Datu valsts inspekcija

Elijas iela 17, Rīga, LV-1050, tālr. 67223131, e-pasts pasts@dvi.gov.lv, www.dvi.gov.lv

Aizkraukles novada pašvaldībai
(nosūtīšanai e-adreses informācijas sistēmā)

Lēmums

Rīgā, 21.11.2025. Nr. 1-2.3/27-DVI

Par Datu valsts inspekcijas 2025. gada 22. septembra lēmuma Nr. 2-2.2/33 apstrīdēšanu

[1.] Datu valsts inspekcijā (turpmāk – Inspekcija) 2025. gada 21. oktobrī saņemts Aizkraukles novada pašvaldības (turpmāk – Pašvaldība) 2025. gada 20. oktobra apstrīdēšanas iesniegums (reģ. ar Nr. 7-4.2/312-S; turpmāk – apstrīdēšanas iesniegums) par Inspekcijas direktora vietnieces L. Dilbas (turpmāk – amatpersona) 2025. gada 22. septembra lēmumu Nr. 2-2.2/33 "Par korektīvā līdzekļa piemērošanu" (turpmāk – Lēmums). Ar apstrīdēšanas iesniegumu Pašvaldība, pamatojoties uz apstrīdēšanas iesniegumā minētajiem argumentiem, apstrīd un lūdz atcelt Lēmumu.

[2.] Izvērtējot apstrīdēšanas iesniegumā minēto un Inspekcijas rīcībā esošos dokumentus, Inspekcijas direktore

konstatē:

[2.1.] Inspekcijā 2024. gada 12. novembrī saņemts Pašvaldības 2024. gada 12. novembra paziņojums par personas datu aizsardzības pārkāpumu, kuram pievienota sabiedrības ar ierobežotu atbildību "ZZ Dats" reģistrācijas numurs 40003278467, (turpmāk – SIA) 2024. gada 7. novembra vēstule Nr. 1.7/24/228 - N. Minētajos dokumentos sniegta informācija, ka SIA konstatējusi kiberdrošības incidentu Vienotā pašvaldību sistēmā (turpmāk – Sistēma), kas izpaudies tā, ka laika posmā no 2024. gada 29. oktobra līdz 2. novembrim nenoskaidrotām personām bija izdevies no vairākām interneta vietnēm nelikumīgi piekļūt Sistēmas atsevišķām datubāzēm un iegūt šajās datubāzēs glabātos Pašvaldības datus (turpmāk – Pārkāpums).

[2.2.] Inspekcijā 2025. gada 24. janvārī saņemta Pašvaldības 2025. gada 24. janvāra vēstule Nr. 4.9/N/25/237, kurai pievienots Pašvaldības 2025. gada 22. janvāra personas datu aizsardzības pārkāpuma ziņojums Nr.10, kurā sniegta plašāka informācija par SIA Pārkāpumu, kā arī dokumenti, kas pamato ziņojumā sniegto informāciju.

[2.3.] Ar Inspekcijas 2025. gada 29. janvāra vēstuli Nr. 2-4.2/110-N Pašvaldība informēta, ka nolūkā pārbaudīt SIA un pārziņu ieviesto tehnisko un organizatorisko pasākumu atbilstību Vispārīgās

datu aizsardzības regulas[1] (turpmāk - Datu regula) prasībām ir uzsākta personas datu apstrādes pārbaude[2], kuras ietvaros tiek veikti uzraudzības pasākumi paziņojumos minēto notikumu apstākļu noskaidrošanai un vērtēta SIA un pārziņu sniegtā informācija par Pārkāpuma rašanās cēloņiem un rīcību pēc tā konstatēšanas.

[2.4.] Ar Inspekcijas 2025. gada 12. februāra vēstuli Nr. 2-4.2/172-N no Pašvaldības saistībā par Pārkāpumu pieprasīts līdz 2025. gada 28. februārim sniegt viedokli un atbildes uz jautājumiem.

[2.5.] Inspekcijā 2025. gada 28. februārī saņemta Pašvaldības 2025. gada 27. februāra vēstule Nr. 4.1/N/25/580, ar kuru Pašvaldība sniedz atbildes uz Inspekcijas jautājumiem. Pašvaldība vēstulei pievienojusi pielikumus, kas atspoguļo Pašvaldības un SIA sadarbību attiecībā uz Sistēmu un tajā veikto personas datu apstrādi.

[2.6.] Ar Inspekcijas 2025. gada 13. marta ziņojumu Nr. 2-5.1/60 pārbaudes lieta Nr. L-2-6/5863 par personas datu aizsardzības pārkāpumu SIA informācijas Sistēmā tiek sadalīta, uzsākot atsevišķas pārbaudes pret katru no 45 pārziņiem, tostarp Pašvaldību, ņemot vērā katra pārziņa individuālo rīcību un apstrādātāja uzraudzības kārtību.

[2.7.] 2025. gada 13. martā uzsākta pārbaudes lieta Nr. L-2-6/5985 (turpmāk – Lieta) par Pašvaldības rīcības, izmantojot SIA sniegtos Sistēmas uzturēšanas pakalpojumus, atbilstību Datu regulas 5. panta 1. punkta f) apakšpunkta un 2. punkta, 24. panta 1. un 2. punkta, 25. panta 1. punkta, 28. panta 1. punkta, 3. punkta a), c), f) un h) apakšpunkta, 28. panta 9. punkta un 32. panta 1. punkta b) un d) apakšpunkta un 2. punkta prasībām tās veiktajā personas datu apstrādē.

[2.8.] Izvērtējot Lietā esošos dokumentus, ar Inspekcijas amatpersonas 2025. gada 22. septembra Lēmumu nolemts:

1) izteikt Pašvaldībai rājienu;

2) uzlikt par pienākumu Pašvaldībai līdz 2025. gada 28. novembrim:

a) pārskatīt tās iekšējos personas datu apstrādes noteikumus, tostarp izstrādāt Pašvaldības veiktās personas datu apstrādes risku novērtējumu un personas datu aizsardzības pārkāpumu (incidentu) reaģēšanas kārtību;

b) noslēgt ar apstrādātāju SIA atbilstošu datu apstrādes līgumu (noteikumus), tajā jo īpaši iekļaujot visas Datu regulā noteiktās prasības, lai tiktu nodrošināts datu subjektu personas datu aizsardzībai un iespējamiem riskiem atbilstošs drošības līmenis;

3) par šī lēmuma izpildi rakstveidā informēt Inspekciju, līdz 2025. gada 5. decembrim iesniedzot informāciju par veiktajām darbībām.

[2.9.] Inspekcijā 2025. gada 21. oktobrī reģistrēts apstrīdēšanas iesniegums.

[3.] Izvērtējot Inspekcijas rīcībā esošos dokumentus, kā arī konstatētos apstākļus un to juridisko vērtējumu, Inspekcija

secina:

[1] Eiropas Parlamenta un Padomes regulas (ES) 2016/679 par fizisko personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK

[2] Lieta Nr. L-2-6/5863

[3.1.] Saskaņā ar Administratīvā procesa likuma 81. panta pirmo daļu augstāka iestāde izskata lietu vēlreiz pēc būtības kopumā vai tajā daļā, uz kuru attiecas iesniedzēja iebildumi. Administratīvā procesa likuma 81. panta piektajā daļā ir noteikts, ka apstrīdētais administratīvais akts iegūst savu galīgo noformējumu tādā veidā, kādā tas noformēts lēmumā par apstrīdēto administratīvo aktu. Šādā veidā tas ir izpildāms un to var pārsūdzēt tiesā. Administratīvā procesa likuma 76. panta trešajā daļā ir noteikts, ka administratīvā akta apstrīdēšana ir sākotnējās administratīvās lietas turpinājums.

Līdz ar to, Inspekcijas direktore kā augstāka amatpersona, atkārtoti izskata lietu pēc būtības saistībā ar apstrīdēšanas iesniegumā norādītajiem iebildumiem, vērtē un pārbauda, vai amatpersona ir pieņēmusi pamatotu, tiesiski pareizu un Lietas apstākļiem atbilstošu lēmumu.

[3.2.] Saskaņā ar Administratīvā procesa likuma 79. panta pirmo daļu administratīvo aktu var apstrīdēt viena mēneša laikā no tā spēkā stāšanās dienas, bet, ja rakstveida izdotajā administratīvajā aktā nav norādes, kur un kādā termiņā to var apstrīdēt, - viena gada laikā no tā spēkā stāšanās dienas. Ņemot vērā minēto un šā lēmuma [2.8.] un [2.9.] apakšpunktā konstatēto, secināms, ka apstrīdēšanas iesniegums ir iesniegta termiņā, līdz ar to tā izskatīšana ir pieļaujama.

[3.3.] Pašvaldība norāda, ka tai nav tiesību veikt savas pārbaudes vai auditus par Sistēmas drošību, jo šādas darbības esot pretrunā ar Latvijas Republikas normatīvajiem aktiem.

Pašvaldība norāda, ka gan Pašvaldība, gan SIA ir Nacionālā kiberdrošības likuma (turpmāk - Kiberdrošības likums) subjekts. Atbilstoši Kiberdrošības likuma 41. pantam un 44. panta otrajai daļai subjektu uzraudzību veic Nacionālais kiberdrošības centrs vai Satversmes aizsardzības birojs, savukārt ārējo auditu veic neatkarīgs kiberdrošības auditors. Tā kā auditoru saraksts tika apstiprināts tikai 2025. gada 31. jūlijā, Pašvaldībai nebija tiesību veikt subjekta atbilstības auditu (t.sk. savas pārbaudes vai auditus) attiecībā uz SIA uzturēto Sistēmu. Ņemot vērā minēto, Pašvaldība uzskata, ka Lēmumā ietvertais secinājums, norādot, ka Pašvaldība neveic SIA uzraudzību, ir nekorekts.

[3.3.1.] Inspekcijas direktore norāda, ka Pašvaldība kļūdaini pretnostata divus dažādus tiesiskos regulējumus. Kiberdrošības likums ir vērsts uz informācijas un komunikācijas tehnoloģiju un pakalpojumu noturības nodrošināšanu nacionālās drošības ietvarā. Proti, tas regulē sistēmu un pakalpojumu drošību kā tādu. Datu regula savukārt ir vērsta uz fizisku personu pamattiesību - tiesību uz personas datu aizsardzību - nodrošināšanu.

Saskaņā ar Kiberdrošības likumā ietverto informatīvo atsauci uz Eiropas Savienības direktīvām, minētais likums ir izdots, pamatojoties uz NIS2 direktīvu [3], lai izpildītu NIS2 direktīvas prasības un sasniegtu nolūku panākt vienādi augstu kiberdrošības līmeni visā Eiropas Savienībā.

Turpretim Datu regulas 24. pantā, 25. pantā, 28. un 32. pantā ietvertā regulējuma mērķis ir mazināt riskus attiecībā uz fizisku personu tiesībām un brīvībām, kurus rada apstrāde. Tehniskie un organizatoriskie pasākumi tiek īstenoti, lai efektīvi īstenotu datu aizsardzības principus nolūkā aizsargāt datu subjektu tiesības.

[3.3.2.] Kiberdrošības likums un NIS2 direktīva neatceļ, negroza un neierobežo pārziņa pienākumus, kas tam noteikti Datu regulā.

NIS2 direktīvas 14. apsvērumā skaidrots, ka jebkādai personas datu apstrādei saskaņā ar šo direktīvu piemēro Eiropas Savienības datu aizsardzības tiesību aktus un Savienības privātuma tiesību aktus. Konkrētāk, šī direktīva neskar Datu regulu un Eiropas Parlamenta un Padomes Direktīvu 2002/58/EK.

[3.3.3.] Saskaņā ar Kiberdrošības likuma II un VII nodaļu, Inspekcija nav noteikta kā par kiberdrošību atbildīgā institūcija un attiecīgi tā neuzrauga un neizvirza prasības subjektiem saistībā ar

[3] Eiropas Parlamenta un Padomes 2022. gada 14. decembra Direktīvu (ES) 2022/2555, ar ko paredz pasākumus nolūkā panākt vienādi augstu kiberdrošības līmeni visā Savienībā un ar ko groza Regulu (ES) Nr. 910/2014 un Direktīvu (ES) 2018/1972 un atceļ Direktīvu (ES) 2016/1148 (TID 2 direktīva)

kiberdrošības nodrošināšanu. Inspekcija saskaņā ar Datu regulas VI nodaļu un Fizisko personu datu apstrādes likuma (turpmāk – Datu likums) 3. pantu ir personas datu uzraudzības iestāde, kas pilda Datu regulā un Datu likumā noteiktos uzdevumus datu apstrādes jomā. Attiecīgi Inspekcija rīkojas tikai savas kompetences ietvaros un tās rīcība ir vērsta uz to, lai Pašvaldības datu apstrāde atbilstu Datu regulas prasībām.

Lēmumā Inspekcija nav uzdevusi Pašvaldībai veikt ar kiberdrošības prasību ievērošanas kontroli saistītas darbības, tai skaitā nav uzdevusi veikt Kiberdrošības likuma 44. pantā minēto subjektu atbilstības auditu. Inspekcijas secinājumi par pārziņa atbildību atbilstošu tehnisko un organizatorisko pasākumu nodrošināšanā un attiecībā uz SIA kā apstrādātāja nepietiekamu uzraudzību no Pašvaldības kā pārziņa puses, ir izdarīti analizējot Datu regulas 24. panta, 25. panta 1. punkta, 28. un 32. panta prasības un amatpersonas secinājumi ir Lietas apstākļiem atbilstoši.

Ņemot vērā minēto, Pašvaldība nepamatoti savā iebildumā ir atsaukusies uz Kiberdrošības likuma 41. pantu, 44. panta otro daļu un Ministru kabineta noteikumiem, kas nosaka kiberdrošības auditoram izvirzāmās prasības un kiberdrošības auditoru reģistrācijas kārtību, kā arī norādījusi uz to, ka Inspekcija ir nekorekti norādījusi, ka Pašvaldība neveic SIA uzraudzību.

[3.4.] Pašvaldība atsaucas uz CERT.lv un Nacionālais kiberdrošības centra atbildēm, kurās sniegti ieteikumi un skaidrojumi par atsevišķām Kiberdrošības likuma prasībām.

Inspekcijas direktore norāda, ka tehniskie un organizatoriskie pasākumi, ko paredz Datu regula, nav pielīdzināmi Kiberdrošības likumā paredzētajam nacionālās drošības auditam vai citiem kiberdrošības pasākumiem. Inspekcija no Pašvaldības nesagaida, piemēram, pilnvērtīgu ielaušanās testu veikšanu, bet gan sagaida, ka Pašvaldība kā pārzinis veiks tos pienākumus, ko tai paredz Datu regula, piemēram, pieprasīs un izvērtēs SIA datu aizsardzības politikas, pieprasīs pierādījumus par ieviestajām tehniskajiem un organizatoriskajiem pasākumiem un veiks citas darbības specifiski par personas datu aizsardzību.

CERT.lv un Nacionālajam kiberdrošības centram Datu regulā nav noteikta kompetence un tas nevar sniegt ieteikumus vai skaidrojumus Pašvaldībai par apstrādātāja uzraudzību saskaņā ar Datu regulas prasībām. Ņemot vērā minēto, Pašvaldības atsauce uz minētajām vēstulēm nav pamatota.

[3.5.] Pašvaldība norāda, ka Lēmumā ietvertais secinājums par to, ka starp Pašvaldību un SIA nav noslēgts personu datu apstrādes līgums ir tikai daļēji pamatots, jo vispārīgā vienošanās Nr. VRAAEIS/2019/17/AK/CI-118PG (turpmāk – Vienošanās), kas noslēgta starp Valsts reģionālās attīstības aģentūru un SIA, paredz pienākumu SIA nodrošināt Valsts reģionālās attīstības aģentūras prasības attiecībā uz informāciju sistēmu (t.sk. Sistēmas) prasībām datu aizsardzībā un informācijas sistēmu drošībā, kā arī nosaka līgumsodus un citas uz Pretendentu attiecināmās prasības. Pašvaldības noslēgtās vienošanās ar SIA par Sistēmas izmantošanu ietvaros tika piemēroti "VPS uzturēšanas noteikumi 2024" (turpmāk – Noteikumi). Noteikumi ietver atsauci uz 44. punktu, kas nosaka, ka Izpildītājs nodrošina personu datu apstrādi atbilstoši normatīvajiem aktiem, tai skaitā, Datu regulai, kā arī šie noteikumi ietver arī citus pienākumus apstrādātājam, ievērojot Datu regulas nosacījumus. Savukārt 45. punkts nosaka, ka Izpildītājs, tiklīdz tam kļuvis zināms personas datu aizsardzības pārkāpums, nekavējoties ziņo Klientam, ievērojot, ka Klientam atbilstoši Datu regulai no incidenta konstatēšanas brīža ir jāziņo 72 stundu laikā.

Inspekcijas direktore secina, ka Lēmuma pieņemšanas ietvaros amatpersona ir izvērtējusi norādīto dokumentu saturu, tai skaitā apstrīdēšanas iesniegumam pievienotos Noteikumus, un Lēmuma [3.6] apakšpunktā secinājusi, ka starp Pašvaldību un SIA nav noslēgts personas datu apstrādes līgums. Lai gan atsevišķi noteikumi ir minēti Vienošanās un Noteikumos, tie ir pārāk vispārīgi.

Datu regulas 28. panta 3. punktā ir noteikti minimālie nosacījumi, ko līgumam vai citam

juridiskam aktam starp pārzini un apstrādātāju būtu jāietver, tostarp līguma priekšmetu, apstrādes raksturu un nolūku, personas datu veidu un norādi, ka apstrādātājs īsteno visus pasākumus, kas nepieciešami saskaņā ar Datu regulas 32. pantu. Ņemot vērā, ka Pašvaldības norādītie dokumenti neparedz minētās prasības, Lēmumā pamatoti secināts, ka starp Pašvaldību un apstrādātāju nav noslēgts personas datu apstrādes līgums.

Papildus minētajam secināms, ka Pašvaldība 2025. gada 22. janvāra personas datu aizsardzības pārkāpuma ziņojumā Nr.10 norādīja ka, slēdzot jauno vienošanos ar SIA par Sistēmas lietošanu 2025. gadā, nepieciešams noslēgt arī personas datu apstrādes līgumu, tajā iekļaujot papildus prasības attiecībā uz datu aizsardzību, t.sk. izvērtēt iespējas noteikt līgumsodus, ja šādas prasības netiek izpildītas vai tiek izpildītas ar kavēšanos (piemēram, gadījumos, kad informācija par notikušo datu aizsardzības pārkāpumu tiek sniegta novēloti). Minētais fakts ir tiešs apliecinājums tam, ka spēkā esošajās vienošanās ietvertās normas nebija atbilstošas vai pietiekamas.

Vienlaikus norādāms, ka korektīvais līdzeklis - rājiens - Pašvaldībai piemērots par pārkāpumu, kas jau ir noticis un radījis datu noplūdi. Rīcība pēc faktiskā notikuma nemaina pagātnē izdarīto pārkāpumu.

Ņemot vērā minēto, secināms, ka Lēmuma [3.6] apakšpunktā informācija ir norādīta atbilstoši Lietas apstākļiem un Pašvaldības arguments atzīstams par nepamatotu.

Ņemot vērā minētos faktiskos un tiesiskos apstākļus, pamatojoties uz Datu regulas 24. pantu, 25. pantu, 28. pantu, 32. pantu un VI nodaļu, Datu likuma 3. pantu, Kiberdrošības likuma II nodaļu, VII nodaļu un 44. pantu, NIS2 direktīvas 14. apsvērumu, Administratīvā procesa likuma 76. panta trešo daļu, 79. panta pirmo daļu, 81. panta pirmo, otro un piekto daļu, Inspekcijas direktore

nolemj:

– atstāt negrozītu Datu valsts inspekcijas 2025. gada 22. septembra lēmumu Nr. 2-2.2/33.

Saskaņā ar Administratīvā procesa likuma 70. panta pirmo un otro daļu lēmums stājas spēkā ar brīdi, kad tas paziņots adresātam, savukārt lēmumu paziņo adresātam atbilstoši Paziņošanas likumam. Paziņošanas likuma 9. panta 1^1 daļā noteikts, ka dokuments, kas nosūtīts uz oficiālo elektronisko adresi, uzskatāms par paziņotu otrajā darba dienā pēc tā nosūtīšanas.

Šo lēmumu saskaņā ar Administratīvā procesa likuma 188. pantu un 189. panta pirmo daļu un Fizisko personu datu apstrādes likuma 24. panta otro daļu un Tieslietu padomes 2025. gada 24. jūlija lēmumu Nr. 48 “Par tiesām, to darbības teritorijām un atrašanās vietām” var pārsūdzēt viena mēneša laikā no tā spēkā stāšanās dienas Administratīvās rajona tiesas attiecīgajā tiesu namā pēc pieteicēja adreses [fiziskā persona — pēc deklarētās dzīvesvietas adreses, papildu adreses (Dzīvesvietas deklarēšanas likuma izpratnē) vai nekustamā īpašuma atrašanās vietas, juridiskā persona — pēc juridiskās adreses].

Direktore J.Macuka

[..]