinių aplinkybių vertinimo. Esminę reikšmę turi aiškus atribojimas tarp privačios komunikacijos, nepatenkančios į Tarnybos kompetencijos ribas, ir tokio pobūdžio informacijos skleidimo, kuris dėl turinio pobūdžio, paskleidimo masto ar faktinio prieinamumo tampa viešosios erdvės dalimi bei atitinka visuomenės informavimo kriterijus. Atsižvelgiant į šias aplinkybes, 2025 metais Tarnybos praktikoje skundų nagrinėjimas grįstas ne vien turinio vertinimu, bet ir informacijos paskleidimo apimties, auditorijos dydžio bei realaus prieinamumo analizės kriterijais. Toks požiūris leido nuosekliai atriboti Reglamento taikymo ribas, užtikrinti aiškų kompetencijų pasidalijimą ir kartu sudaryti prielaidas veiksmingai asmens teisių apsaugai skaitmeninėje aplinkoje.

Taigi 2025 metų praktika leidžia konstatuoti, kad socialiniai tinklai tapo pagrindine asmens duomenų apsaugos pažeidimų erdve, kurioje asmens duomenų apsaugos ribų peržengimas dažnai susijęs su tarpasmeniniais konfliktais, bendruomeniniu spaudimu ar įsigalėjusia viešinimo kultūra. Šios tendencijos suponuoja poreikį ne tik reaguoti į pavienius pažeidimus, bet ir nuosekliai plėtoti prevencinio pobūdžio informavimo praktiką, aiškiai komunikuojant, kad socialinių tinklų aplinka nesudaro išimties asmens duomenų apsaugos reikalavimų taikymui, o duomenų viešinimas be teisėto pagrindo gali sukelti teisines pasekmes.

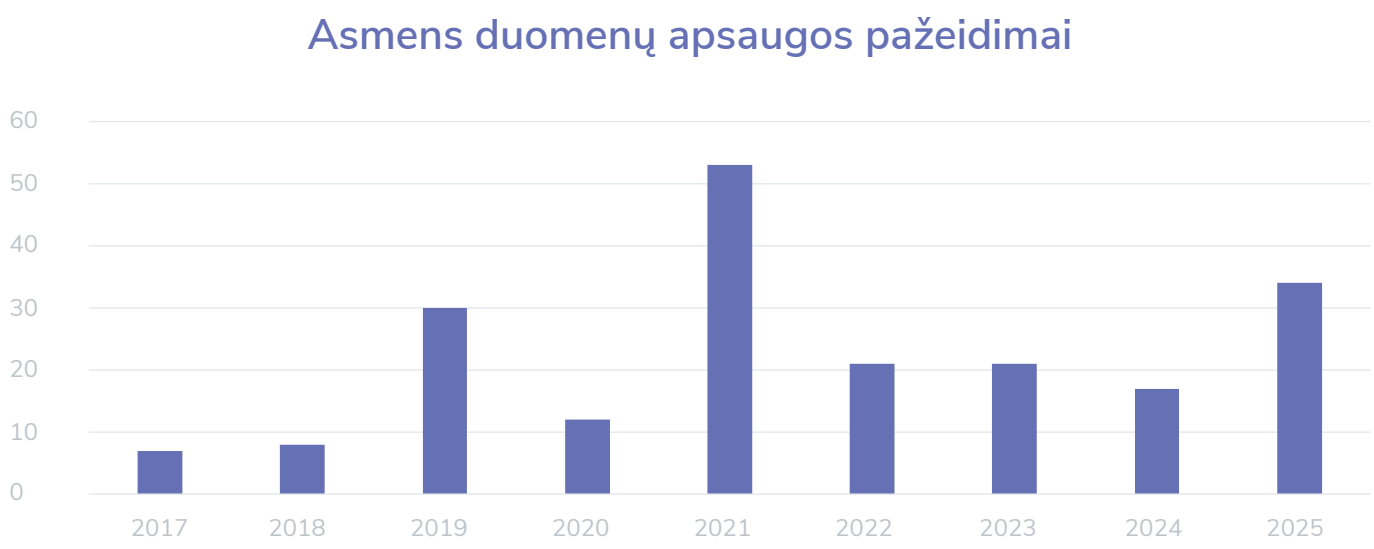
Atsižvelgiant į skundų analizėje išryškėjusias tendencijas, toliau aptariama Tarnybos sprendimų praktika, kurioje vertinta, ar konkrečiais atvejais asmens duomenų skelbimas atitiko Reglamento nustatytus teisėtumo bei proporcingumo reikalavimus.

Tarnybos sprendimai leidžia įvertinti, kaip praktikoje taikomi asmens duomenų apsaugos reikalavimai nagrinėjant skunduose iškeltas situacijas.

Konstatuotų asmens duomenų tvarkymo pažeidimų visuomenės informavimo priemonėse skaičius ataskaitiniais metais padidėjo:

2025 metais nustatyti 34 teisės į asmens duomenų apsaugą pažeidimai (žr. 5 diagramą). Asmens duomenų tvarkymo pažeidimas pripažintinas tais atvejais, kai nustatomas faktas, kad tvarkyta informacija laikytina asmens duomenimis; faktas, kad tvarkyti pareiškėjo asmens duomenys; faktas, jog atlikti asmens duomenų tvarkymo veiksmai; faktas, kad asmens duomenys tvarkyti nesant Reglamento 6 straipsnyje nustatytų asmens duomenų tvarkymo teisėtumą patvirtinančių sąlygų. Sprendimų analizė rodo, kad asmens duomenų apsaugos pažeidimai dažniausiai susiję su paskelbtų duomenų apimtimi ir jų būtinybe siekiamam visuomenės informavimo tikslui. Vertinant konkrečias situacijas sprendimuose nuosekliai analizuota, ar paskelbti asmens duomenys turėjo objektyvų ryšį su visuomenės interesu ir ar jų atskleidimas proporcingas nagrinėjamai temai.

5 diagrama



2025 m. sprendimų visuma rodo, kad asmens duomenų apsaugos klausimai sudarė reikšmingą nagrinėtų skundų dalį ir pasižymėjo aiškia disproporcija pagal informacijos sklaidos kanalus. Nors skundai teikti tiek dėl profesionalios žiniasklaidos, tiek dėl skaitmeninėse platformose skelbiamo turinio, konstatuotų pažeidimų dauguma susijusi su socialiniais tinklais ir kitomis naudotojų kuriamo turinio erdvėmis. Profesionalios žiniasklaidos subjektų veikla sudarė mažesnę dalį, tačiau būtent šiuose tyrimuose plėtota reikšminga proporcingumo ir duomenų kiekio ribojimo analizė. Sprendimuose ne kartą pabrėžta, kad viešosios informacijos rengėjai (skleidėjai), prieš skelbdami informaciją, privalo atsakingai įvertinti jos turinį ir įsitikinti, jog planuojamas informacijos paskelbimas atitinka asmens duomenų tvarkymo principus ir teisėtumo sąlygas, o duomenų subjekto interesai bei pagrindinės teisės ir laisvės nėra nepagrįstai pažeidžiami. Kartu akcentuota pareiga gauti asmens sutikimą skelbti jo duomenis arba, tokio sutikimo neturint ir nesant teisėto pagrindo, susilaikyti nuo tokios informacijos viešinimo.

Socialinių tinklų aplinka: teisėto pagrindo nebuvimas ir asmens duomenų naudojimas konfliktinėse situacijose

Socialiniuose tinkluose nustatyti pažeidimai pasižymėjo kitokiu pobūdžiu. Šioje erdvėje dominavo situacijos, kai asmens duomenys skelbti neturint jokio teisėto jų tvarkymo pagrindo arba naudojami siekiant tikslų, nesuderinamų su Reglamente nustatytais duomenų tvarkymo principais, pavyzdžiui, viešinant informaciją asmeninių nesutarimų kontekste, siekiant diskredituoti konkretų asmenį ar daryti jam viešą spaudimą. Tokiais atvejais asmens duomenų paskelbimas nesusijęs su visuomenės informavimo funkcija ar viešojo intereso tenkinimu, todėl vertintas kaip nepagrįstas ir neatitinkantis teisėto duomenų tvarkymo reikalavimų. Sprendimuose pažymėta, kad socialiniuose tinkluose asmens duomenų skelbimas dažnai įgyja kitokią funkciją nei profesionalioje žiniasklaidoje – jis naudojamas ne informuoti visuomenę, o viešai identifikuoti konkretų asmenį ir perkelti konfliktą į platesnę auditoriją. Tokiose situacijose vertintas ne tik informacijos turinys, bet ir jos paskelbimo kontekstas bei tikslas, nustatant, ar duomenų viešinimas teisėtas.

Vienu atveju konstatuota, kad *Facebook* paskelbtas vaizdo įrašas paskleistas tarpusavio ginčo kontekste, o ne siekiant informuoti visuomenę reikšminga tema. Nors filmavimas vyko viešoje vietoje, pažymėta, kad ši aplinkybė nesukuria savarankiško pagrindo viešai skelbti asmens atvaizdą be jo sutikimo. Kitu atveju *YouTube* platformoje paskelbtame vaizdo įraše, deklaruojant tikslą informuoti investuotojus apie galimą finansinę riziką, paviešinti ne tik vardas ir pavardė, bet ir asmens kodas, gimimo data bei gyvenamosios vietos adresas. Sprendime konstatuota, kad tokie duomenys nėra būtini visuomenės informavimui apie galimą riziką ir jų atskleidimas laikytas pertekliniu. Reikšmingą dalį sudarė situacijos, kai aštriose diskusijose skelbti asmens vardas, pavardė, darbovietė, kontaktiniai duomenys ar kita identifikuojanti informacija, siekiant perspėti kitus ar diskredituoti konkretų asmenį. Sprendimuose pažymėta, kad toks duomenų paskelbimas susijęs su tarpusavio nesutarimų eskalavimu ir negali būti laikomas teisėtu visuomenės informavimu.

Ypatingą vietą 2025 m. užėmė nepilnamečių asmens duomenų atskleidimo atvejai, kurie sprendimuose vertinami kaip ypač jautri duomenų tvarkymo kategorija. Pažymėta, kad nepilnamečių duomenų skleidimas reikalauja itin atsargaus proporcingumo vertinimo, nes vaikai laikomi pažeidžiama duomenų subjektų grupe, kuriai turi būti užtikrinama aukštesnio lygio apsauga. Vienu atveju politinio turinio vaizdo įraše panaudotas nepilnamečio atvaizdas, nors jis neturėjo savarankiškos reikšmės nagrinėjamai temai ir neprisidėjo prie visuomenei aktualios informacijos atskleidimo. Sprendime konstatuota, kad net ir filmuojant viešoje vietoje nepilnamečio atvaizdo paskelbimas be teisėto pagrindo pažeidžia jo asmens duomenų apsaugą, kadangi viešosios erdvės aplinkybė savaime nesuteikia teisės neribotai viešinti nepilnamečio atvaizdo. Kitoje situacijoje paskelbtas procesinių dokumentų turinys, įskaitant informaciją apie nepilnametės gyvenamosios vietos nustatymą, išlaikymo dydį ir kitus šeimos gyvenimo aspektus. Sprendime pažymėta, kad tokios informacijos viešinimas ne tik neturėjo savarankiško viešojo

intereso pagrindo, bet ir atskleidė jautrias nepilnametės gyvenimo aplinkybes, kurios pagal savo pobūdį priklauso vienai privačiausių asmens gyvenimo sričių. Konstatuota, kad procesinių dokumentų detalių paviešinimas socialinėje erdvėje sudarė prielaidas identifikuoti nepilnametę ir išplėtė įsibrovimą į jos privatų gyvenimą, todėl pripažintas nepagrįstu ir nesuderinamu su asmens duomenų apsaugos reikalavimais. Analogiškos problematikos atvejis vertintas ir kitame tyrime. Nagrinėtu atveju įrašo socialiniame tinkle tikslas – paviešinti nepilnametės elgesį šunų parodoje ir inicijuoti diskusiją apie jaunųjų vedlių atsakomybę bei skaidrumą, todėl pati tema galėjo būti laikoma atitinkančia visuomenės interesą. Vis dėlto sprendime pažymėta, kad toks informavimo tikslas galėjo būti pasiektas ir kitomis, nepilnametės asmens duomenų apsaugos nepažeidžiančiomis priemonėmis. Konstatuota, kad nepilnametės vardo, pavardės ir amžiaus atskleidimas nebūtinas siekiant aptarti nagrinėjamą problemą, todėl šių duomenų paskelbimas laikytas pertekliniu ir nesuderinamu su nepilnamečių asmens duomenų apsaugos reikalavimais.

Visais atvejais priminta, kad nepilnamečių atvaizdai, vardai ar kiti asmens duomenys gali būti skelbiami tik gavus teisėtų atstovų sutikimą ir tik tais atvejais, kai toks duomenų paskelbimas yra objektyviai būtinas siekiamam visuomenės informavimo tikslui.

Sprendimuose taip pat akcentuota, kad net ir tais atvejais, kai informacija skelbiama viešos diskusijos ar teisėto visuomenės informavimo kontekste, nepilnamečių tapatybę atskleidžiančių duomenų viešinimas negalimas, o tokios informacijos sklaida gali būti pateisinama tik tada, kai yra gautas teisėtų atstovų sutikimas ir nepažeidžiamos nepilnamečio teisės į privatų gyvenimą bei jo interesų apsaugą. 2025 m. praktika patvirtino, kad nepilnamečių asmens duomenų apsauga sprendimuose vertinama kaip ypač jautri sritis, kurioje proporcingumo kriterijai taikomi itin griežtai. Net ir tais atvejais, kai aptariama tema gali būti laikoma visuomenei aktualia, nepilnamečio tapatybę atskleidžiančių duomenų paskelbimas nėra laikomas būtinu visuomenės informavimo tikslui pasiekti.

Ataskaitiniais metais nagrinėti skundai, kuriuose vertintas asmens atvaizdo paskelbimas socialinio tinklo uždarose grupėse, nors faktiškai toks turinys prieinamas gerokai platesniam asmenų ratui. Vertintais atvejais pareiškėjų atvaizdai panaudoti socialinio tinklo grupės viršelio nuotraukoms, todėl jie matomi ne tik grupės nariams, bet ir kitiems platformos naudotojams, kurie galėjo matyti grupės turinį ar jos pagrindinį puslapį. Sprendime pažymėta, kad tokia atvaizdo panaudojimo forma išplečia asmens duomenų paskelbimo mastą ir sudaro prielaidas identifikuoti konkretų asmenį platesnėje auditorijoje. Vertinant šias situacijas sprendimuose pabrėžta, kad formali socialinio tinklo grupės „uždarumo“ aplinkybė savaime nepaneigia pareigos laikytis asmens duomenų apsaugos reikalavimų. Pažymėta, kad duomenų tvarkymo teisėtumas turi būti vertinamas atsižvelgiant ne tik į deklaruojamą prieigos ribojimą, bet ir į faktinį turinio prieinamumą bei galimybę jį matyti viešai. Todėl tais atvejais, kai asmens atvaizdas ar kiti identifikuojantys duomenys paskelbiami taip, kad juos gali matyti neapibrėžtas socialinio tinklo naudotojų skaičius, konstatuota, jog tokia informacijos sklaida laikytina viešu asmens duomenų paskelbimu ir turi atitikti bendruosius duomenų tvarkymo teisėtumo ir proporcingumo reikalavimus.

Apibendrinant sprendimų dėl socialiniuose tinkluose viešinamų asmens duomenų praktiką matyti, kad asmens duomenų apsaugos pažeidimai dažniausiai nustatyti tais atvejais, kai paskelbta perteklinė identifikuojanti informacija, neturėjusi objektyvaus ryšio su nagrinėjamu klausimu ar visuomenės interesu. Ypač dažnai tokios situacijos fiksuotos socialinių tinklų aplinkoje, kur asmens duomenys naudojami konfliktinėse situacijose arba siekiant viešai identifikuoti konkretų asmenį. Sprendimuose nuosekliai pabrėžta, kad net ir viešojo intereso kontekste skelbiami duomenys turi būti ribojami iki tokios apimties, kuri yra būtina informavimo tikslui pasiekti.

Skundai dėl asmens duomenų tvarkymo profesionalioje žiniasklaidoje

Ataskaitinių metų skundų praktika rodo, kad skundai dėl asmens duomenų tvarkymo profesionalioje žiniasklaidoje, nors kiekybiškai sudaro mažesnę dalį bendrame asmens duomenų apsaugos skundų kontekste, pasižymi didesniu teisiniu sudėtingumu ir yra reikšmingi formuojant Tarnybos praktiką. Šie skundai dažniausiai susiję su naujienų portalų skelbiamu turiniu, kurio prieinamumas yra ilgalaikis, o poveikis asmenims gali būti platesnis. Tipiniai skundų pavyzdžiai apima atvejus, kai publikacijose identifikuojami asmenys (nurodant vardą ir pavardę), nors patys pareiškėjai nelaiko savęs viešaisiais asmenimis ir neįžvelgia pakankamo viešojo intereso jų tapatybės atskleidimui. Skunduose pabrėžiama, kad asmenų vaidmuo aprašomame įvykyje yra antraeilis arba neturi savarankiškos reikšmės visuomenės informavimo požiūriu. Pavyzdžiui, gautas skundas dėl publikacijos apie vietinį konfliktą, kurioje nurodytas privataus asmens vardas, pavardė ir gyvenamoji vieta, nors pareiškėjo vertinimu informacijos tikslui pasiekti būtų pakakę apibendrintų ar anonimizuotų duomenų. Reikšminga skundų dalis susijusi su ikiteisminių tyrimų ar baudžiamųjų bylų nušvietimu tais atvejais, kai publikacijos paskelbtos teisinio proceso pradžioje, tačiau vėliau bylos baigtis pasikeitė, neretai pareiškėjui palankia linkme. Tokiais atvejais skunduose nurodoma, kad nors informacija paskelbimo metu galėjo būti laikoma aktualia, jos ilgalaikis viešinimas sukelia neproporcingą neigiamą poveikį pareiškėjo reputacijai. Vienu atvejų pareiškėjas skundėsi dėl publikacijos, kurioje jis įvardintas įtariamuoju, nors vėliau ikiteisminis tyrimas nutrauktas. Be to, fiksuoti skundai dėl perteklinio asmens duomenų atskleidimo, kai naujienų portale, be pagrindinės informacijos apie įvykį, pateikiamos papildomos privataus gyvenimo detalės. Pavyzdžiui, publikacijoje apie nelaimingą atsitikimą nurodyta nukentėjusio asmens gyvenamoji vieta, šeiminė padėtis ir kita kontekstinė informacija, kuri, pareiškėjo teigimu, neturėjo reikšmės visuomenės informavimo tikslams.

2025 metais gauta reikšminga dalis skundų dėl mirusių asmenų duomenų galimo neteisėto skelbimo viešojoje erdvėje. Dauguma šių kreipimųsi pateikti mirusiųjų artimųjų ir susiję su informacijos apie nusižudžiusius asmenis viešinimu. Tokia informacija dėl savo pobūdžio yra itin jautri ir gali sukelti reikšmingą emocinį poveikį mirusiųjų artimiesiems. Vis dėlto Reglamento nuostatos taikomos tik gyvų fizinių asmenų asmens duomenims, todėl mirusių asmenų duomenų tvarkymas nepatenka į šio Reglamento taikymo sritį. Atitinkamai skundai dėl mirusių asmenų duomenų tvarkymo negali būti vertinami Reglamento kontekste, neatsižvelgiant į tai, ar tokios informacijos viešinimas gali būti laikomas neetišku arba netinkamu kitų teisės normų požiūriu.

Skundų turinio analizė leidžia išskirti pasikartojančias asmens duomenų kategorijas, kurių paviešinimas profesionalioje žiniasklaidoje daugeliu atveju tampa ginčo objektas.

Dažniausiai skundžiamasi dėl šių asmens duomenų paviešinimo:

Vardo ir pavardės

Tai viena dažniausių skundų kategorijų. Pareiškėjai kreipiasi, kai profesionalioje žiniasklaidoje identifikuojami privatūs asmenys, kurių vaidmuo aprašomame įvykyje, jų teigimu, nėra pakankamai reikšmingas viešojo intereso požiūriu. Skunduose pabrėžiama, kad asmens tapatybės atskleidimas nėra būtinas informavimo tikslui ir galėjo būti pasiektas nuasmeninus duomenis.

Atvaizdo (nuotraukų ar vaizdo medžiagos)

Reikšminga dalis skundų susijusi su asmens atvaizdo paskelbimu be sutikimo, ypač kai atvaizdas leidžia lengvai identifikuoti asmenį. Tokie atvejai pasitaiko televizijos programų reportažuose ar publikacijose, kai naudojamos nuotraukos iš viešų vietų, renginių arba socialinių tinklų, tačiau jų panaudojimas, pareiškėjų teigimu, nėra tiesiogiai susijęs su viešojo intereso įgyvendinimu.

Duomenų apie procesinį statusą

Dažnai skundžiamasi dėl to, kad publikacijose asmuo įvardijamas įtariamuoju, kaltinamuoju ar kitaip siejamas su teisminiais ar ikiteisminiais procesais. Skunduose pažymima, kad problema ypač ryški tais atvejais, kai procesas dar nėra pasibaigęs, tačiau pirminė informacija išlieka viešai prieinama žiniasklaidos priemonėse.

Gyvenamosios ar buvimo vietos informacijos

Skunduose nurodoma, kad profesionalioje žiniasklaidoje kartais pateikiami adresai, konkretūs miestai, rajonai ar kiti duomenys, leidžiantys nustatyti asmens gyvenamąją ar buvimo vietą. Pareiškėjų teigimu, tokia informacija neturi informacinės vertės ir kelia asmens duomenų pažeidimo riziką ir nesaugumą.

Privataus gyvenimo aplinkybių

Skundai dėl asmens duomenų pažeidimo teikiami ir dėl šeiminių santykių, sveikatos būklės, giminystės ryšių, asmeninių konfliktų ar kitų jautrių aplinkybių atskleidimo. Nors pats įvykis gali būti laikomas viešai reikšmingu, ginčijama būtent tai, kad žiniasklaidoje viešinamos perteklinės detalės, nesusijusios su visuomenės interesu.

Netiesioginių duomenų

Vis dažniau skunduose keliamas klausimas dėl netiesioginių duomenų – pavyzdžiui, telefono numerio, darbo užmokesčio, nekilnojamojo turto vertės, gyvenamojo namo nuotraukų, darbo vietos, pareigų ar specifinių biografinių ar fizinių detalių – kurie, nors atskirai neidentifikuoja asmens, tačiau apskritai leidžia jį atpažinti. Tokiais atvejais pareiškėjai pabrėžia kontekstinį identifikavimą kaip pagrindinį asmens duomenų apsaugos pažeidimo šaltinį.

2025 metų skundų analizė rodo, kad profesionalioje žiniasklaidoje dažnai ginčijamas ne pats informacijos paskelbimo faktas, o pasirinkta asmens duomenų apimtis ir detalumo lygis. Pareiškėjai nuosekliai kelia klausimą, ar visuomenės informavimo tikslas galėjo būti pasiektas neatskleidžiant perteklinių, asmenį identifikuojančių arba jautrių duomenų, o tai patvirtina proporcingumo principo reikšmę Tarnybos praktikoje.

Ataskaitiniais metais išliko aktualūs skundai, susiję su asmens duomenų tvarkymu televizijos programose, kurių turinys grindžiamas realių situacijų, konfliktų ar teisėsaugos veiksmų fiksavimu, pirmiausia programose „Farai“ ir „TV Pagalba“. Šių programų formatas, orientuotas į dokumentinį vaizdavimą ir emociškai sustiprintą pateikimo formą, kelia specifinius asmens duomenų apsaugos iššūkius, ypač tais atvejais, kai filmuojami privatūs asmenys situacijose, galinčiose turėti neigiamą poveikį jų asmens duomenų apsaugai. Skunduose dėl programos „Farai“ dažniausiai keliami klausimai dėl asmenų atvaizdo, balso ir elgesio viešinimo, kai filmuojami asmenys identifikuojami tiesiogiai arba netiesiogiai. Pareiškėjai nurodo, kad net ir uždengus veidus ar nepateikus vardų, kontekstinė informacija (balso tembras, gyvenamoji aplinka, įvykio vieta, naudojamos frazės) leidžia atpažinti konkretų asmenį, ypač vietos bendruomenėse. Tokiais atvejais ginčijama, ar pasirinktos nuasmeninimo priemonės yra pakankamos realiam asmens tapatybės apsaugos užtikrinimui. Skunduose dėl programos „TV Pagalba“ dažniausiai akcentuojamas perteklinis privataus gyvenimo aplinkybių atskleidimas, kai viešinamos šeimos konfliktų detalės, tarpasmeniniai santykiai, sveikatos ar socialinės problemos. Pareiškėjai nurodo, kad nors dalyvavimas programoje formaliai grindžiamas sutikimu, praktikoje kyla abejonių dėl sutikimo apimties ir informuotumo, ypač kai vėliau pasikeitus aplinkybėms asmenys siekia apriboti jau paskelbto turinio prieinamumą. Abiejų televizijos programų atvejais skunduose taip pat keliami netiesioginio identifikavimo klausimai, kai asmenys atpažįstami ne iš tiesiogiai nurodytų duomenų, o iš visumos: gyvenamosios vietos detalių, aplinkos, šeimos narių, vaikų, kaimynų ar pasakojimo specifikos. Tokia identifikavimo forma skundų praktikoje vertinama kaip galinti sukelti ilgalaikes neigiamas pasekmes asmens duomenų apsaugai ir kitoms neturtinėms teisėms. Svarbus probleminis aspektas, išryškėjantis skunduose dėl programų „Farai“ ir „TV Pagalba“, yra turinio ilgalaikis prieinamumas skaitmeninėje erdvėje. Skunduose pabrėžiama, kad televizijos programų epizodai, patalpinti interneto platformose ar transliuotojo archyvuose, išlieka viešai prieinami neribotą laiką, taip didindami galimo asmens duomenų pažeidimo mastą.

Apibendrinant galima konstatuoti, kad praktika atskleidžia kompleksinį interesų derinimo klausimą tarp visuomenės informavimo interesų, pramoginio dokumentinio formato ypatumų ir asmens duomenų apsaugos pažeidžiamose situacijose. Tarnybos praktika tokiais atvejais orientuota į individualų konkrečių aplinkybių vertinimą, ypatingą dėmesį skiriant sutikimo turiniui, nuasmeninimo pakankamumui ir proporcingumo kriterijų taikymui, siekiant užtikrinti, kad visuomenės informavimo tikslai nebūtų įgyvendinami neproporcingai ribojant asmens teisę į asmens duomenų apsaugą ir kartu nebūtų pažeista visuomenės teisė žinoti. Skundų analizėje išryškėjusios problemos atsispindi ir Tarnybos sprendimuose, kuriuose vertinama, ar konkrečiais atvejais paskelbti asmens duomenys atitiko teisėtumo ir proporcingumo reikalavimus.

Profesionalios žiniasklaidos atvejai: identifikavimo mastas ir vizualinės informacijos proporcingumas

Sprendimų praktika rodo, kad profesionalioje žiniasklaidoje pažeidimai nustatomi tais atvejais, kai egzistuojant visuomenės interesui peržengta būtinos informacijos apimtis. Tokiose situacijose sprendimuose pažymėta, kad visuomenės interesas pateisina pačios temos nagrinėjimą, tačiau nesuteikia neribotos teisės atskleisti bet kokią su konkrečiu asmeniu susijusią informaciją. Vertinant tokius atvejus analizuota, ar paskelbti asmens duomenys, atvaizdai arba kitos identifikuojančios detalės objektyviai būtini nagrinėjamai problemai atskleisti ir ar be jų nebūtų buvę galima pasiekti visuomenės informavimo tikslo. Kai nustatyta, kad tam tikri duomenys ar vizualiniai elementai neprisidėjo prie visuomenei reikšmingos informacijos pateikimo ir tik išplėtė asmens identifikavimo galimybes ar viešino perteklinius duomenis, konstatuota, jog peržengtos proporcingos informacijos atskleidimo ribos. Tokiais atvejais nustatyta, kad net ir teisėtai siekiant informuoti visuomenę būtinos informacijos apimtis turi būti ribojama iki tiek, kiek tai yra objektyviai reikalinga konkrečiai temai atskleisti. Viename iš sprendimų vertintas atvejis, kai informuojant apie rezonansinį nusikaltimą televizijos reportažuose ir publikacijose parodyti su nusikalstama veika nesusijusių asmenų – įtariamojo tėvų – gyvenamojo namo ir aplinkos vaizdai. Nors pati nusikalstama veika turėjo akivaizdžią visuomeninę reikšmę, nustatyta, kad gyvenamosios aplinkos vizualizavimas neprisidėjo prie įvykio atskleidimo, tačiau išplėtė įsibrovimą į privatų gyvenimą ir netiesiogiai susiejo šeimos narius su neigiamu kontekstu.

Net ir viešojo intereso kontekste skelbiant asmens duomenis, jų turi būti skelbiama tiek, kiek yra būtina aptariamai temai atskleisti.

Tai iliustruoja atvejis, kai publikacijoje apie galimą interesų konfliktą savivaldybėje pagrįstai aptariami viešųjų lėšų paskirstymo aspektai, tačiau papildomai paskelbta pareiškėjos gyvenamojo namo nuotrauka. Sprendime pažymėta, kad tokia vizualinė medžiaga perteklinė, neturėjo tiesioginio ryšio su nagrinėjama problema ir papildomai išplėtė asmens duomenų atskleidimo apimtį. Trečiasis atvejis susijęs su publikacija apie administracinį pažeidimą – trumpalaikį transporto priemonės sustojimą draudžiamoje vietoje. Nors tema galėjo būti siejama su viešosios tvarkos užtikrinimu, konstatuota, kad konkretaus asmens atvaizdo paskelbimas nebūtinas šiam tikslui pasiekti. Problema galėjo būti aptarta apibendrintai, neidentifikuojant duomenų subjekto.

Šie pavyzdžiai rodo, kad profesionalios žiniasklaidos kontekste 2025 m. nustatyti pažeidimai pavienio pobūdžio ir daugiausia susiję su proporcingumo ribų peržengimu – situacijomis, kai teisėtas visuomenės informavimo tikslas įgyvendinamas pasitelkiant perteklines asmens identifikavimo priemones ar vizualinę informaciją. Bendrame kontekste tokie pažeidimai sudarė nedidelę visų konstatuotų asmens duomenų pažeidimų dalį, o tai rodo, kad profesionalios žiniasklaidos praktikoje dažniau kyla ne paties informavimo teisėtumo, bet konkrečių identifikuojančių elementų apimties ir jų proporcingumo klausimai.

2025 m. sprendimai atskleidžia nuosekliai formuojamą asmens duomenų apsaugos vertinimo praktiką ir leidžia identifikuoti pagrindines problematikos kryptis. Sprendimuose pabrėžiama, kad viešojo intereso egzistavimas savaime nesuteikia teisės atskleisti bet kokių su asmeniu susijusių duomenų – jis turi būti konkretus ir tiesiogiai susijęs su skelbiamos informacijos turiniu. Kartu akcentuota, kad proporcingumo principas reiškia ne tik nagrinėjamos temos visuomeninę reikšmę, bet ir pareigą vertinti, ar konkretūs paskelbti duomenys yra objektyviai būtini šiai temai

atskleisti. Sprendimų analizė taip pat rodo, kad didžiausia asmens duomenų apsaugos pažeidimų dalis nustatyta socialinių tinklų aplinkoje, kur asmens duomenys neretai viešinami ne siekiant informuoti visuomenę, bet kaip reakcija į asmeninius konfliktus ar emocines situacijas. Tokiais atvejais duomenų paskelbimas tampa spaudimo, diskreditavimo ar viešo ginčo eskalavimo priemone, o ne visuomenės informavimu. Dėl šios priežasties sprendimuose nuosekliai pabrėžta, kad esminiu vertinimo kriterijumi tampa santykis tarp visuomenės informavimo tikslo ir asmens identifikavimo masto – kai paskelbti duomenys nėra būtini nagrinėjamai temai atskleisti, jų viešinimas laikomas nepagrįstu.

Analizuojant ataskaitiniais metais nustatytus pažeidimus matyti, kad dažniausiai jie susiję su pertekliniu ar nepagrįstu tam tikrų asmens duomenų viešinimu. Dažniausiai paviešinami duomenys apėmė asmens vardą ir pavardę, ypač tais atvejais, kai jų paskelbimas nepagrįstas aiškiu viešuoju interesu, taip pat asmens atvaizdą, kuris socialiniuose tinkluose neretai skelbiamas be duomenų subjekto sutikimo. Nustatyta ir atvejų, kai paviešinama kontaktinė ar identifikuojanti informacija, pavyzdžiui, gyvenamosios vietos adresai, telefono numeriai ar transporto priemonių valstybiniai numeriai, taip pat privataus gyvenimo detalės, susijusios su asmens sveikatos būkle ar šeiminiais santykiais. Reikšmingą dalį sudarė ir nepilnamečių duomenų atskleidimo atvejai – jų nuotraukų, vardų ar kitų identifikuojančių duomenų paskelbimas. Praktika rodo, kad šie pažeidimai dažniausiai kilo dėl perteklinio asmens duomenų viešinimo, kai nebuvo aiškaus informavimo tikslo ar realaus viešojo intereso, taip pat dėl privačių duomenų naudojimo asmeniniuose ginčuose siekiant diskredituoti konkretų asmenį ir dėl nepakankamo duomenų nuasmeninimo, kai paskelbta informacija leidžia aiškiai identifikuoti asmenis, įskaitant nepilnamečius.

Teisės būti pamirštam problematika

Atskira asmens duomenų problematikos kryptis ataskaitiniais metais susijusi su teisės reikalauti ištrinti duomenis („teisės būti pamirštam“) taikymu. 2025 metais, palyginti su 2024 metais, fiksuotas skundų dėl teisės būti pamirštam skaičiaus padidėjimas – tokie skundai sudarė apie 4 proc. visų Tarnybai pateiktų skundų, kai 2024 metais jų dalis siekė apie 2 proc. Šis pokytis rodo augantį pareiškėjų siekį riboti ilgalaikį su jų asmeniu susijusios informacijos viešą prieinamumą skaitmeninėje erdvėje, nepaisant nacionaliniame teisiniame reguliavime įtvirtintų teisės būti pamirštam taikymo ribojimų. Analizuojant 2025 metais pateiktų skundų pobūdį, matyti, kad jie iš esmės išlieka panašūs į ankstesnių metų skundus. Dauguma skundų teikiami asmenų, kurie anksčiau sieti su nusikalstamomis veikomis ar kitais viešai aptartais teisiniais procesais, dažniausiai susijusiais su senų bylų, ikiteisminių tyrimų ar teismo sprendimų paviešinimu žiniasklaidoje. Pareiškėjai skunduose paprastai nurodo, kad nors informacija teisinga jos paskelbimo metu, jos ilgalaikis išlikimas internete, jų vertinimu, nebeatitinka teisės į asmens duomenų ir privatumo apsaugos reikalavimų, daro neigiamą poveikį socialinei reintegracijai, o pareiškėjams palanki bylos baigtis netinkamai ar pakankamai aiškiai atspindėta viešojoje erdvėje. Be kita ko, dažnai akcentuojama, kad paieškos sistemų algoritmai prioritetą teikia neigiamai informacijai, ignoruodami vėlesnius pozityvius asmens gyvenimo ar veiklos pokyčius. Taigi nepaisant išimties iš šios teisės, įtvirtintos Reglamente, pareiškėjai 2025 metais aktyviai naudojosi teise kreiptis dėl senesnės, su jų asmeniu susijusios informacijos viešo prieinamumo ribojimo. Skunduose dažniausiai keliami klausimai dėl archyvinės informacijos, kuri paskelbta teisėtai, tačiau, pareiškėjų vertinimu, laikui bėgant prarado aktualumą ir nebeatitinka proporcingumo kriterijų, ypač kai asmuo nebėra viešasis, pasikeitė jo socialinis ar profesinis statusas, arba kai viešai prieinama informacija toliau daro neigiamą poveikį reputacijai. Pareiškėjų pozicija šiuose skunduose dažnai grindžiama ne siekiu paneigti istorinius faktus, bet prašymu persvarstyti ilgalaikį informacijos prieinamumą skaitmeninėje erdvėje, atsižvelgiant į pasikeitusias aplinkybes. Ypač pabrėžiama, kad žiniasklaidos archyvuose ar paieškos sistemose išliekanti informacija, net ir esant teisės būti pamirštam išimtims, praktikoje sukuria nuolatinį privatumo ribojimo efektą, kuris pareiškėjų vertinimu nebėra pateisinamas viešuoju interesu.

Praktikoje pasitaiko situacijų, kai teisės „būti pamirštam“ netaikymas kelia klausimų dėl proporcingumo, ypač tais atvejais, kai ilgą laiką viešai prieinama archyvinė informacija ir toliau daro reikšmingą poveikį asmens privatumui, nors jos aktualumas viešojo intereso požiūriu yra praėjęs. Pavyzdžiui, viename iš Tarnyboje vertintų skundų ginčijama informacija buvo paskelbta prieš 16 metų, publikacijoje pareiškėjas dalinosi privataus gyvenimo aplinkybėmis, detalizavo ryšį su tuometine sužadėtine, verslo kūrimo aspektus. Per šį laikotarpį publikacijoje nurodytos aplinkybės reikšmingai pasikeitė – pareiškėjas išsiskyrė su sužadėtine, jie abu sukūrė kitas šeimas. Tebesitęsiantis informacijos skelbimas nėra malonus pareiškėjui ir jo buvusiai sužadėtinei, o ir publikacijos tema nesusijusi su jokiu visuomenei aktualiu viešo intereso klausimu. Tokiais atvejais teisės „būti pamirštam“ įgyvendinimas galėtų būti siejamas su alternatyviomis priemonėmis, orientuotomis ne į

informacijos pašalinimą, bet į jos prieinamumo ribojimą. Delistingavimas, ribojantis informacijos pasiekiamumą per paieškos sistemas, galėtų būti proporcinga priemonė, leidžianti sumažinti ilgalaikį archyvinės informacijos poveikį asmens privatumui, kartu išsaugant visuomenės teisę susipažinti su šia informacija.

Tarnybos sprendimų dėl teisės būti pamirštam pagrįstumas vertintas ir teismų praktikoje. Pažymėtina, jog nors Asmens duomenų teisinės apsaugos įstatyme nustatyta, kad tais atvejais, kai asmens duomenys tvarkomi žurnalistikos tikslu, Reglamento 17 straipsnis, įtvirtinantis teisę būti pamirštam, netaikomas, ataskaitiniais metais pareiškėjas nesutiko su šia nuostata ir žurnalistų etikos inspektoriaus sprendimus, kuriuose pareiškėjo skundai dėl teisės būti pamirštam neįgyvendinimo atmesti, apskundė Regionų administraciniam teismui. 2025-09-04 Regionų administracinis teismas priėmė sprendimą administracinėje byloje Nr. el3-10074-1114/2025, kuriame patvirtino žurnalistų etikos inspektoriaus vertinimą, jog Asmens duomenų teisinės apsaugos įstatymo 4 straipsnio nuostata, nustatanti Reglamento taikymo išimtis tvarkant asmens duomenis žurnalistikos tikslu, yra imperatyvi, todėl pareiškėjo atžvilgiu įgyvendinti teisę būti pamirštam atsisakyta pagrįstai. Šis Regionų administracinio teismo sprendimas apskųstas Lietuvos vyriausiajam administraciniam teismui (toliau – LVAT). Vis dėlto savo prasme tai reikšmingas išaiškinimas dėl žurnalistų etikos inspektoriaus sprendimų dėl teisės būti pamirštam pagrįstumo ir tinkamo Reglamento išimčių taikymo. Teismo sprendimas patvirtina Tarnybos Reglamento išimčių aiškinimą ir parodo, kad žurnalistikos tikslu tvarkomų duomenų kontekste teisės būti pamirštam įgyvendinimas yra ribotas.

Analizuojant 2025 metais priimtus sprendimus matyti, kad asmens duomenų apsaugos užtikrinimas visuomenės informavimo srityje reikalauja nuoseklaus ir proporcingo vertinimo. Kiekvienu atveju būtina įvertinti, ar konkrečiu atveju duomenų paskelbimas objektyviai būtinas informavimo tikslui pasiekti, ar pasirinkta mažiausiai asmens teises ribojanti priemonė ir ar viešinimo mastas neperžengia teisėtų visuomenės intereso ribų. Sprendimų praktika taip pat atskleidžia, kad didžiausios asmens duomenų rizikos kyla socialinių tinklų aplinkoje, kur nustatyta didžioji dalis pažeidimų. Šiose platformose asmens duomenys neretai viešinami neįvertinus jų paskelbimo teisėtumo, proporcingumo ir būtinybės, o paskelbta informacija dažnai leidžia identifikuoti asmenis ar atskleidžia jų privataus gyvenimo aplinkybes, įskaitant nepilnamečių duomenis, nors tokia informacija nėra būtina nagrinėjamai temai atskleisti. Tai patvirtina, kad vertinant asmens duomenų skelbimo teisėtumą lemiamą reikšmę turi ne tik informacijos tema, bet ir konkrečių duomenų paskelbimas bei jų paskleidimo mastas.

Apibendrinant Tarnybos nagrinėtus skundus ir priimtus sprendimus asmens duomenų apsaugos srityje, pažymėtina, kad 2025 m. ginčai šioje srityje daugiausia kilo dėl viešojoje erdvėje paskelbtų identifikuojančių duomenų – vardo ir pavardės, atvaizdo, kontaktinės informacijos ar kitų su konkrečiu asmeniu siejamų detalių – viešinimo teisėtumo ir proporcingumo. Skundai rodo, kad

asmens duomenų apsaugos klausimai dažnai persipina su kitomis teisėmis – privatumo, garbės ir orumo apsauga ar nekaltumo prezumpcijos. Praktika patvirtina, kad rizika asmens teisėms kyla ne tik dėl akivaizdžiai jautrių duomenų paskelbimo, bet ir dėl atskirų, savaime jautriais nelaikomų duomenų visumos, kuri kartu sudaro realias prielaidas nustatyti asmens tapatybę ar susieti asmenį su konkrečiomis aplinkybėmis. Ypač jautrūs išlieka atvejai, kai viešinami nepilnamečių duomenys, duomenys apie vykstančius teisminius procesus ar informacija, leidžianti identifikuoti asmenį konfliktinėse ar socialiai pažeidžiamose situacijose.

2025 metais gauti skundai dėl asmens duomenų rinkimo teisėtumo išryškino problemas dėl viešosios informacijos rengėjo (skleidėjo) sąvokos apibrėžties bei aiškinimo, o kartu ir su tuo susijusių teisių apimties. Ataskaitiniais metais gauti trijų asmenų skundai dėl jų asmens duomenų rinkimo veiksmų VĮ Registrų centro valdomuose registruose, kuriuos atliko VšĮ „Vilniaus magas“ (tyrimo metu pavadinimas pakeistas į VšĮ „Spaudos klubas“). Pareiškėjams kreipusis į VĮ Registrų centrą buvo paaiškinta, kad VšĮ „Vilniaus magas“ yra registruota Viešosios informacijos rengėjų ir skleidėjų informacinėje sistemoje (VIRSIS), renka duomenis žurnalistikos tikslu ir su ja buvo sudaryta Vieninga duomenų teikimo sutartis, pagal kurią VšĮ „Vilniaus magas“ turi teisę neatlygintinai gauti duomenis ir informaciją iš registro ar valstybės informacinės sistemos tvarkytojo. Pareiškėjai skunduose kvestionavo, ar šiuo atveju žurnalistikos tikslas nėra imituojamas, kadangi VšĮ „Vilniaus magas“ nevaldo jokios visuomenės informavimo priemonės ir nėra paskelbęs jokių publikacijų ar kitos viešosios informacijos. Įstaiga paaiškinimuose žurnalistų etikos inspektoriui nurodė, jog ketina išleisti knygą „Vilniaus magas“ apie slaptus žiniasklaidos, verslo ir nusikalstamo pasaulio ryšius ir būtent šios knygos parengimui renka duomenis VĮ Registrų centre. Šis atvejis paskatino įvertinti Visuomenės informavimo įstatyme įtvirtintas viešosios informacijos rengėjo ir skleidėjo apibrėžtis bei atsižvelgti į tai, nuo kurio momento asmuo gali būti laikomas viešosios informacijos rengėju ir (ar) skleidėju.

Neabejotina, kad tiek viešosios informacijos rengėjo (skleidėjo) sąvoka, tiek žurnalistikos tikslas siejamas ir su informacijos rengiamam kūriniui rinkimu. Tačiau viešosios informacijos rengėjo (skleidėjo) veikla turi būti reali, o ne menama ar galimai atsirasianti ateityje.

Pažymėtina, jog abstrakti viešosios informacijos rengėjo (skleidėjo) sąvokos apibrėžtis Visuomenės informavimo įstatyme galėjo sudaryti galimybes piktnaudžiauti ir asmenims užsiregistravus Viešosios informacijos rengėjų ir skleidėjų informacinėje sistemoje naudotis viešosios informacijos rengėjo (skleidėjo) statusu, t. y. teise neatlygintinai gauti duomenis ir informaciją iš registro ar valstybės informacinės sistemos tvarkytojo, taip pat teise gauti iš valstybės ir savivaldybių institucijų bei įstaigų informaciją per vieną darbo dieną, nors jokia reali viešosios informacijos rengėjo (skleidėjo) veikla nėra vykdoma. Ši situacija kartu demonstruoja poreikį įvertinti Viešosios informacijos rengėjų ir skleidėjų informacinės sistemos (VIRSIS) nuostatų tinkamumą ir papildomų registracijos kontrolės mechanizmų įtvirtinimo galimybę, kadangi pagal šiuo metu galiojančią tvarką duomenys sistemoje įregistruojami ir paskelbiami viešai nuo juos teikiančio asmens pasirašymo momento, tačiau nei sistemos valdytojas, nei tvarkytojas neatlieka kontrolės veiksmų įvertinimui, ar besiregistruojantis asmuo ir jo veikla atitinka viešosios informacijos rengėjo ir (ar) skleidėjo kriterijus. Kontrolės ar peržiūros nebuvimas sudaro sąlygas bet kuriam asmeniui užsiregistruoti Viešosios informacijos rengėjų ir skleidėjų informacinėje sistemoje (VIRSIS) ir nepagrįstai naudotis viešosios informacijos rengėjams (skleidėjams) garantuojamomis teisėmis. Kartu tokia situacija sukelia rimtą grėsmę asmens duomenų apsaugai, kai itin jautri informacija tampa prieinama asmeniui, kuris prisidengia žurnalistikos tikslu ir viešosios informacijos rengėjo (skleidėjo) statusu, nors tokios veiklos nevykdo ir asmens duomenis renka neaiškiais tikslais.

KONSULTACINĖ VEIKLA

Kaip ir ankstesniais metais, Tarnyba 2025 m. aktyviai plėtojo konsultacinę veiklą. Kaip į kompetencijas žiniasklaidos teisės ir žmogaus teisių apsaugos žiniasklaidos sferoje telkiančią instituciją, į Tarnybą kreipiamasi ne tik su skundais, bet ir su įvairiais paklausimais, prašymais suteikti konsultacijas bei informaciją visuomenės informavimo srityje. Tarnyba stengiasi, kad šios paslaugos būtų kokybiškos ir prieinamos kuo platesniam visuomenės ratui. Tokia veikla prisideda tiek prie Tarnybos žinomumo didinimo, tiek prie gilesnio asmens neturtinių teisių apsaugos žiniasklaidoje suvokimo stiprinimo.

Suinteresuotų asmenų konsultavimas ir informacijos teikimas žurnalistų etikos inspektoriaus kompetencijai priskirtais klausimais sudaro svarbią Tarnybos veiklos dalį. Kiekvienas asmuo, kuriam kyla klausimų dėl viešosios informacijos skelbimo, žmogaus teisių apsaugos, saviraiškos ir informacijos laisvės realizavimo visuomenės informavimo priemonėse, gali kreiptis į Tarnybą dėl konsultacijos. Siekiame efektyviai patenkinti kiekvieno į Tarnybą besikreipiančio asmens teisėtus ir pagrįstus lūkesčius. Konsultacijos teikiamos žodžiu (telefonu arba atvykus į Tarnybą), raštu, elektroniniu paštu. Kiekvienas Tarnybos interneto svetainės lankytojas gali užduoti klausimą, palikti pastabą, pateikti pasiūlymą užpildydamas specialią formą, taip pat pateikti užklausą per Tarnybos *Facebook* paskyrą. Tarnybos atstovai į kiekvieną kreipimąsi reaguoja operatyviai, suteikia prašomą informaciją ar konsultaciją, padeda geriau suprasti teisės aktų reikalavimus.

2025 m. Tarnyba iš viso suteikė 1073 konsultacijas. Lyginant su praėjusiu ataskaitiniu laikotarpiu, bendras suteiktų konsultacijų skaičius šiek tiek padidėjo (2024 m. – 1007, 2023 m. – 1120, 2022 m. – 779). Praktiškai liko nepakitusios dažniausiai suteiktų konsultacijų tendencijos – daugiausia asmenys domėjosi Reglamento aiškinimo ir taikymo žiniasklaidos srityje klausimais. Tai sudarė apie du trečdalius visų teikiamų konsultacijų. Nors šis Europos Sąjungos teisės aktas, įgyvendinęs asmens duomenų apsaugos reformą, taikomas jau nuo 2018 m. gegužės 25 d., Tarnybos praktika rodo, kad klausimų dėl asmens duomenų tvarkymo žurnalistikos, akademinės, meninės ar literatūrinės saviraiškos tikslais skaičius išlieka aukštas.

6 diagrama

Tarnybos veiklos rezultatai rodo, kad Reglamentas iš esmės pakeitė visuomenės požiūrį į asmens duomenų apsaugą ir privatumą žiniasklaidoje, o jo reikšmė laikui bėgant nemažėja. Tai patvirtina nuolat išliekantis didelis tiek skundų, tiek konsultacijų dėl asmens duomenų tvarkymo žurnalistikos (visuomenės informavimo) tikslais skaičius. Vis labiau pastebimas augantis duomenų subjektų sąmoningumas ir didėjantys lūkesčiai dėl savo teisių apsaugos asmens duomenų tvarkymo srityje. Toks nuoseklus visuomenės aktyvumas sudaro tvirtą pagrindą užtikrinti, kad Reglamentas būtų ne tik formaliai taikomas, bet ir realiai bei veiksmingai įgyvendinamas praktikoje.

Dėl finansinių išteklių stokos atskiro tyrimo dėl Informacijos teikimo gairių žiniasklaidos ir viešojo sektoriaus atstovams, t. y. praktinio pobūdžio gairių dėl informacijos, kuria disponuoja viešajame sektoriuje veikiančios institucijos ir kurioje esama asmens duomenų, teikimo žiniasklaidos atstovams[1] (toliau – Gairės), kurias Tarnyba 2023 metais parengė kartu su Mykolo Romerio universitetu, poveikio vertinimo nėra atlikta, tačiau iš susitikimų ir pokalbių su žurnalistais bei žiniasklaidos asocijuotomis organizacijomis matyti, kad Gairės vertinamos palankiai, kaip reikšmingas ir darbą palengvinantis įrankis. Visi pripažįsta, kad Gairės veikia ir padeda, tačiau reikšmingą Tarnybos teikiamų konsultacijų dalį 2025 metų laikotarpiu ir toliau sudarė suinteresuotų asmenų konsultavimas dėl žiniasklaidos atstovų teisės gauti informaciją iš viešojo sektoriaus subjektų.

Žiniasklaidos atstovai vis dar susiduria su problema, kai neteisingai aiškinant Reglamentą, yra nepagrįstai ribojama žurnalistų teisė į informaciją, ypač kai kalbama apie žurnalistinius tyrimus, susijusius su viešaisiais asmenimis, biudžeto lėšų panaudojimu ir pan.

Konsultavimo praktika rodo, kad Reglamentas vis dar naudojamas kai kurių valstybės ir savivaldybių institucijų bei įstaigų kaip priemonė išvengti nepageidaujamo žiniasklaidos gilinimosi į užčiuoptą temą, kurią norima nuslėpti nuo visuomenės.

[1]Žr. https://www.zeit.lt/data/public/uploads/2023/02/gaires-1.pdf

Kaip ir praėjusiais metais, viešajame sektoriuje veikiančios institucijos į Tarnybą dažniausiai kreipėsi su prašymais suteikti konsultacijas, kaip teisingai nustatyti žurnalistų teisės į informaciją ir teisės į duomenų apsaugą pagal Reglamentą santykį. Valdžios ir viešojo sektoriaus atstovams kyla klausimų dėl teiktinų duomenų apimties, žurnalisto sąvokos, žurnalistinės veiklos apibrėžimo išaiškinimo. Daugiausia neaiškumų Teisės gauti informaciją ir duomenų pakartotinio naudojimo įstatymą įgyvendinančioms institucijoms kėlė vis labiau populiarėjančių laisvai samdomų žurnalistų ir piliečių žurnalistikos atstovų statusas bei jų teisė gauti informaciją, ypač susijusią su asmens duomenimis. Dažnu atveju buvo prašoma paaiškinti, kaip valdžios institucija galėtų įsitikinti, kad informacijos prašantis asmuo yra žurnalistas arba jam prilygintas asmuo, kaip reaguoti į žurnalistų prašymus, kai prašomi pertekliniai duomenys, kaip pritaikyti konkrečius su duomenų tvarkymu susijusius principus.

Pažymėtina, kad teismų praktika yra formuojama ta linkme, jog siekiant atsižvelgti į saviraiškos laisvės svarbą visai demokratinei bendruomenei, su ja susijusias sąvokas, įskaitant žurnalistiką, reikia aiškinti plačiai. Išimtis žurnalistikos veiklai nėra siejama su darbo teisiniais santykiais konkrečioje žiniasklaidos priemonėje ar profesiniu priklausymu žurnalistų profesinei organizacijai. Ji suteikiama kiekvienam asmeniui, užsiimančiam veikla, kurios tikslas – bet kokiu perdavimo būdu visuomenei skleisti informaciją, nuomones ar idėjas.

Informacijos, kurioje yra asmens duomenų, iš viešojo sektoriaus institucijų prašantys žiniasklaidos atstovai turi užtikrinti teisėtą ir sąžiningą tolimesnį duomenų tvarkymą. Žiniasklaidos atstovai, prašydami iš viešojo sektoriaus institucijų informacijos, kurioje yra asmens duomenų, turi užtikrinti jos teisėtą ir sąžiningą tolesnį tvarkymą. Tokia abipusiais įsipareigojimais grįsta viešojo sektoriaus ir žiniasklaidos sąveika duomenų prieinamumo srityje geriausiai atspindi saviraiškos laisvės svarbą demokratinėje visuomenėje. Gairės yra rekomendacinio pobūdžio dokumentas ir negali išspręsti visų Reglamento interpretavimo problemų ar pateikti universalių atsakymų į visus klausimus. Kiekviena duomenų tvarkymo situacija vertinama individualiai, atsižvelgiant į konkrečias aplinkybes. Gairės gali būti naudingas orientyras viešojo sektoriaus institucijoms, padedantis atlikti proporcingumo vertinimą tvarkant duomenis, skaidriai teikti informaciją bei asmens duomenis žurnalistams ir užtikrinti tinkamą informacijos laisvės bei asmens duomenų apsaugos balansą.

Tarnybos veikla rodo, kad Gairių naudojimas tampa vis plačiau paplitęs. Siekiant dar labiau palengvinti bendradarbiavimą tarp valdžios institucijų ir žurnalistų, prašančių informacijos, Tarnyba toliau aktyviai sieks didinti Gairių žinomumą ir jų pritaikomumą.

Ženkli dalis Tarnyboje gaunamų konsultacijų prašymų yra susijusi su asmenų filmavimu (fotografavimu) viešose vietose, renginiuose, ugdymo įstaigose, tokių atvaizdų viešu skelbimu, vaikų nuotraukų platinimu be tėvų sutikimo, asmens vardo, pavardės, atvaizdo, gyvenamosios vietos adreso, automobilio valstybinio registracijos numerio skelbimu, informacijos apie asmens sveikatą, duomenų subjektų teisių visuomenės informavimo priemonių veikloje įgyvendinimu. 2025 m. parodė panašias tendencijas. Griežti asmens duomenų teisinės apsaugos reikalavimai padidino poreikį konsultuotis dėl tinkamos sutikimo tvarkyti duomenis išraiškos formos, duomenų saugoji-

mo trukmės, vaizdo stebėjimo ir neteisėto informacijos apie privatų asmens gyvenimą rinkimo bei viešinimo. Atsižvelgiant į tai, kad asmens duomenų tvarkymui žurnalistikos tikslais Reglamentas taikomas ne visa apimtimi, suinteresuoti asmenys dažnai teiraujasi dėl išimčių, kai teisė į asmens duomenų apsaugą derinama su saviraiškos ir informacijos laisve, sankcijų už duomenų tvarkymo pažeidimus ir kitais klausimais.

Asmens duomenų tvarkymo teisėtumo klausimai dažnai buvo keliami ne dėl žurnalistų, o su šia profesija nesusijusių asmenų, jų parengtos ir paskelbtos informacijos (socialinių tinklų paskyrų valdytojų, turinio kūrėjų, influencerių, piliečių žurnalistikos atstovų, komentarų autorių ir pan.) atžvilgiu. Nors ir nebūdami žurnalistais, tokie asmenys yra laikomi viešosios informacijos rengėjais (skleidėjais), kuriems taip pat galioja duomenų apsaugos reikalavimai, taikomos teisinio poveikio priemonės ir kyla atsakomybė už pažeidimus.

Praėjusiais metais Tarnyboje konsultuotasi ir dėl mokslo bei visuomenės labui viešai skelbiamų naujų lietuvių kalboje atsiradusių žodžių – naujadarų, tokių kaip *blinkevičiūtinti* (reikšmė „pažadėti, bet neištesėti“), *gabrieliauti* (reikšmė „daryti neaiškaus ilgumo pauzę kokioje nors veikloje“) ir pan., atitikties asmens duomenų teisinės apsaugos, garbės ir orumo ar konfidencialumo reikalavimams. Aiškintasi, ar minėti žodžiai gali būti siejami ne tik su konkrečių duomenų subjektų (viešai žinomų asmenų) asmens duomenimis (šiuo atveju pavarde ir vardu), bet ir su nebūtinai visiems žinomų asmenų asmens duomenimis, jeigu tie duomenys (pavardė ar vardas) formaliai sutampa.

Tarnyba teikė konsultacijas ne tik dėl žurnalistikos tikslu tvarkomų asmens duomenų, bet ir dėl meninės saviraiškos tikslu tvarkomų duomenų. Buvo įvertintos situacijos dėl asmens duomenų (atvaizdų ir asmenų vaizdo įrašų) naudojimo spektaklio metu, pasisakyta dėl asmenų teisių ir teisėtų interesų apsaugos priemonių tinkamumo ir pakankamumo. Šiame kontekste Tarnyba teikė išaiškinimus ir dėl scenos meno kūrinių atlikėjų pasirodymų tiesioginių transliacijų socialiniuose tinkluose teisėtumo sąlygų.

Kaip ankstesniais metais, taip ir ataskaitiniu laikotarpiu, susidomėjimo neprarado teisė būti pamirštam internete. Šios teisės įgyvendinimo žiniasklaidoje galimybėmis labiausiai domisi ir siekia teisti, reputacijos problemų turintys asmenys. Visuomenės informavimo priemonės naudojasi specifinėmis teisėmis, garantijomis ir išimtimis iš bendrų asmens duomenų apsaugos taisyklių.

Nors teisė būti pamirštam yra įtvirtinta Reglamente, tačiau Lietuva šios teisės taikymui, kai asmens duomenys tvarkomi įgyvendinant saviraiškos ir informacijos laisvę, yra įtvirtinusi išimtį.

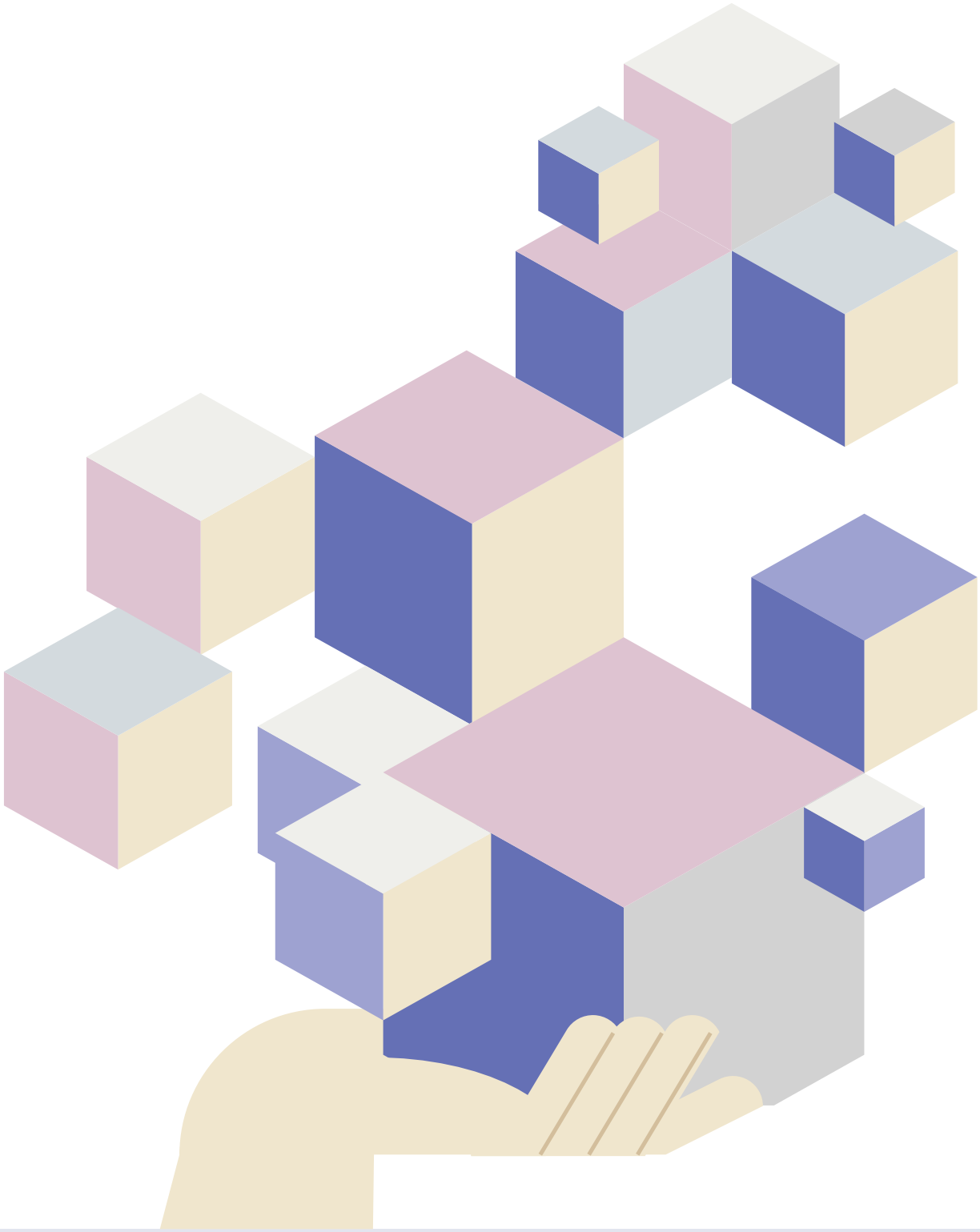
Kai asmens duomenys tvarkomi žurnalistikos tikslu, Reglamento 17 straipsnis („Teisei būti pamirštam“) yra netaikomas. Net teistumo išnykimas nėra pakankama faktinė aplinkybė, galinti įpa-

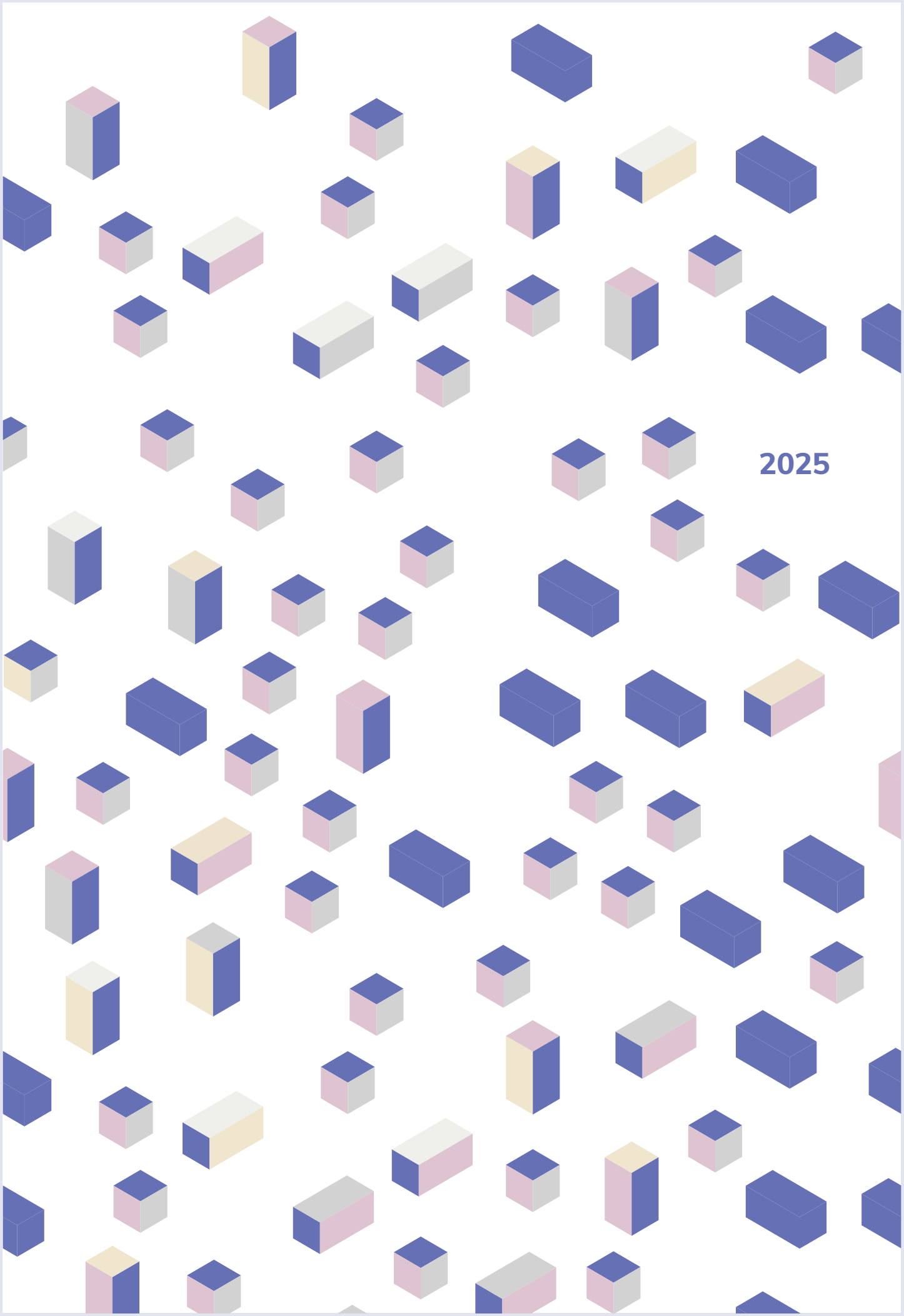
reigoti interneto svetainės valdytoją „pamiršti“ teistą asmenį. Lietuvos įstatymų leidėjas įtvirtino praktiškai absoliučią „teisės būti pamirštam“ išimtį Lietuvoje. Vienintelis atvejis, kai teisė būti pamirštam turi būti praktiškai realizuojama yra tada, kai duomenų subjektas atšaukia sutikimą tvarkyti jo asmens duomenis ir toks sutikimas buvo vienintelis pagrindas tvarkyti jo duomenis. Svarbu pažymėti, kad sutikimo atšaukimas nedaro poveikio sutikimu pagrįsto duomenų tvarkymo, atlikto iki sutikimo atšaukimo, teisėtumui. Be to, asmuo negali reikalauti ištrinti visą žiniasklaidoje paskelbtą turinį remdamasis Reglamentu, nes šis teisės aktas nenumato informacijos, kuri nėra asmens duomenys, pašalinimo pareigos.

Asmenims kilo klausimų, ar galima ir kokia apimtimi bei kokiais atvejais viešinti vaizdus, kuriuose fiksuojami teisės pažeidimai ar jų pasekmės, pažeidėjų asmens duomenys, pavyzdžiui, kelių eismo taisyklių pažeidimai, žiaurus elgesys su gyvūnais, transporto priemonės vairavimas neblaiviam ir pan.

Tarnybos veiklos prioritetai ir toliau bus orientuoti į veiklos efektyvumo ir kokybės stiprinimą bei žinomumo visuomenėje didinimą. Sieksime aiškiai pristatyti Tarnybos teikiamą naudą visuomenei, institucijos kuriamą pridėtinę vertę, profesionalaus ir kokybiško darbo rezultatus bei indėlį į demokratijos stiprinimą. Tarnyba ir toliau daug dėmesio skirs rekomendacijų, gairių ir konsultacijų teikimui bei kitoms visuomenę informuojančioms, šviečiančioms ir edukacinėms veikloms, padedančioms geriau suprasti ir įgyvendinti visuomenės informavimą reglamentuojančių teisės aktų reikalavimus.

REVIEW OF PERSONAL DATA PROTECTION SUPERVISION IN LITHUANIA BY THE OFFICE OF THE INSPECTOR OF JOURNALIST ETHICS




2025

FOREWORD BY THE INSPECTOR OF JOURNALIST ETHICS

Dainius Radzevičius
Inspector of Journalist Ethics

The relationship between the General Data Protection Regulation (the 'Regulation') and the producers and disseminators of public information, particularly journalists, is a subject of constant public debate. The Office of the Inspector of Journalist Ethics continuously receives inquiries regarding the scope of the Regulation and the application of exemptions for journalistic purposes. Increasingly, media representatives approach the Office requesting expert advice when state or municipal institutions refuse to provide information by citing the Regulation. Conversely, there is a growing number of complaints regarding personal data disseminated publicly, particularly on international algorithmic platforms. The Office of the Inspector of Journalist Ethics defends individual rights within the media; therefore, the Office's staff must ensure that human rights are protected in the media sector. The Office most frequently investigates complaints from individuals regarding violations of their honour and dignity or their right to privacy, as well as complaints submitted by data subjects under the Regulation. The right to be forgotten is becoming an increasingly frequent issue, requiring a continuous assessment of the justification for keeping such data public, while the journalistic purpose exemption is also significant for information published in media archives.

The Office is one of two supervisory authorities for the Regulation in Lithuania; therefore, close cooperation with the State Data Protection Inspectorate ensures the effective coordination of activities.

The Office dedicates, and plans to dedicate even more, attention to providing advice and training in the future. Although sufficient financial and human resources are not allocated to perform this function, close cooperation with other institutions, relevant organisations, and the media enables the effective dissemination of important information to the target audience.

Lithuania has established exceptional conditions for journalists to receive data, including data concerning private individuals, from state-managed registers and information systems free of charge; consequently, the status of producers and disseminators of public information, as well as journalists, is becoming an increasingly relevant topic, and isolated complaints indicate that it may be necessary to initiate additional amendments to legislation in this area, which are currently being discussed by the Media Council under the Ministry of Culture. This topic requires exceptional sensitivity and attention, as any new regulation may impact media freedom and its reflection in international press freedom indices.

MANDATE OF THE INSPECTOR OF JOURNALIST ETHICS

The Inspector of Journalist Ethics is an independent state official accountable to the Seimas, responsible for overseeing the implementation of the Law on the Provision of Information to the Public and the Law on the Protection of Minors against the Detrimental Effect of Public Information. They are also vested with the powers of a supervisory authority in the field of personal data protection – where data is processed for journalistic purposes or for the purposes of academic, artistic or literary expression, the Inspector of Journalist Ethics monitors the application of the Law on Legal Protection of Personal Data, and performs the functions of the supervisory authority in the Republic of Lithuania under Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (the 'Regulation') and the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data concluded in Strasbourg on 28 January 1981 (ETS No 108) and its protocols.

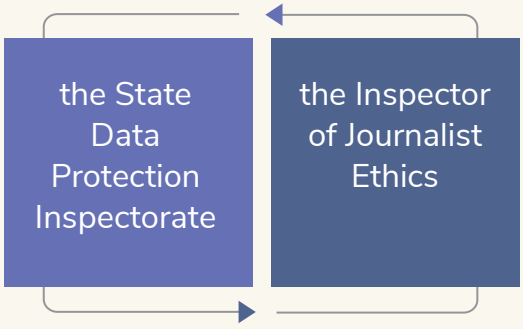
One of the key operational areas of the Office of the Inspector of Journalist Ethics (the 'Office') is fulfilling the institution's mandate to oversee prohibited online information. Under the Law on Information Society Services, which implements Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC, the Office is designated as a competent authority and is empowered to ensure the enforcement of this Regulation within its remit.

The primary function of the Inspector of Journalist Ethics is to investigate complaints from interested parties regarding violations of their honour and dignity or their right to privacy in the media, as well as complaints submitted by data subjects under the Regulation concerning the processing of personal data for journalistic, academic, artistic or literary purposes. It should be noted that, although the primary function of the Inspector of Journalist Ethics is to investigate complaints from interested parties, this function is performed in light of their role, as provided for in the Law on the Provision of Information to the Public, as a guarantor of human rights in the media sector, i.e., by ensuring the proper realisation of the public interest: freedom of speech and the press, and public information.

In addition to the primary function of investigating complaints and examining violations, the Inspector of Journalist Ethics performs a range of other functions: assessing compliance with the fundamental principles of public information, monitoring content in the media (excluding radio and television), conducting expert assessments of published content regarding the incitement of hatred on various grounds, classifying media content into erotic, pornographic, and/or violent categories, submitting proposals to the Seimas and other state institutions on improving and implementing legislation regulating public information, collaborating with counterpart institutions in the European Union and other countries, and representing the Republic of Lithuania in international organisations within their remit.

Providing guidance on public information matters and conducting educational activities are not included in the statutory functions of the Inspector of Journalist Ethics. Nevertheless, subject to available resources, the Inspector and representatives of the Office organise training sessions and seminars, and deliver presentations on safeguarding human rights in the media, the legal protection of personal data in the media, and combating illegal content in the media. To contribute to a better understanding of the legal provisions regulating the media sector, the Inspector of Journalist Ethics and Office specialists provide advice and information to all interested parties on matters within the Office's remit.

Under the established legal framework, supervision of the application of the Regulation and the Law on Legal Protection of Personal Data in Lithuania is carried out by two entities: the Inspector of Journalist Ethics and the State Data Protection Inspectorate (the 'SDPI').



For effective personal data protection, it is essential to ensure seamless cooperation between these two institutions. During the reporting period, inter-institutional meetings were organised to discuss pertinent operational issues, share expertise, and exchange information. The Inspector of Journalist Ethics or representatives of the Office were invited to and participated in various events, conferences, and training sessions, where, alongside SDPI representatives, they shared their expertise and insights on personal data protection and the right to privacy.

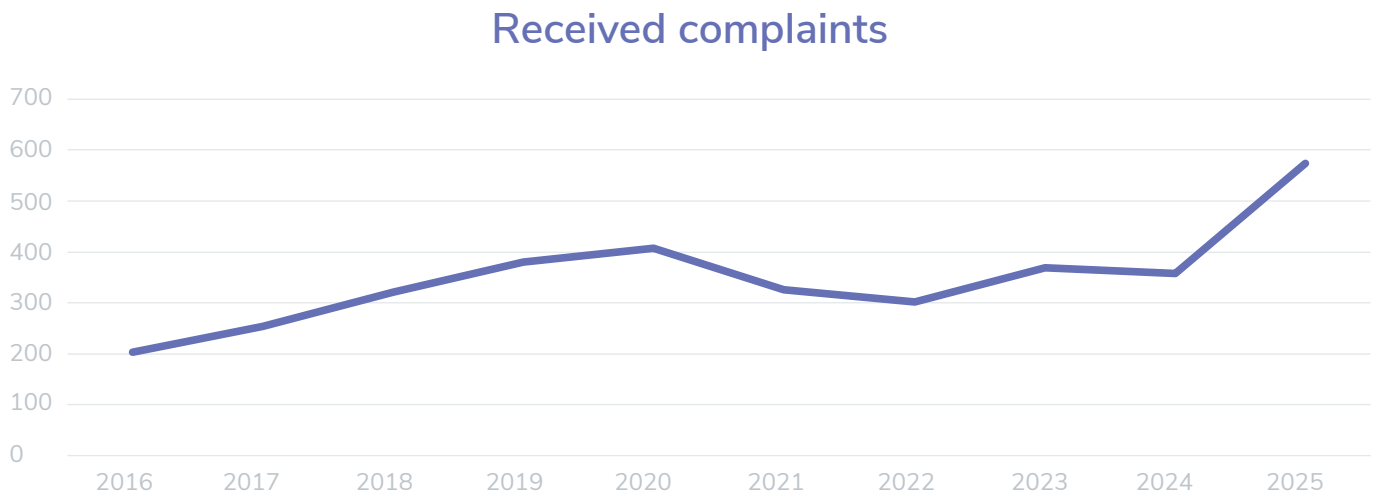
The need for cooperation with the State Data Protection Inspectorate is steadily growing, as practical cases become increasingly complex, and clearly defining and separating the remits of the two supervisory authorities poses additional challenges. There is a growing need to align institutional positions to ensure the uniform interpretation and application of the Regulation's provisions, appropriate reporting, the prompt exchange of relevant information, and constructive discussions on key issues concerning the supervision of the Regulation's implementation. Efforts are also being made to develop coordinated working mechanisms to ensure effective and consistent supervision, alongside preparation for the *ex post* evaluation provided for in the Law on Legal Protection of Personal Data.

Under the Regulation, each personal data supervisory authority must prepare an annual report on its activities, to be submitted to the European Data Protection Board, the European Commission, and the public. In cooperation with the SDPI, the Office submits its report on data processing supervision as a single joint document.

OVERALL STATISTICS ON COMPLAINTS AND DECISIONS

During the reporting period, the Office received a total of 574 complaints (358 in 2024) (see Figure 1). This indicates a significant increase in the number of complaints regarding potential violations in the media sector. Analysis of the complaints received reveals that an increasing proportion relates to content published on social networks. Information published on social networks is easily accessible and quickly reaches a wide audience; disputes frequently involve direct communication, which means that potential violations of personal rights on these platforms are more readily noticed and identified. This is likely one of the main reasons driving the overall increase in the number of complaints submitted to the Office.

Figure 1



A proportion of the complaints were forwarded to the Office by other institutions in accordance with their respective remits; there has also been a significant increase in the number of complaints concerning potential personal data violations forwarded by the SDPI. Various national police commissariats were highly active, forwarding cases falling within the Office's remit for investigation in accordance with their statutory duties.

Analysing these complaints helps identify key conflict situations and issues in the media sector; however, an analysis of the decisions issued provides a more comprehensive assessment of these trends. The decisions of the Inspector of Journalist Ethics reveal how the provisions of

the Law on the Provision of Information to the Public and other legislation are applied in specific situations; they also enable an assessment of emerging practical trends in defending individuals' personal rights. Analysing these decisions makes it possible to evaluate not only the nature of the identified violations, but also the criteria applied when balancing freedom of expression with the protection of individuals' honour and dignity, professional reputation, privacy, and personal data, as well as adherence to the fundamental principles of public information.

In 2025, the Inspector of Journalist Ethics issued a total of 435 decisions (see Figure 2), which assessed potential violations of the Law on the Provision of Information to the Public and other legislation regulating the media sector. When investigating complaints, each case involves an assessment of whether the balance between competing constitutional values (freedom of expression and the protection of an individual's honour and dignity, professional reputation, privacy, and personal data) has been compromised. The decisions analyse not only the content of the published information but also the context of its presentation, its purpose, and its connection to the public interest.

These decisions reflect not only the outcomes of individual complaint investigations but also the practical trends developed by the Office regarding the reconciliation of freedom of expression with the protection of individuals' personal rights.

Figure 2

Of all the complaints investigated in 2025, 109 were deemed unfounded. Such decisions are most frequently associated with situations where the disputed information pertains to matters of public interest, or where the applicants are considered public figures subject to broader limits of permissible criticism. At the same time, the decisions emphasise that freedom of expression is not absolute and cannot justify the dissemination of unfounded or factually unsupported information.

During the reporting period, a proportion of the investigations were terminated (56), including instances where the dispute was settled amicably through a mediation procedure (22). This method of resolution is applied in situations where the producer (disseminator) of public information rectifies the identified violations, and the applicant withdraws their complaint. Certain complaints are not investigated based on grounds established in the Law on the Provision of Information to the Public and the Law on Legal Protection of Personal Data; for example, when the complaint falls outside the Inspector's remit, there is insufficient data to initiate an investigation, or the time limit for submitting a complaint has expired.

PERSONAL DATA PROTECTION PRACTICE IN THE MEDIA SECTOR

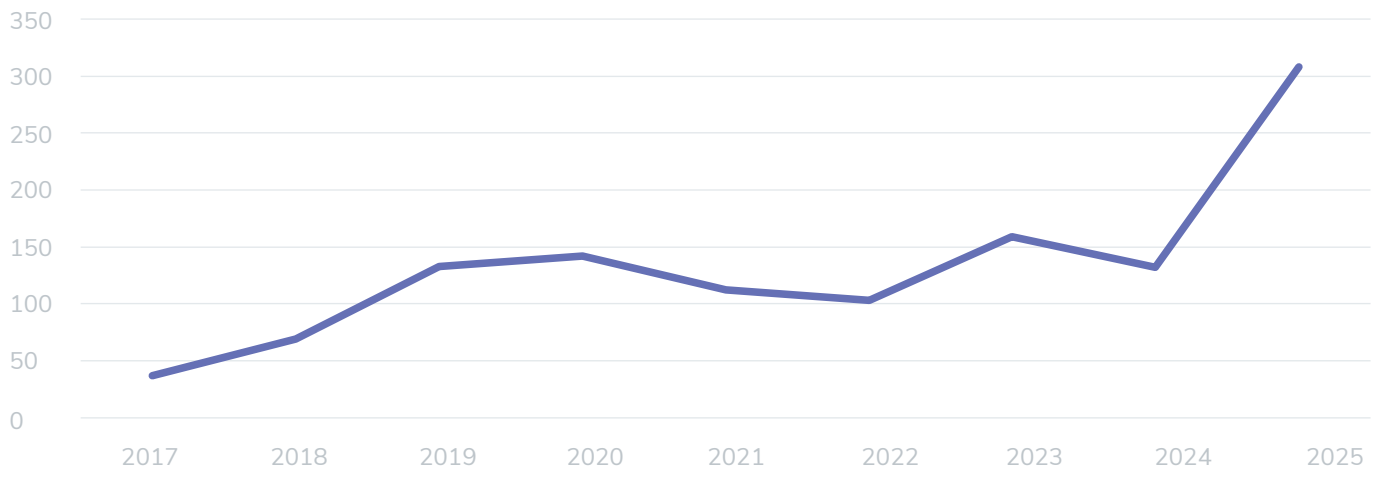
The 2025 data confirm a significant increase in complaints regarding the right to personal data protection. In 2025, 308 complaints were received (53% of all complaints) (see Figure 3); this figure has more than doubled compared to 2024, when 132 such complaints were received. It is important to note not only the absolute increase in these complaints, but also the shift in their relative proportion within the overall number of complaints: In 2024, they accounted for 37%, whereas in 2025 their share increased to 53%.

Therefore, more than half of the complaints submitted to the Office now relate specifically to personal data protection.

These dynamics reflect not only the increasing activity and awareness of data subjects in exercising their rights under the Regulation, but also the growing relevance of personal data protection issues in the contemporary information environment. At the same time, this shift indicates that personal data protection matters are becoming one of the predominant areas of complaints investigated by the Office, and complaints in this category are gaining increasing practical significance. Consequently, there is a need not only to ensure the effective investigation of individual complaints but also to consistently strengthen preventive measures and guidance aimed at implementing personal data protection requirements in the digital environment.

Figure 3

Complaints regarding personal data protection

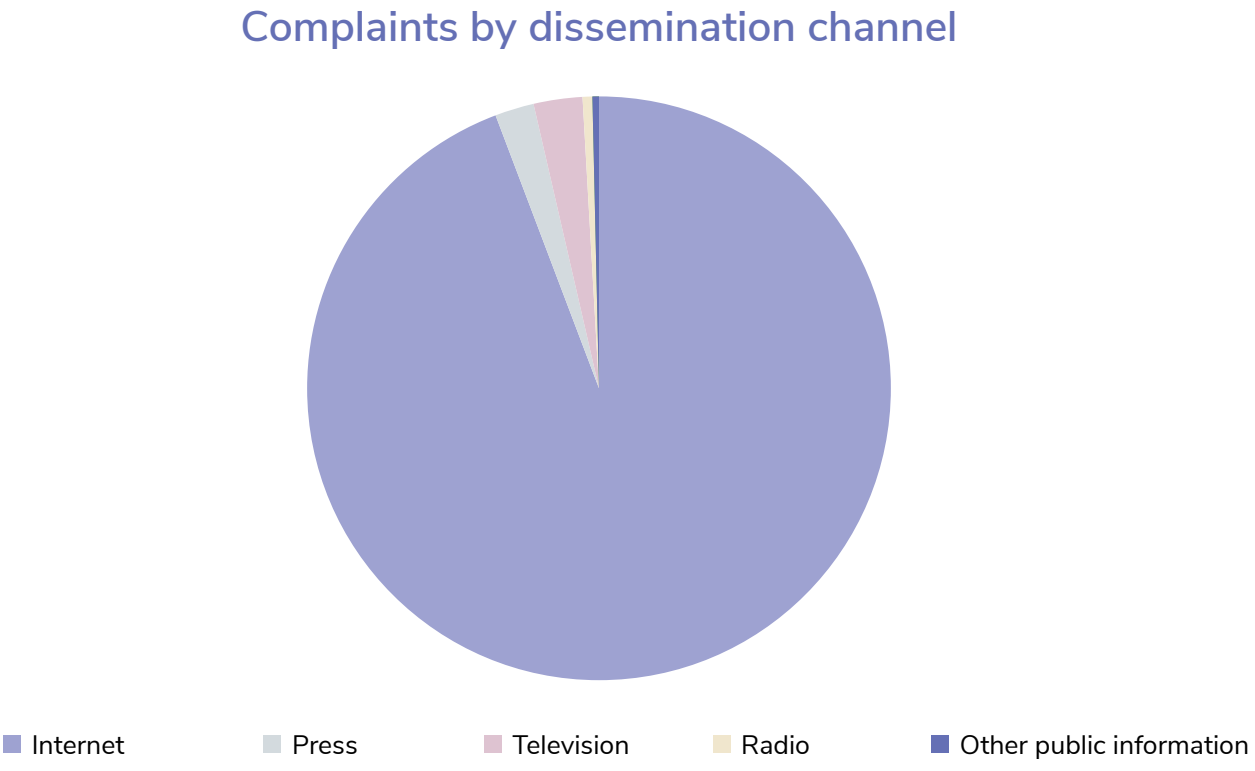


Investigating complaints during the reporting year confirmed that applying personal data protection requirements is inevitably linked to balancing the right to personal data protection and freedom of expression, particularly when personal data is processed for journalistic purposes or to serve the public interest. Although journalistic activity does not exempt one from the obligation to comply with the Regulation, data protection must not be applied in a manner that disproportionately restricts the public's right to receive information. Data processed for journalistic purposes is subject to certain data protection exemptions and derogations; however, these must be applied in accordance with the principles of proportionality and necessity. Below is an analysis of the complaints received in 2025, revealing the predominant data processing situations, the most frequently contested dissemination channels, and the primary challenges encountered when applying personal data protection requirements.

Predominant Complaint Category: Disclosure of Personal Data on Social Networks

As previously mentioned, a significant increase in complaints concerning potential personal data protection violations was recorded in 2025, driven primarily by the disclosure of information on social networks. It has been observed that the number of complaints regarding information published in traditional media (internet portals, the press, radio, and television) remains relatively stable. This confirms that personal data protection violations are increasingly concentrated on social networks, where information is disseminated rapidly and on a large scale, and where content is predominantly user-generated.

Figure 4



As in previous years, individuals frequently seek to defend their right to personal data protection when data is processed by social network account administrators who are not professional journalists. It must be emphasised that the majority of such complaints arise from interpersonal conflicts between private individuals seeking to publicly disseminate information about another person, their behaviour, or their alleged unreliability, as well as to disclose subjective personal stories. Situations where information about another person is presented in a conflictual or degrading context on social networks are particularly common in these complaints. For example, an instance was recorded where family photographs were published on the social network *Facebook* with the aim of publicly escalating an interpersonal dispute; this demonstrates that disclosure practices frequently overstep the boundaries of a legitimate purpose and amount to bringing a private conflict into the public domain.

One of the most commonly reported violations on social networks is the disclosure of personal data with the aim of publicly labelling another person as 'dishonest', a 'scammer', or a 'fraudster'. In such situations, names, surnames, photographs, and telephone numbers are published without consent, and the posts are frequently presented as a 'warning' to the community. For instance, in multiple cases on a *Facebook* account, an individual was publicly labelled a 'scammer' alongside the disclosure of their telephone number and photograph. Similarly, within *Facebook* groups titled 'SCAMMERS!!! FRAUDSTERS!!! CHEATS!!!', instances were noted where, even after the dispute was resolved (funds were returned), the posts were not removed, resulting in the ongoing disclosure of personal data. It is observed that on social networks, information regarding allegedly dishonest individuals (unreliable tenants, tradesmen, debtors) is increasingly published not only in specially created groups, but also—to reach a wider audience—in specific city noticeboards, marketplace groups, and other thematic groups. However, it should be noted that, although information published in closed groups frequently falls under the household exemption, a case was evaluated in 2025 where disputed information was published on the cover photo of a closed group, the content of which was visible to any user of the social network.

A significant proportion of complaints relates to the publication of residential addresses or photographs of private houses on social networks. Revealing a residential address is considered one of the most sensitive forms of personal data disclosure, as such information may, in certain cases, enable the identification of a specific individual and, as highlighted in the complaints, increase the risk of further security and privacy violations. The complaints frequently emphasise that the address or specific details of the living environment are disclosed during interpersonal disagreements, aiming to publicly escalate disputes, stigmatise another individual, or influence the individual's standing within the community. Such instances demonstrate that residential data on social networks frequently becomes a form of deliberate disclosure for private identification, giving rise to additional privacy risks. A typical case was recorded on the social network *Facebook*, where the applicant complained that their residential address had been disclosed with the aim of bringing neighbourhood disagreements into the public domain.

Social networks are becoming a space where data subjects encounter public 'naming' or identification within community groups. In practice, there are instances where an individual is photographed in a public place and their image is published in a social network group alongside derogatory comments or accusations. In one instance, a complaint was received regarding the publication of photographs of a minor child in *Facebook* groups, where the child was identified and discussed in conversations between adults. Such instances reveal that social network groups frequently become informal spaces for negative public evaluation, where privacy boundaries are easily crossed.

The year 2025 saw a high volume of complaints concerning minors' personal data, particularly a surge in the disclosure of their images on social networks. This is an exceptionally sensitive and high-risk area for personal data protection violations. The cases presented in the complaints demonstrate that a child's image, name, or other identification data are frequently disclosed without a lawful basis, often during conflicts, and without considering the potential long-term consequences of such information dissemination for the child. One of the most frequently occurring scenarios is the publication of minors' images in social network groups or on accounts, where the child becomes the subject of discussion or disagreement, despite not being connected to the underlying issue. For example, a complaint was received regarding the images of minor children when a mother of one of the pupils arrived, filmed the classroom, shouted at the teacher, and subsequently published the video recording featuring the visible faces of the minor children on her *Facebook* account, where the children were identified in a context completely unrelated to them. Such cases reveal that a child's image on social networks can be used as a tool in interpersonal disputes between adults, leaving the child's privacy interests unprotected. In practice, highly sensitive situations also arise where photographs of minors are disclosed alongside derogatory comments or negative evaluations. In one instance, an applicant filed a complaint because photographs of his minor daughter were disclosed in the chat channel of a *Facebook* group, accompanied by negative and derogatory remarks. Such cases pose an exceptional risk to the protection of minors' privacy. The complaints received also highlight instances where minors' data is disclosed in an institutional or community context, for example, at school events or meetings. In another instance, a complaint was filed that pupils were filmed and photographed during meetings, and this material was subsequently disclosed on social networks without explicit consent. Such situations indicate that, in practice, there is still a lack of clear understanding regarding the requirements for protecting minors' data and the obligation to ensure their privacy online.

The broader scale of the problem is revealed by cases where a public figure (a Member of the Seimas) published minors' personal data on their social network account, specifically, lists with the full names of pupils intending to attend a protest. This data was published publicly on so-

cial networks and linked to specific processes or circumstances that hold no independent public interest in terms of identifying the minors. Furthermore, the pupils were described as 'hecklers' alongside other negative epithets. In this instance, the minors became the subject of public discussion solely because their data was included in political or publicly oriented communication. Such practice is particularly problematic as publishing the minors' full names allows them to be directly identified, while the data subjects have no realistic ability to control the dissemination of this information. It is important to mention that the disclosure was carried out by an individual with significant influence in public discourse and a broad audience reach; therefore, the scale of information dissemination and the potential impact on the minors' privacy is objectively greater than in the case of ordinary social network users. Additionally, such communication may create the conditions for stigmatising the minors, attracting unwanted attention, or fostering negative evaluations within their social environment. This case revealed a significant practical problem: the use of minors' personal data in public and political communication without adequately considering their special legal status and heightened need for protection. The Office's practice confirms that even when aiming to publicly discuss pertinent societal issues, disclosing data that identifies minors cannot be considered a proportionate or necessary measure.

During the reporting year, complaints were received regarding sensitive health data published on social networks; although these do not constitute a significant proportion of the total number of complaints, they stand out due to the nature of the data processed. In one instance, a complaint was made concerning another person's medical record publicly displayed on the social network *TikTok*; this was published by mistake but contained highly sensitive data regarding the individual's health condition, allowing the data subject to be directly identified. It is evident that even the unintentional publication of such information creates the conditions for an exceptionally wide-scale dissemination of data, given the characteristics of content proliferation on social networks. In another instance, a complaint was submitted regarding comments on a *Facebook* post, where a doctor disclosed an individual's mental health condition while commenting on their capacity to hold a certain position. Such information was disclosed without consent; therefore, the issue of whether a lawful basis existed for processing the data and its proportionality was addressed. A complaint was received regarding an individual's HIV diagnosis published on a social network, where highly sensitive health information was disclosed alongside data identifying the individual. Such complaints have highlighted significant personal data protection risks arising from the highly sensitive nature of the data processed. These cases confirm that even the unintentional or limited-scale disclosure of health information on social networks can have a disproportionate impact on an individual's privacy and necessitates a particularly responsible assessment of the lawfulness of publishing such information.

An analysis of complaints from 2025 identifies a significant trend: the practical normalisation of personal data disclosure on social networks, where data revealing an individual's identity is increasingly perceived as an acceptable means of social communication. In such cases, the dis-

closure is frequently justified by a subjective aim to 'warn', 'defend oneself', or express an opinion, although objectively such practice does not meet the criteria of proportionality and necessity required for processing personal data. This trend is particularly pronounced in various community-based social network groups, where the disclosure of personal data becomes an instrument for exerting social pressure or forming negative evaluations. In such situations, the boundaries of privacy gradually weaken, and data subjects effectively lose the ability to control the dissemination of their information. The complaint analysis also indicates that social network account administrators frequently fail to realise that their public disclosure of personal data falls within the scope of the Regulation, regardless of whether they are considered professional producers and disseminators of public information.

Based on the practice established by the courts and developed by the Office, the public publication of personal data, when not based on a lawful purpose, such as serving the public interest, may be considered unlawful processing of personal data and give rise to legal liability.

This is especially pertinent on social networks, where information dissemination is rapid, the audience is broad, and the potential negative consequences for the data subject are difficult to control and complex to rectify.

As in previous years, a proportion of the received complaints relates to the dissemination of information in closed or semi-closed social network spaces, for example, private accounts, restricted-access groups, or other virtual platforms where content is accessible only to a circle of individuals defined by specific criteria. In such cases, applying the so-called 'household exemption' enshrined in point (c) of Article 2(2) of the Regulation is particularly relevant; under this exemption, the provisions of the Regulation do not apply when the processing of personal data is carried out by a natural person in the course of a purely personal or household activity. Practice has confirmed that instances of disseminating information in closed or restricted-access digital spaces require an exceptionally meticulous assessment of the factual circumstances. A clear distinction is essential between private communication, which falls outside the Office's remit, and the dissemination of information that, due to its content, scale of distribution, or actual accessibility, becomes part of the public sphere and meets the criteria for public information. In light of these circumstances, the investigation of complaints in the Office's practice in 2025 was based not only on assessing the content but also on analytical criteria concerning the scope of information distribution, audience size, and actual accessibility. Such an approach allowed for a consistent delineation of the limits of the Regulation's application, ensuring a clear division of remits while simultaneously establishing the conditions for the effective protection of individual rights in the digital environment.

Consequently, the practice of 2025 leads to the conclusion that social networks have become the primary arena for personal data protection violations, where overstepping the boundaries of personal data protection is frequently linked to interpersonal conflicts, community pressure, or an entrenched culture of public disclosure. These trends imply a need not only to respond to isolated violations but also to consistently develop preventive guidance, communicating clearly that social networks are not exempt from the application of personal data protection requirements, and that disclosing data without a lawful basis can lead to legal consequences.

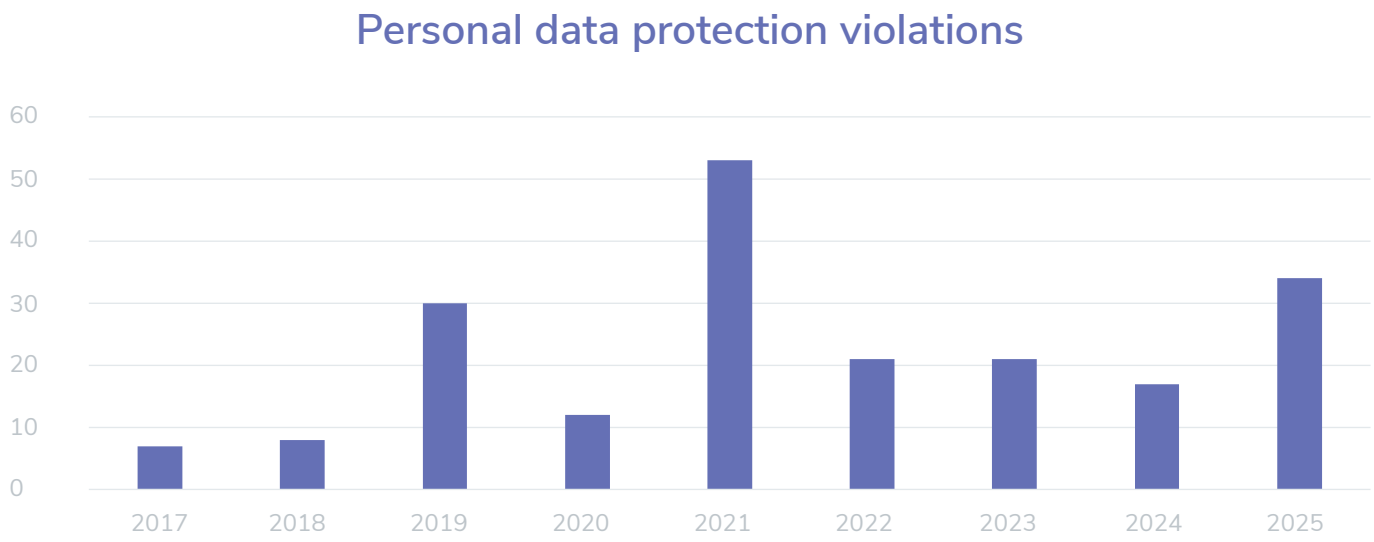
Taking into account the trends highlighted in the complaint analysis, the decision-making practice of the Office is discussed below, evaluating whether the publication of personal data in specific cases complied with the lawfulness and proportionality requirements set out in the Regulation.

The Office's decisions provide an opportunity to assess how personal data protection requirements are applied in practice when investigating the situations raised in the complaints.

The number of established violations of personal data processing in the media increased during the reporting year:

In 2025, 34 violations of the right to personal data protection were identified (see Figure 5). A violation of personal data processing is recognised in cases where the following facts are established: the processed information is considered personal data; the applicant's personal data was processed; actions constituting personal data processing were performed; and the personal data was processed without meeting the conditions for lawful processing set out in Article 6 of the Regulation. An analysis of the decisions indicates that personal data protection violations are most frequently related to the scope of the published data and its necessity for the intended purpose of informing the public. When evaluating specific situations, the decisions consistently analysed whether the published personal data had an objective connection to the public interest and whether its disclosure was proportionate to the topic under consideration.

Figure 5



The decisions issued in 2025 indicate that personal data protection issues constituted a significant proportion of the investigated complaints and exhibited a distinct disproportion across information dissemination channels. Although complaints were submitted regarding both the professional media and content published on digital platforms, the majority of the established violations relate to social networks and other user-generated content environments. Professional media activities accounted for a smaller proportion; however, it was precisely within these investigations that a significant analysis of proportionality and data minimisation was conducted. The decisions repeatedly emphasised that producers (disseminators) of public information must responsibly evaluate content before publication, ensuring that the planned publication aligns with the principles of personal data processing and the conditions of lawfulness, and that the data subject's interests, fundamental rights, and freedoms are not unjustifiably infringed. At the same time, the obligation to obtain an individual's consent to publish their data was highlighted, or, in the absence of such consent and a lawful basis, to refrain from disclosing such information.

The Social Network Environment: The Absence of a Lawful Basis and the Use of Personal Data in Conflicts

Violations identified on social networks were of a different nature. This space was dominated by situations where personal data was published without any lawful basis for its processing, or was used to achieve aims incompatible with the data processing principles set out in the Regulation, such as disclosing information during personal disagreements to discredit a specific individual or exert public pressure on them. In such cases, the publication of personal data was unrelated to the role of public information or the realisation of the public interest; therefore, it was deemed unfounded and failing to meet the requirements for lawful data processing. The decisions noted that publishing personal data on social networks frequently serves a different function from that in the professional media: it is used not to inform the public, but to publicly identify a specific individual and bring a conflict to a broader audience. In such situations, not only the content of the information but also the context and purpose of its publication were evaluated to determine whether the disclosure of the data was lawful.

In one instance, it was established that a video recording published on *Facebook* was disseminated in the context of a mutual dispute, rather than to inform the public on a significant issue. Although the filming took place in a public location, it was noted that this circumstance does not create an independent basis to publish an individual's image without their consent. In another instance, a video recording published on the *YouTube* platform, while declaring the aim of informing investors about potential financial risks, disclosed not only a full name, but also a personal identity number, date of birth, and residential address. The decision established that such data is not necessary for informing the public about potential risks, and its disclosure was deemed excessive. A significant proportion of cases involved situations where an individual's full name, workplace, contact details, or other identifying information was published during heated discussions to warn others or discredit a specific individual. The decisions noted that such data publication is linked to the escalation of mutual disagreements and cannot be considered lawful public information.

Instances of disclosing minors' personal data featured prominently in 2025, being evaluated in the decisions as an exceptionally sensitive category of data processing. It was noted that disseminating minors' data requires a particularly cautious assessment of proportionality, as children are considered a vulnerable group of data subjects who must be afforded a higher level of protection. In one instance, a minor's image was used in a political video recording, although it held no independent significance to the topic under consideration and did not contribute to disclosing information relevant to the public. The decision established that, even when filming in a public place, publishing a minor's image without a lawful basis violates the protection of their personal data, as being in a public space does not inherently grant the right to unrestrictedly disclose a minor's image. In another situation, the content of procedural documents was published, including information concerning the determination of a minor's residence, maintenance payments, and other aspects of family life. The decision noted that disclosing such information not only lacked an independent basis of public interest but also revealed sensitive circumstances of the minor's life, which by their nature belong to one of the most private spheres of an individual's life. It

was established that publishing details of procedural documents on social networks created the conditions for identifying the minor and expanded the intrusion into her private life; therefore, it was deemed unfounded and incompatible with personal data protection requirements. A case involving similar issues was also evaluated in another investigation. In the examined instance, the purpose of a post on a social network was to disclose a minor's behaviour at a dog show and initiate a discussion regarding the responsibility and transparency of junior handlers; therefore, the topic itself could be considered a matter of public interest. Nevertheless, the decision noted that such an informational aim could have been achieved through other measures that do not violate the protection of the minor's personal data. It was established that revealing the minor's full name and age was not necessary to discuss the issue at hand; therefore, publishing this data was deemed excessive and incompatible with the requirements for protecting minors' personal data.

In all instances, a reminder was issued that the images, names, or other personal data of minors may only be published after obtaining the consent of their legal representatives, and only in cases where publishing such data is objectively necessary for the intended purpose of public information.

The decisions also emphasised that even in cases where information is published within the context of a public discussion or lawful public information, disclosing data that identifies minors is not permissible; the dissemination of such information can only be justified when the consent of their legal representatives has been obtained and the minor's right to a private life and the protection of their interests are not violated. The practice of 2025 confirmed that the protection of minors' personal data is evaluated in the decisions as a particularly sensitive area, where the criteria of proportionality are applied exceptionally strictly. Even in cases where the topic being discussed may be considered relevant to the public, publishing data that identifies a minor is not deemed necessary to achieve the aim of informing the public.

During the reporting year, complaints were investigated concerning the publication of an individual's image in closed social network groups, although in reality, such content is accessible to a significantly broader circle of individuals. In the evaluated cases, the applicants' images were used for a social network group's cover photos; therefore, they were visible not only to the group's members but also to other users of the platform who could view the group's content or its main page. The decision noted that this form of image usage expands the scale of personal data publication and creates the conditions for identifying a specific individual to a broader audience. When evaluating these situations, the decisions emphasised that the formal circumstance of a social network group's 'closed nature' does not inherently negate the obligation to comply with personal data protection requirements. It was noted that the lawfulness of data processing must be evaluated taking into account not only the declared access restriction but also the actual accessibility of the content and the ability to view it publicly. Therefore, in cases where an individual's image or other identifying data is published in a manner that allows an indefinite number of social network users to view it, it was established that such information dissemination constitutes the public publication of personal data and must comply with the general requirements of data processing lawfulness and proportionality.

A summary of the decision-making practice regarding personal data disclosed on social networks reveals that personal data protection violations are most frequently established in cases where excessive identifying information is published that lacks an objective connection to the issue at hand or the public interest. Such situations are recorded particularly frequently on social networks, where personal data is used in conflicts or with the aim of publicly identifying a specific individual. The decisions consistently emphasised that, even within the context of public interest, published data must be limited to the extent necessary to achieve the purpose of informing.

Complaints Regarding Personal Data Processing in the Professional Media

The complaint practice during the reporting year demonstrates that complaints regarding personal data processing in the professional media, although quantitatively forming a smaller proportion within the overall context of personal data protection complaints, are characterised by greater legal complexity and are significant in shaping the Office's practice. These complaints are most frequently related to content published by news portals, which remains accessible long-term, and where the impact on individuals may be broader. Typical examples of complaints include instances where individuals are identified (by specifying their full name) in publications, although the applicants themselves do not consider themselves public figures and fail to see sufficient public interest for their identity to be revealed. The complaints emphasise that the individuals' role in the described event is secondary or lacks independent significance from the perspective of public information. For example, a complaint was received regarding a publication about a local conflict, which specified a private individual's full name and place of residence, although, in the applicant's assessment, generalised or anonymised data would have been sufficient to achieve the informational aim. A significant proportion of complaints relate to the coverage of pre-trial investigations or criminal cases in instances where information was published at the onset of the legal process, yet the outcome of the case subsequently changed, frequently in a direction favourable to the applicant. In such cases, the complaints indicate that although the information may have been considered relevant at the time of publication, its long-term disclosure causes a disproportionate negative impact on the applicant's reputation. In one instance, an applicant complained about a publication where he was identified as a suspect, even though the pre-trial investigation was subsequently dropped. Furthermore, complaints were recorded concerning the excessive disclosure of personal data, where a news portal provided additional details of an individual's private life alongside the primary information about an event. For example, a publication about an accident specified the injured party's place of residence, marital status, and other contextual information which, according to the applicant, lacked significance for the purpose of informing the public.

In 2025, a significant proportion of complaints was received concerning the potential unlawful publication of deceased persons' data in the public domain. The majority of these appeals were submitted by the relatives of the deceased and related to the disclosure of information concerning individuals who had committed suicide. Such information, by its nature, is highly sensitive and may cause a significant emotional impact on the relatives of the deceased. Nevertheless, the provisions of the Regulation apply exclusively to the personal data of living natural persons; therefore, the processing of deceased persons' data falls outside the scope of this Regulation. Accordingly, complaints regarding the processing of deceased persons' data cannot be evaluated

under the Regulation, regardless of whether the disclosure of such information may be considered unethical or inappropriate from the perspective of other legal norms.
An analysis of the content of the complaints identifies recurring categories of personal data, the disclosure of which in the professional media frequently becomes the subject of a dispute.

Complaints are most frequently lodged regarding the disclosure of the following personal data:

Full Name

This is one of the most frequent categories of complaints. Applicants appeal when private individuals are identified in the professional media whose role in the described event, they assert, is insufficiently significant from a public interest perspective. The complaints emphasise that revealing an individual's identity is not necessary for the purpose of providing information and could have been achieved by anonymising the data.

Image (Photographs or Video Material)

A significant proportion of complaints relates to publishing an individual's image without consent, particularly when the image allows for the easy identification of the person. Such cases occur in television programme reports or publications where photographs from public places, events, or social networks are used, yet their use, according to the applicants, is not directly linked to serving the public interest.

Data Concerning Procedural Status

Complaints are frequently made regarding an individual being named as a suspect, an accused, or otherwise linked to judicial or pre-trial processes in publications. The complaints note that the problem is particularly pronounced in instances where the process has not yet concluded, yet the initial information remains publicly accessible in the media.

Information Regarding Place of Residence or Location

The complaints indicate that the professional media occasionally provides addresses, specific cities, districts, or other data allowing the determination of an individual's place of residence or location. According to the applicants, such information holds no informational value and poses a risk of personal data violation and a threat to personal security.

Circumstances of Private Life

Complaints regarding personal data violations are also submitted concerning the disclosure of family relations, health condition, kinship ties, personal conflicts, or other sensitive circumstances. Although the event itself may be considered a matter of public interest, it is specifically the disclosure of excessive details in the media, unrelated to the public interest, that is disputed.

Indirect Data

Increasingly, complaints raise the issue of indirect data, for example, a telephone number, salary, property value, photographs of a residential house, workplace, job title, or specific biographical or physical details, which, although not individually identifying a person, cumulatively allow them to be recognised. In such cases, the applicants emphasise contextual identification as the primary source of the personal data protection violation.

In summary, the analysis of complaints from 2025 indicates that in the professional media, it is frequently not the fact of publishing information that is disputed, but the chosen scope and level of detail of the personal data. Applicants consistently raise the question of whether the aim of informing the public could have been achieved without disclosing excessive, identifying, or sensitive data, which confirms the significance of the principle of proportionality in the Office's practice.

During the reporting year, complaints relating to personal data processing in television programmes whose content is based on recording real-life situations, conflicts, or law enforcement actions remained pertinent, primarily concerning the programmes 'Farai' and 'TV Pagalba'. The format of these programmes, oriented towards documentary portrayal and an emotionally heightened form of presentation, poses specific personal data protection challenges, particularly in cases where private individuals are filmed in situations capable of exerting a negative impact on their personal data protection. Complaints regarding the programme 'Farai' most frequently raise issues concerning the disclosure of an individual's image, voice, and behaviour, where the filmed individuals are identified directly or indirectly. Applicants indicate that even when faces are obscured or names are omitted, contextual information (vocal timbre, living environment, location of the event, phrases used) allows for the recognition of a specific individual, particularly within local communities. In such cases, it is disputed whether the chosen anonymisation measures are sufficient to genuinely ensure the protection of the individual's identity. Complaints concerning the programme 'TV Pagalba' predominantly highlight the excessive disclosure of private life circumstances, where details of family conflicts, interpersonal relationships, and health or social problems are published. Applicants point out that, although participation in the programme is formally based on consent, in practice, doubts arise regarding the scope of the consent and the level of awareness, particularly when circumstances subsequently change and individuals seek to restrict the accessibility of previously published content. In the cases of both television programmes, the complaints also raise issues of indirect identification, where individuals are recognised not from directly specified data, but from the entirety: details of the place of residence, environment, family members, children, neighbours, or the specifics of the narrative. This form of identification is evaluated in the complaint practice as capable of causing long-term negative consequences for personal data protection and other personal rights. An important problematic aspect emerging in the complaints regarding the programmes 'Farai' and 'TV Pagalba' is the long-term accessibility of the content in the digital space. The complaints emphasise that episodes of television programmes hosted on internet platforms or the broadcaster's archives remain publicly accessible indefinitely, thereby increasing the scale of the potential personal data violation.

In summary, it can be concluded that the practice reveals a complex issue of balancing interests between the interests of informing the public, the characteristics of an entertaining documentary format, and personal data protection in vulnerable situations. The Office's practice in such cases is oriented towards the individual assessment of specific circumstances, paying particular attention to the content of the consent, the sufficiency of anonymisation, and the application of proportionality criteria, to ensure that the aims of public information are not realised by disproportionately restricting an individual's right to personal data protection, while concurrently not violating the public's right to know. The problems highlighted in the complaint analysis are also reflected in the Office's decisions, which evaluate whether the personal data published in specific cases complied with the requirements of lawfulness and proportionality.

Cases of Professional Media: Scale of Identification and Proportionality of Visual Information

Decision-making practice demonstrates that violations in the professional media are established in cases where, despite the existence of public interest, the necessary scope of information is exceeded. In such situations, the decisions noted that the public interest justifies examining the topic itself, but does not grant an unlimited right to disclose any information relating to a specific individual. When assessing such cases, an analysis was conducted as to whether the published personal data, images, or other identifying details were objectively necessary to reveal the issue at hand, and whether the aim of informing the public could have been achieved without them. When it was established that certain data or visual elements did not contribute to presenting information significant to the public and merely expanded the possibilities of identifying an individual or published excessive data, it was concluded that the proportionate limits of information disclosure had been overstepped. In such cases, it was determined that even when lawfully aiming to inform the public, the scope of the necessary information must be limited to the extent objectively required to reveal the specific topic. One of the decisions evaluated a case where, while reporting on a high-profile crime, television reports and publications showed images of the residential house and environment of individuals unconnected to the criminal act, i.e. the suspect's parents. Although the criminal act itself held an obvious public significance, it was established that visualising the living environment did not contribute to revealing the event, but expanded the intrusion into private life and indirectly associated family members with a negative context.

Even when publishing personal data within the context of the public interest, it must be published only to the extent necessary to reveal the topic under discussion.

This is illustrated by a case where a publication concerning a potential conflict of interest in a municipality justifiably discussed aspects of public fund allocation, yet additionally published a photograph of the applicant's residential house. The decision noted that such visual material was excessive, lacked a direct connection to the issue at hand, and additionally expanded the scope of personal data disclosure. A third case related to a publication concerning an administrative offence: the short-term parking of a vehicle in a prohibited location. Although the topic could be linked to ensuring public order, it was established that publishing the specific individual's image was not necessary to achieve this aim. The issue could have been discussed in generalised terms, without identifying the data subject.

These examples demonstrate that in the context of the professional media, the violations established in 2025 were isolated in nature and predominantly related to overstepping the limits of proportionality – situations where a lawful aim of informing the public is realised through the use of excessive identification methods or visual information. Within the overall context, such violations constituted a minor proportion of all established personal data violations, which indicates that in the practice of the professional media, questions more frequently arise not regarding the lawfulness of the information itself, but concerning the scope of specific identifying elements and their proportionality.

The decisions of 2025 reveal a consistently developed practice of evaluating personal data protection and allow for the identification of the primary directions of the issues arising. The decisions emphasise that the existence of a public interest does not inherently grant the right

to disclose any data relating to an individual – it must be specific and directly linked to the content of the published information. At the same time, it was highlighted that the principle of proportionality entails not only the societal significance of the topic under consideration but also the obligation to evaluate whether the specific published data is objectively necessary to reveal this topic. An analysis of the decisions also demonstrates that the largest proportion of personal data protection violations was established on social networks, where personal data is frequently disclosed not with the aim of informing the public, but as a reaction to personal conflicts or emotional situations. In such cases, the publication of data becomes a tool for exerting pressure, discrediting, or escalating a public dispute, rather than public information. For this reason, the decisions consistently emphasised that the relationship between the aim of informing the public and the scale of individual identification becomes the essential criterion for evaluation – when the published data is not necessary to reveal the topic at hand, its disclosure is deemed unfounded.

Analysing the violations established during the reporting year reveals that they are most frequently related to the excessive or unfounded disclosure of specific personal data. The most frequently disclosed data included an individual's full name, particularly in cases where their publication is not justified by a clear public interest, as well as an individual's image, which is frequently published on social networks without the data subject's consent. Instances were also established where contact or identifying information was disclosed, for example, residential addresses, telephone numbers, or vehicle registration plates, as well as details of private life relating to an individual's health condition or family relations. A significant proportion also comprised instances of disclosing minors' data: the publication of their photographs, names, or other identifying data. Practice indicates that these violations most frequently arose due to the excessive disclosure of personal data where there was no clear informational aim or genuine public interest, as well as the use of private data in personal disputes with the aim of discrediting a specific individual, and due to insufficient data anonymisation, where the published information allows individuals, including minors, to be clearly identified.

Issues Concerning the 'Right to be Forgotten'

A distinct theme of personal data issues during the reporting year related to the application of the right to request the erasure of data (the 'right to be forgotten'). In 2025, compared to 2024, an increase in the number of complaints regarding the right to be forgotten was recorded. Such complaints constituted approximately 4% of all complaints submitted to the Office, whereas in 2024 their proportion stood at around 2%. This shift indicates a growing desire among applicants to restrict the long-term public accessibility of information relating to them in the digital space, despite the restrictions on the application of the right to be forgotten enshrined in the national legal framework. An analysis of the nature of the complaints submitted in 2025 shows that they remain fundamentally similar to the complaints of previous years. The majority of complaints are submitted by individuals previously linked to criminal acts or other publicly discussed legal processes, most frequently relating to the publication of old cases, pre-trial investigations, or court judgments in the media. Applicants typically assert in their complaints that, although the information was accurate at the time of its publication, its long-term retention on the internet, in their assessment, no longer complies with the requirements of the right to personal data and privacy protection, exerts a negative impact on their social reintegration, and that a case outcome favourable to the applicants is not appropriately or sufficiently clearly reflected in the public sphere. Inter alia, it is frequently emphasised that search engine algorithms prioritise negative information, ignoring subsequent positive changes in an individual's life or activities. Consequently, despite the exemption from this right enshrined in the Regulation, applicants actively exercised their right to request the restriction of public accessibility to older information relating to them in 2025. The complaints most frequently raise issues concerning archival information that was published lawfully but, in the applicants' assessment, has lost its relevance over time and no longer meets the criteria of proportionality, particularly when the individual is no longer a public figure, their social or professional status has changed, or when publicly accessible information continues to exert a negative impact on their reputation. The applicants' position in these complaints is frequently based not on an aim to deny historical facts, but on a request to reconsider the long-term accessibility of information in the digital space in light of changed circumstances. It is particularly emphasised that information remaining in media archives or search engines, even where exemptions to the right to be forgotten exist, in practice creates a persistent effect of privacy restriction which, in the applicants' assessment, is no longer justified by the public interest.

In practice, situations arise where the non-application of the 'right to be forgotten' raises questions of proportionality, particularly in cases where archival information publicly accessible for a long period continues to exert a significant impact on an individual's privacy, although its relevance from a public interest perspective has passed. For example, in one of the complaints evaluated by the Office, the disputed information was published 16 years ago; in the publication, the applicant shared circumstances of their private life, detailing their relationship with their then-fiancée and aspects of establishing a business. During this period, the circumstances specified in the publication changed significantly. The applicant separated from the fiancée, and both established other families. The continued publication of the information is distressing for the applicant and their former fiancée, and the topic of the publication is unrelated to any issue of public

interest relevant to society. In such cases, the implementation of the 'right to be forgotten' could be linked to alternative measures oriented not towards the removal of information, but towards restricting its accessibility. Delisting, which restricts the accessibility of information via search engines, could serve as a proportionate measure, enabling a reduction in the long-term impact of archival information on an individual's privacy while concurrently preserving the public's right to access this information.

The validity of the Office's decisions regarding the right to be forgotten was also evaluated in case law. It should be noted that, although the Law on Legal Protection of Personal Data establishes that Article 17 of the Regulation, which enshrines the right to be forgotten, does not apply when personal data is processed for journalistic purposes, during the reporting year an applicant disagreed with this provision and appealed to the Regional Administrative Court against the decisions of the Inspector of Journalist Ethics, in which the applicant's complaints concerning the non-implementation of the right to be forgotten were rejected. On 4 September 2025, the Regional Administrative Court adopted a decision in administrative case No eI3-10074-1114/2025, in which it confirmed the assessment of the Inspector of Journalist Ethics that the provision of Article 4 of the Law on Legal Protection of Personal Data, establishing exemptions to the application of the Regulation when processing personal data for journalistic purposes, is imperative; therefore, the implementation of the right to be forgotten in respect of the applicant was lawfully refused. This decision of the Regional Administrative Court has been appealed to the Supreme Administrative Court of Lithuania (the 'SACL'). Nevertheless, in its essence, this is a significant clarification regarding the validity of the Inspector of Journalist Ethics' decisions concerning the right to be forgotten and the appropriate application of the Regulation's exemptions. The court's decision confirms the Office's interpretation of the Regulation's exemptions and demonstrates that in the context of data processed for journalistic purposes, the implementation of the right to be forgotten is restricted.

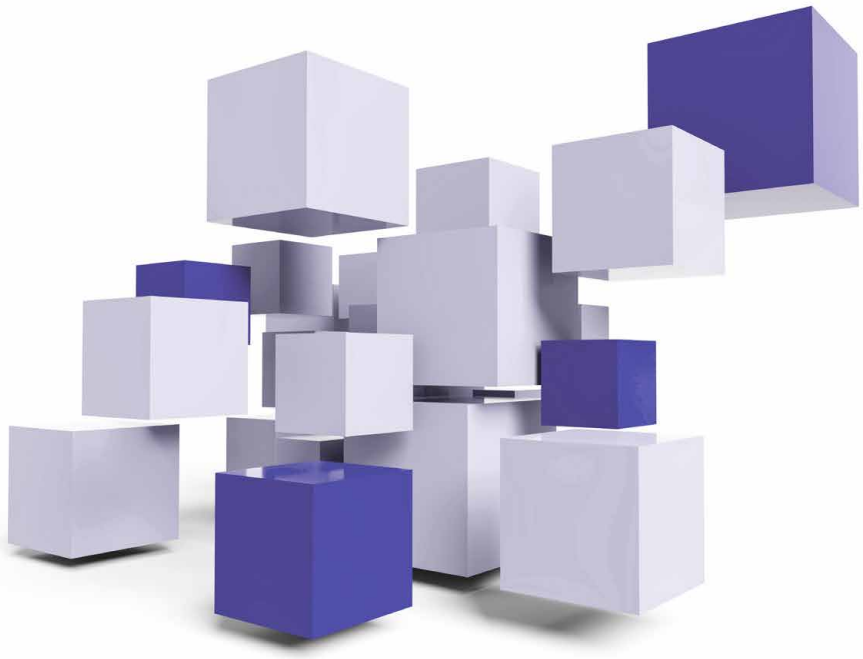
An analysis of the decisions adopted in 2025 shows that ensuring personal data protection in the media sector requires consistent and proportionate evaluation. In each instance, it is necessary to evaluate whether the publication of data in the specific case is objectively necessary to achieve the informational aim, whether the measure least restrictive to individual rights has been chosen, and whether the scale of disclosure oversteps the boundaries of legitimate public interest. Decision-making practice also reveals that the greatest personal data risks arise on social networks, where the majority of violations were established. On these platforms, personal data is frequently disclosed without evaluating the lawfulness, proportionality, and necessity of its publication, and the published information frequently allows individuals to be identified or reveals circumstances of their private life, including minors' data, even though such information is not necessary to reveal the topic under consideration. This confirms that when evaluating the lawfulness of publishing personal data, decisive significance lies not only in the topic of the information but also in the publication of specific data and the scale of its dissemination.

Summarising the complaints investigated and the decisions adopted by the Office in the field of personal data protection, it should be noted that in 2025, disputes in this area predominantly arose regarding the lawfulness and proportionality of disclosing identifying data published in the public sphere: a full name, image, contact information, or other details linked to a specific individual. The complaints demonstrate that personal data protection issues frequently intertwine with other rights: the protection of privacy, honour and dignity, or the presumption of innocence. Practice confirms that a risk to individual rights arises not only from the publication of inherently sensitive data but also from a combination of individual data points, not considered sensitive in themselves, which collectively create genuine preconditions for establishing an individual's identity or linking an individual to specific circumstances. Instances where minors' data, data concerning ongoing judicial processes, or information allowing for the identification of an individual in conflictual or socially vulnerable situations are disclosed remain particularly sensitive.

Complaints received in 2025 regarding the lawfulness of personal data collection highlighted issues concerning the definition and interpretation of the concept of a producer (disseminator) of public information, and concurrently, the scope of rights associated therewith. During the reporting year, complaints were received from three individuals regarding personal data collection actions in registers managed by Registrų Centras VĮ, carried out by Vilniaus Magas VšĮ (the name was changed to Spaudos Klubas VšĮ during the investigation). When the applicants contacted Registrų Centras VĮ, it was explained that Vilniaus Magas VšĮ is registered in the Information System of Producers and Disseminators of Public Information (VIRSIS), collects data for journalistic purposes, and that a Unified Data Provision Agreement had been concluded with it, under which Vilniaus Magas VšĮ is entitled to receive data and information from the register or state information system manager free of charge. In their complaints, the applicants questioned whether the journalistic purpose was being fabricated in this case, as Vilniaus Magas VšĮ does not manage any media outlets and has not published any publications or other public information. In its explanations to the Inspector of Journalist Ethics, the institution indicated that it intended to publish a book titled 'Vilniaus magas' about the secret links between the media, business, and the criminal world, and was collecting data from Registrų Centras VĮ specifically for this purpose. This case prompted an evaluation of the definitions of a producer and disseminator of public information enshrined in the Law on the Provision of Information to the Public, and a consideration of from what point an individual may be deemed a producer and/or disseminator of public information.

Undoubtedly, both the concept of a producer (disseminator) of public information and the journalistic purpose are also applicable to collecting information for a work in preparation; nevertheless, the activity of a producer (disseminator) of public information must be genuine, rather than hypothetical or potentially arising in the future.

It should be noted that the abstract definition of a producer (disseminator) of public information in the Law on the Provision of Information to the Public may have created opportunities for abuse, allowing individuals to register in the Information System of Producers and Disseminators of Public Information and exploit this status, i.e., the right to receive data and information from a register or state information system manager free of charge, as well as the right to receive information from state and municipal institutions and bodies within one working day, despite not carrying out any genuine activities in this capacity. This situation simultaneously demonstrates the need to evaluate the suitability of the provisions of the Information System of Producers and Disseminators of Public Information (VIRSIS) and the possibility of establishing additional registration control mechanisms; under the current procedure, data is registered in the system and published publicly from the moment it is signed by the individual providing it, yet neither the system manager nor the processor verifies whether the registering individual and their activity meet the criteria for a producer and/or disseminator of public information. The absence of control or review creates the conditions for any individual to register in the Information System of Producers and Disseminators of Public Information (VIRSIS) and unjustifiably exercise the rights guaranteed to producers (disseminators) of public information. At the same time, such a situation poses a serious threat to personal data protection, where highly sensitive information becomes accessible to an individual who operates under the guise of a journalistic purpose and the status of a producer (disseminator) of public information, despite not carrying out such activities and collecting personal data for unclear purposes.



ADVISORY ACTIVITIES

As in previous years, the Office actively developed its advisory activities in 2025. As an institution centralising expertise in media law and the protection of human rights within the media sphere, the Office is approached not only with complaints but also with various inquiries, requests for advice, and requests for information in the media sector. The Office strives to ensure that these services are of high quality and accessible to the broadest possible audience. Such activities contribute both to increasing the Office's visibility and to fostering a deeper understanding of the protection of individuals' personal rights in the media.

Advising interested parties and providing information on matters falling within the remit of the Inspector of Journalist Ethics constitutes an important part of the Office's activities. Any individual who has questions regarding the publication of public information, the protection of human rights, and the realisation of freedom of expression and information in the media may contact the Office for advice. We aim to effectively meet the legitimate and justified expectations of every individual contacting the Office. Advice is provided verbally (by telephone or in person at the Office), in writing, and by email. Every visitor to the Office's website can ask a question, leave a comment, or submit a proposal by completing a special form, as well as submit an inquiry via the Office's Facebook account. The Office's representatives respond promptly to every inquiry, provide the requested information or advice, and assist in gaining a better understanding of legal requirements.

In 2025, the Office provided a total of 1,073 consultations. Compared to the previous reporting period, the overall number of consultations provided slightly increased (1,007 in 2024; 1,120 in 2023; 779 in 2022). The trends regarding the most frequently provided consultations remained practically unchanged: individuals were predominantly interested in questions concerning the interpretation and application of the Regulation within the media sector. This constituted approximately two-thirds of all consultations provided. Although this European Union legislation, which implemented the personal data protection reform, has been applicable since 25 May 2018, the Office's practice indicates that the number of questions regarding the processing of personal data for journalistic, academic, artistic, or literary purposes remains high.

Figure 6

The outcomes of the Office's activities demonstrate that the Regulation has fundamentally altered the public's perception of personal data protection and privacy in the media, and its significance is not diminishing over time. This is confirmed by the consistently high number of both complaints and consultations regarding the processing of personal data for journalistic (public information) purposes. There is an increasingly noticeable growth in the awareness of data subjects and rising expectations concerning the protection of their rights in relation to personal data processing. Such consistent public activity forms a solid foundation for ensuring that the Regulation is not only formally applied, but also genuinely and effectively implemented in practice.

Due to a lack of financial resources, a separate impact assessment of the Guidelines on the Provision of Information to Representatives of the Media and the Public Sector, i.e., the practical guidelines regarding the provision of information held by institutions operating in the public sector that contains personal data to media representatives[1] (the 'Guidelines'), which the Office prepared in conjunction with Mykolas Romeris University in 2023, has not been conducted; however, meetings and conversations with journalists and media-associated organisations indicate that the Guidelines are highly regarded as a valuable tool that facilitates their work. Everyone acknowledges that the Guidelines are effective and helpful; nevertheless, a significant proportion of the consultations provided by the Office during 2025 continued to involve advising interested parties on the right of media representatives to receive information from public sector entities.

Media representatives still encounter problems where, due to an incorrect interpretation of the Regulation, journalists' right to information is unjustifiably restricted, particularly concerning journalistic investigations related to public figures, the use of public funds, and similar matters.

Consultation practice indicates that the Regulation is still used by certain state and municipal institutions and bodies as a tool to avoid undesired media scrutiny into a topic they wish to conceal from the public.

[1]See https://www.zeit.lt/data/public/uploads/2023/02/gaires-1.pdf

As in previous years, public sector institutions most frequently contacted the Office requesting advice on how to correctly balance journalists' right to information and the right to data protection under the Regulation. Questions arise for representatives of the government and the public sector regarding the scope of data to be provided, the concept of a journalist, and the interpretation of the definition of journalistic activity. The status of increasingly popular freelance journalists and representatives of citizen journalism, alongside their right to receive information, particularly information involving personal data, caused the most uncertainty for institutions implementing the Law on the Right to Obtain Information and Data Re-use. Frequently, requests were made to clarify how a public authority could ascertain that the individual requesting information is a journalist or a person equated to one, how to respond to requests from journalists when excessive data is requested, and how to apply specific principles related to data processing.

It should be noted that case law is developing in a direction where, aiming to take into account the importance of freedom of expression for the entire democratic community, the concepts associated with it, including journalism, must be interpreted broadly. The exemption for journalistic activities is not linked to legal employment relations within a specific media outlet or professional membership of a journalists' professional organisation. It is granted to any individual engaged in an activity whose aim is to disseminate information, opinions, or ideas to the public by any means of transmission.

Media representatives requesting information containing personal data from public sector institutions must ensure the lawful and fair further processing of the data. Media representatives, when requesting information containing personal data from public sector institutions, must ensure its lawful and fair further processing. Such interaction between the public sector and the media in the area of data accessibility, based on mutual commitments, best reflects the importance of freedom of expression in a democratic society. The Guidelines are a recommendatory document and cannot resolve all problems of interpreting the Regulation or provide universal answers to all questions. Every data processing situation is evaluated individually, taking specific circumstances into account. The Guidelines can serve as a useful benchmark for public sector institutions, assisting them in carrying out proportionality assessments when processing data, transparently providing information and personal data to journalists, and ensuring an appropriate balance between freedom of information and personal data protection.

The Office's activities demonstrate that the use of the Guidelines is becoming increasingly widespread. Aiming to further facilitate cooperation between public authorities and journalists requesting information, the Office will continue to actively seek to increase the visibility of the Guidelines and their applicability.

A significant proportion of the consultation requests received by the Office relate to filming (photographing) individuals in public places, at events, and in educational institutions, the public publication of such images, the distribution of children's photographs without parental consent, the publication of an individual's full name, image, residential address, or vehicle registration plate, information concerning an individual's health, and the implementation of data subjects' rights in the activities of the media. The year 2025 demonstrated similar trends. The strict requirements for the legal protection of personal data increased the need for advice regarding the appropriate form of expressing consent to process data, the duration of data retention, video surveillance,

and the unlawful collection and disclosure of information concerning an individual's private life. Taking into account that the Regulation does not apply in its entirety to the processing of personal data for journalistic purposes, interested parties frequently inquire about the exemptions where the right to personal data protection is reconciled with freedom of expression and information, sanctions for data processing violations, and other matters.

Questions regarding the lawfulness of processing personal data were frequently raised not in respect of journalists, but concerning individuals unconnected to this profession and the information they prepared and published (administrators of social network accounts, content creators, influencers, representatives of citizen journalism, authors of comments, etc.). Despite not being journalists, such individuals are considered producers (disseminators) of public information to whom data protection requirements also apply, legal enforcement measures are applicable, and liability arises for violations.

Last year, the Office was also consulted regarding the compliance of new words that have emerged in the Lithuanian language (neologisms published publicly for the benefit of science and society) such as *blinkevičiūtinti* (meaning 'to promise but fail to deliver'), *gabrieliauti* (meaning 'to make a pause of unclear duration in some activity') and similar, with the requirements for the legal protection of personal data, honour and dignity, or confidentiality. Clarification was sought as to whether the aforementioned words could be linked not only to the personal data of specific data subjects (publicly known individuals) (in this case, their full name), but also to the personal data of individuals who are not necessarily known to everyone, if their name formally coincides.

The Office provided advice not only concerning personal data processed for journalistic purposes but also regarding data processed for the purpose of artistic expression. Situations concerning the use of personal data (images and video recordings of individuals) during a theatrical performance were evaluated, and opinions were issued regarding the suitability and sufficiency of measures for protecting individuals' rights and legitimate interests. Within this context, the Office also provided clarifications regarding the conditions for the lawful live broadcasting of performing arts artists' performances on social networks.

As in previous years, during the reporting period, interest in the right to be forgotten on the internet did not diminish. Convicted individuals and persons with reputational problems are the most interested in, and seek to utilise, the possibilities of implementing this right in the media. The media enjoys specific rights, guarantees, and exemptions from the general personal data protection rules.

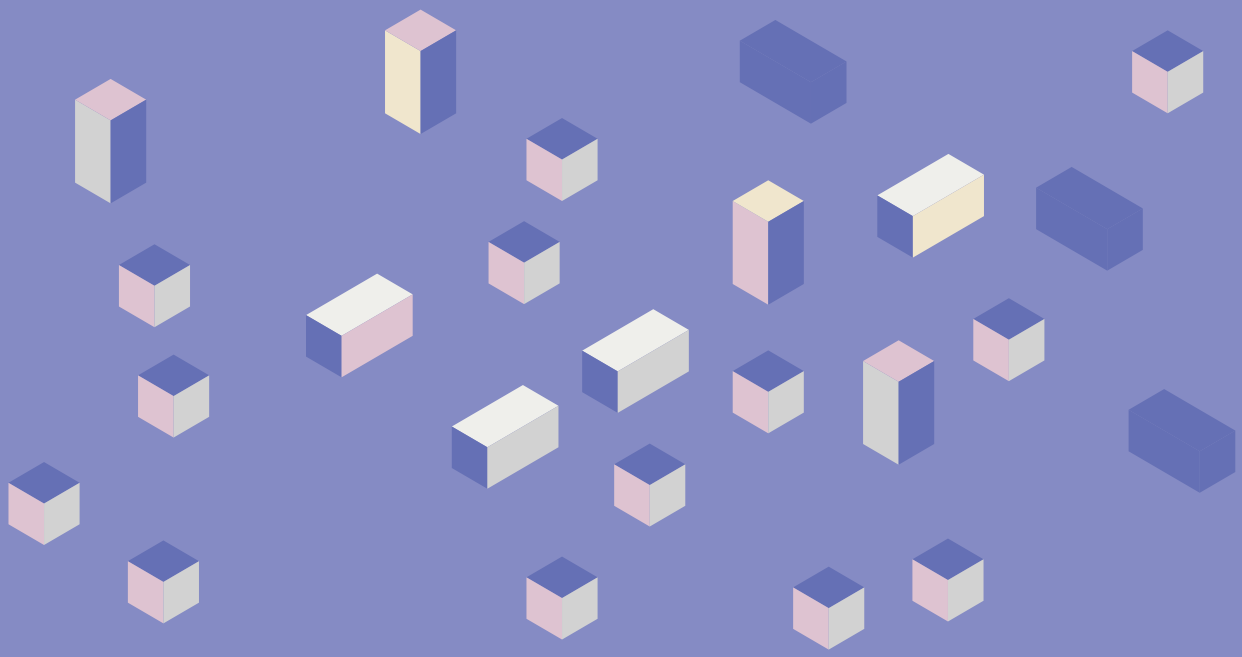
Although the right to be forgotten is enshrined in the Regulation, Lithuania has established an exemption to the application of this right when personal data is processed in the exercise of freedom of expression and information.

When personal data is processed for journalistic purposes, Article 17 of the Regulation (the 'Right to be forgotten') does not apply. Even the expiry of a criminal conviction does not con-

stitute a sufficient factual circumstance capable of obliging a website administrator to 'forget' a convicted individual. The Lithuanian legislator has established a practically absolute exemption to the 'right to be forgotten' in Lithuania. The only instance where the right to be forgotten must be practically realised is when the data subject withdraws their consent to the processing of their personal data, and such consent was the sole basis for processing their data. It is important to note that the withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal. Furthermore, an individual cannot demand the erasure of all content published in the media based on the Regulation, as this legislation does not provide for an obligation to remove information that does not constitute personal data.

Questions arose for individuals as to whether it is permissible, to what extent, and in what cases to publish images capturing legal violations or their consequences, alongside the personal data of the offenders, for example, road traffic rule violations, cruel treatment of animals, driving a vehicle while intoxicated, and similar.

The priorities of the Office's activities will continue to be oriented towards strengthening the efficiency and quality of its operations, and increasing public awareness. We will aim to clearly present the benefits provided by the Office to the public, the added value created by the institution, the results of its professional and high-quality work, and its contribution to the strengthening of democracy. The Office will continue to devote significant attention to providing recommendations, guidelines, and advice, as well as to other public information, awareness-raising, and educational activities that assist in better understanding and implementing the requirements of the legislation regulating the media sector.



LT

VALSTYBINĖ DUOMENŲ APSAUGOS INSPEKCIJA
L. Sapiegos g. 17, 10312 Vilnius
+370 5 271 28 04
ada@ada.lt
https://vdai.lrv.lt/lt/

ŽURNALISTŲ ETIKOS INSPEKTORIAUS TARNYBA
Gedimino pr. 60, 01110 Vilnius
+370 600 81936
zeit@zeit.lt
https://www.zeit.lt/lt

EN

STATE DATA PROTECTION INSPECTORATE
L. Sapiegos St. 17, LT-10312 Vilnius, Lithuania
+370 5 271 28 04
ada@ada.lt
https://vdai.lrv.lt/en/

THE OFFICE OF THE INSPECTOR OF JOURNALIST ETHICS
Gedimino Ave. 60, LT-01110 Vilnius, Lithuania
+370 600 81936
zeit@zeit.lt
https://www.zeit.lt/en