



Datu valsts inspekcija

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

Lieta Nr. L-2-6/5982

Siguldas novada pašvaldībai
eAdrese

Lēmums

Rīgā, 22.09.2025.

Nr. 2-2.2/66

Par korektīvā līdzekļa piemērošanu

[1] Datu valsts inspekcijas (turpmāk – Inspekcija) rīcībā nonāca informācija par notikušo personas datu aizsardzības pārkāpumu (turpmāk – Pārkāpums), kā rezultātā laika posmā no 2024. gada 29. oktobra līdz 2. novembrim nenoskaidrotām personām izdevās no vairākām interneta vietnēm nelikumīgi piekļūt Sabiedrības ar ierobežotu atbildību “ZZ Dats”, vienotais reģistrācijas Nr. 40003278467 (turpmāk – ZZ Dats), informācijas sistēmas atsevišķām datubāzēm un iegūt šajās datubāzēs glabātos fizisko personu personas datus (vārds, uzvārds, personas kods un deklarētā dzīvesvietas adrese), kopskaitā vairāk nekā 25 miljoniem ierakstu, tostarp par Siguldas novada pašvaldībā (turpmāk – Pašvaldība) deklarētajām fiziskajām personām.

[1.1] Saistībā ar notikušo Pārkāpumu Inspekcija saņēma Pašvaldības 2024. gada 8. novembra paziņojumu¹ (turpmāk – Sākotnējais paziņojums), kurā tika norādīts, ka Pašvaldība konstatēja Pārkāpumu 2024. gada 7. novembrī, saņemot vēstuli no ZZ Dats, kurā ZZ Dats informēja Pašvaldību par konstatēto kiberdrošības incidentu Vienotā pašvaldību sistēmā (turpmāk – VPS). Paziņojumam tika pievienota informācija par Pārkāpumā ietekmētajiem iedzīvotāju datu kategorijām.

Inspekcija saņēma Pašvaldības 2024. gada 14. novembra² un 2024. gada 5. decembra³ papildu paziņojumus (turpmāk kopā – Papildu paziņojums), kurā sniegta plašāka informācija par Pārkāpumu. Norādīts, ka ugunsmūra konfigurācijas atjaunošanas kļūdas dēļ, vairākas dienas daļa datu, kas atrodas meklēšanas indeksā bija pieejami bez autorizācijas. Pārkāpumā skarti visu pašvaldību attiecīgie dati un metadati sistēmā. Sistēmā glabāto dokumentu datnes Pārkāpuma nav skartas un nav nelikumīgi iegūtas. 2024. gada 2. novembrī incidents tika novērsts, atjaunota VPS drošība un tiek turpināta incidenta seku analīze, kā arī uzskaitīti datu veidi un skaits, kas tika skarti incidentā, precizējot, ka datu integritāte nav cietusi. Pašvaldība norāda, ka tai ir noslēgts līgums ar ZZ Dats kā apstrādātāju par informācijas sistēmu pakalpojumu izmantošanu, apstrādātājam ieviesta IDS sistēma Security Onion, apstrādātāja Informācijas drošības un kvalitātes vadības sistēmu sertificēta atbilstoši standartiem ISO/IEC 27001:2022, ISO 9001:2015. Uzskaitīti Pašvaldības veikti pasākumi pārkāpuma

¹ Inspekcijā saņemts un reģistrēts 2024. gada 8. novembrī ar Nr. 2-5.2/119

² Inspekcijā saņemts un reģistrēts 2024. gada 14. novembrī ar Nr. 2-5.2/157

³ Inspekcijā saņemts 2024. gada 5. decembrī un reģistrēts 2024. gada 6. decembrī ar Nr. 2-5.2/178

ietekmes mazināšanai, tostarp sabiedrības (datu subjektu) informēšanas pasākumi, kā arī iesniegta papildu dokumentācija par Pārkāpumu⁴.

[1.2] Nolūkā pārliecināties par Pašvaldības veikto darbību tiesiskumu, apstrādājot tās iedzīvotāju personas datus, Inspekcija saskaņā ar Fizisko personu datu apstrādes likuma (turpmāk – Datu likums) 5. panta pirmās daļas 3. punktu un Vispārīgās datu aizsardzības regulas⁵ (turpmāk – Datu regula) 58. panta 1. punkta e) apakšpunktu 2025. gada 12. februārī aicināja Pašvaldību sniegt papildu informāciju⁶: par ZZ Dats kā apstrādātāja izvēli, par personas datu apstrādes līguma noslēgšanu, par ZZ Dats kā apstrādātāja uzraudzību, t.sk., vai ir izstrādāti apstrādātāja uzraudzības noteikumi, par ZZ Dats kā apstrādātāja risku analīzi, kādā veidā ZZ Dats informē Pašvaldību par izmaiņām ZZ Dats īstenotajos tehniskajos un organizatoriskajos pasākumos pārziņu personas datu apstrādē, par kārtību, kādā ZZ Dats informē Pašvaldību par notikušiem personas datu aizsardzības pārkāpumiem, kā arī aicināja Pašvaldību iesniegt ziņojumu par Pārkāpuma izmeklēšanu.

[1.3] Pašvaldība 2025. gada 28. februāra atbildes vēstulē Nr. 123-1-7/6⁷ un tās 2025. gada 13. marta papildinājumos⁸ (turpmāk viss kopā – Atbildes vēstule) sniedza turpmāk norādīto informāciju uz Inspekcijas jautājumiem.

[1.3.1] Attiecībā uz ZZ Dats kā apstrādātāja izvēli, Pašvaldība paskaidroja, ka ZZ Dats ir vienīgais pakalpojumu sniedzējs, kurš var nodrošināt visu funkciju izpildi VPS. Neraugoties uz to, ka ir atsevišķi uzņēmumi, kas var piedāvāt individuālus risinājumus (piemēram, lietvedības un grāmatvedības uzskaites programmas), tomēr to integrācija ir sarežģīta, tehniski komplicēta un ekonomiski nepamatota. Pašvaldības rīcībā nav resursu izveidot analoģu sistēmu no tirgū pieejamajiem dažādu izstrādātāju produktiem.

[1.3.2] Attiecībā uz personas datu apstrādes līguma noslēgšanu, Pašvaldība paskaidroja, ka Pārkāpuma brīdī starp Pašvaldību un ZZ Dats bija spēkā 2024. gadā noslēgtā Vienošanās pie darījuma Nr. SIGND/2024/70 par VPS uzturēšanas pakalpojumu sniegšanu.

Saskaņā ar Vienošanos pakalpojuma sniegšanas ietvaros abas puses ievēro VPS uzturēšanas Noteikumus⁹, kuros ir skaidri definēti drošības un integritātes nosacījumi attiecībā uz VPS uzturēšanu, kā arī noteikti Pašvaldības un ZZ Dats pienākumi un tiesības personas datu apstrādes kontekstā. Noteikumu 44. punktā ir īpaši uzsvērts, ka ZZ Dats apņemas nodrošināt personas datu apstrādi atbilstoši spēkā esošajiem normatīvajiem aktiem, t.sk. Datu regulas prasībām.

Papildus paskaidrots, ka Pašvaldība no savas puses ir piedāvājusi pilnveidot vienošanās formu un datu apstrādes noteikumus, taču vienošanās ar ZZ Dats netika panākta. Uz Atbildes vēstules sagatavošanas dienu ir uzsākta Personas datu apstrādes līguma iniciatīva un līguma projekts ir saskaņošanas procesā.

Datu regula nenosaka obligātu prasību slēgt atsevišķu līgumu *par datu apstrādi*, bet vienmēr var pastāvēt sadarbības pilnveidošanas iespējas.

[1.3.3] Attiecībā uz ZZ Dats kā apstrādātāja uzraudzību, t.sk., vai ir izstrādāti apstrādātāja uzraudzības noteikumi, Pašvaldība paskaidro, ka ir sūtījusi ZZ Dats vēstules, uzdodot jautājumus par tehnisko un organizatorisko pasākumu ieviešanu un pilnveidošanu.

⁴ ZZ dats vēstule Nr. 1.7/24/302-N *Papildu informācija par kiberdrošības incidentu* ar pielikumiem

⁵ Eiropas Parlamenta un Padomes regula (ES) Nr. 2016/679 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK.

⁶ Inspekcijas 2025. gada 12. februāra vēstule Nr. 2-4.2/172-N *Par pārbaudes uzsākšanu un informācijas pieprasījumu*.

⁷ Inspekcijā saņemta 2025. gada 28. februārī un reģistrēta 2025. gada 3. martā ar Nr. 2-4.2/313-S.

⁸ Inspekcija saņemti un reģistrēti 2025. gada 13. martā ar Nr. 2-4.2/383-S

⁹ <https://www.zzdats.lv/vps-uzturedzanas-noteikumi>

Kopš 2010. gada ZZ Dats ir iegūts kvalitātes vadības sistēmas sertifikāts ISO/IEC 27001 informācijas drošības pārvaldības standartam, kas paredz ikgadējus neatkarīgus auditus, drošības politikas un procedūru ievērošanu (saskaņā ar Datu regulas 42. panta prasībām par sertifikāciju). Vienlaikus Pašvaldība informēja, ka ZZ Dats ir ieviesusi kvalitātes vadības sistēmas sertifikātu ISO 9001:2015, kas nodrošina pakalpojumu atbilstību industrijas labākajai praksei. Līdz šim ZZ Dats kā apstrādātāja darbībā nav konstatēti datu aizsardzības pārkāpumi, kā arī ISO auditu rezultāti un iekšējās kontroles mehānismi liecina, ka ZZ Dats nodrošina Datu regulas prasību ievērošanu.

Pašvaldība norāda, ka, lai gan atsevišķi personas datu apstrādātāja uzraudzības noteikumi nav izstrādāti, jo Datu regula šādu pienākumu tiešā veidā nenosaka, Pašvaldība izvērtēs šādu noteikumu izstrādi un ieviešanu. Līdzšinējā uzraudzība balstījās uz ZZ Dats sniegto publiski pieejamo (t.i. Noteikumos un Datu apstrādes politikā) norādīto informāciju, kā arī atsevišķiem uzdotiem jautājumiem no Pašvaldības puses par organizatorisko un tehnoloģisko pasākumu ieviešanu. Šāda pieeja balstīta arī uz to, ka ZZ Dats ir monopolstāvoklis šāda veida pakalpojuma sniegšanai pašvaldībām un tirgū nav citas alternatīvas, lai nodrošinātu pašvaldības funkciju izpildi. Pašvaldība tiesiski paļaujas, ka šīs garantijas un starptautiskos standartus apstrādātājs ievēro, tāpat to apliecina arī ZZ Dats veiktie regulārie auditi. Pašvaldībām nav izveidotas piekļuves ZZ Dats informācijas sistēmām, lai tehniski pārraudzītu ieviesto tehnisko un organizatorisko pasākumu atbilstību.

[1.3.4] Attiecībā uz ZZ Dats kā apstrādātāja risku analīzi, Pašvaldība informēja, ka ir veikusi ZZ Dats VPS sistēmas izmantošanas risku analīzi.

[1.3.5] Attiecībā uz to, kā ZZ Dats informē Pašvaldību par izmaiņām ZZ Dats īstenotajos tehniskajos un organizatoriskajos pasākumos pārziņu personas datu apstrādē, Pašvaldība paskaidroja, ka saskaņā ar Noteikumu 23. punktu ZZ Dats informē Pašvaldību par plānotajām izmaiņām VPS darbībā: par plānotajām būtiskajām izmaiņām VPS funkcionalitātē Pašvaldība tiek informēta ne vēlāk kā piecas darba dienas iepriekš. Gadījumā, ja ir izlaista jauna programmatūras versija, informācija par to tiek nosūtīta elektroniskajā pastā. Savukārt, ja ir nepieciešamas datu apmaiņas risinājuma izmaiņas, par to tiek sagatavota oficiāla vēstule, uz kuras pamata EIS tiek veikts pirkums ar precīzu darba uzdevumu.

[1.3.6] Attiecībā uz kārtību, kādā ZZ Dats informē Pašvaldību par notikušiem personas datu aizsardzības pārkāpumiem, Pašvaldība paskaidroja, ka šī kārtība ir noteikta Noteikumu 45. punktā. Saskaņā ar minēto punktu, līdz ko ZZ Dats ir kļuvis zināms par notikušo personas datu aizsardzības pārkāpumu, ZZ Dats ir pienākums nekavējoties informēt par to Pārziņa atbildīgo personu. Šī informēšana tiek veikta, ievērojot Datu regulas 33. panta 2. punktā¹⁰ noteiktās prasības.

[1.3.7] Attiecībā uz Pašvaldības ziņojuma par Pārkāpuma izmeklēšanu iesniegšanu, Pašvaldība norādīja, ka iesniedz Inspekcijai vadības ziņojumu par veiktajām darbībām.

[1.3.8] Atbildes vēstules pielikumā Pašvaldība iesniedza šādus dokumentāros pierādījumus un materiālus, kas pamato tās sniegtās atbildes uz Inspekcijas jautājumiem: 1) 2024. gada 21. februāra Vienošanās pie EIS darījuma Nr. SIGND/2024/70; 2) 2024. gada 22. novembra Pašvaldības vēstule Nr. 123-1-7/5; 3) Pašvaldības 2025. gada 27. februāra Riska novērtējums par VPS izmantošanu; 4) ZZ Dats 2024. gada 15. novembra vēstule Nr. 1.7/24/248-N; 5) 2024. gada 29. novembra ziņojums par ZZ Dats kiberdrošības incidentu un veiktajām darbībām; 6) ZZ Dats 2025. gada 25. februāra vēstule Nr. 1.7/25/174-N Par ZZ Dats veiktajiem auditiem un sertifikāciju, ar pielikumiem.

¹⁰ Apstrādātājs, tiklīdz tam kļuvis zināms personas datu aizsardzības pārkāpums, bez nepamatotas kavēšanās paziņo par to pārzinim

[1.3.9] Ar Inspekcijas amatpersonas lēmumu¹¹ Inspekcijas pārbaudes lietā Nr. L-2-6/5930 konstatēts, ka Pārkaupuma cēlonis bija ZZ Dats darbinieka pieļauta kļūda ugunssmūra konfigurācijas izmaiņu ieviešanā, kā rezultātā ugunssmūra noteikumi ļāva trešajām personām nesankcionēti piekļūt VPS esošiem personas datiem. Inspekcija secināja, ka ZZ Dats pirms Pārkaupuma nebija ieviesis Datu regulas 32. panta 1. punkta b) un d) apakšpunkta un 2. panta prasībām atbilstošus tehniskos un organizatoriskos pasākumus, kas cita starpā nodrošinātu VPS nepārtrauktu konfidencialitāti, integritāti, pieejamību un noturību, jo, ja tādi būtu ieviesti un praksē darbotos, tad arī darbinieka pieļautas kļūdas gadījumā, atbilstošs kontroles pasākums nodrošinātu šīs kļūdas “vadīšanu” jeb kontroli un tā tiktu savlaicīgi novērsta, nepieļaujot Pārkaupuma iestāšanos vai mazinot tā iestāšanās risku.

[2] Pamatojoties uz Inspekcijas rīcībā esošo informāciju, Inspekcija saskaņā ar Datu regulas 57. panta 1. punkta a) un h) apakšpunktu un Datu likuma 5. panta pirmās daļas 1. punktu 2025. gada 13. martā uzsāka pārbaudi par Pašvaldības rīcības, izmantojot ZZ Dats sniegtos VPS 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 (turpmāk – Lieta).

Inspekcija konstatē, ka Pašvaldības Sākotnējā un Papildu paziņojumā un Atbildes vēstulē sniegtā informācija satur visu pieprasīto informāciju un materiālus, lai izskatītu Lietu pēc būtības, un nav nepieciešams iegūt citus papildu paskaidrojumus vai pierādījumus no Pašvaldības.

[3] Pamatojoties uz Lietas materiālos esošo informāciju, Inspekcija konstatē un norāda turpmāko.

[3.1] Saskaņā ar Datu regulas 4. panta 7) apakšpunktu par personas datu apstrādes atbilstību tiesiskā regulējuma prasībām ir atbildīgs pārzinis¹². Konkrētajā gadījumā Inspekcija konstatē, ka attiecībā uz Pašvaldībā deklarēto iedzīvotāju veikto personas datu apstrādi VPS Pašvaldība ir uzskatāma par pārzini, savukārt ZZ Dats atbilstoši Datu regulas 4. panta 8) apakšpunktam ir uzskatāma par apstrādātāju¹³. Līdz ar to Pašvaldībai kā personas datu apstrādes pārzinim ir jānodrošina Datu regulas prasību ievērošana, tostarp attiecībās ar izvēlēto apstrādātāju.

[3.2] Datu regulas 5. panta 2. punktā noteiktais pārskatatbildības princips nosaka, ka tieši pārzinim ir pienākums nodrošināt tādu personas datu apstrādes procesu, kas ļauj pierādīt, ka viņa veiktā personas datu apstrāde ir atbilstoša datu aizsardzības tiesiskā regulējuma prasībām. Proti, pārziņa pienākums ir pierādīt tā veiktās apstrādes tiesiskumu, piemēram, vai ir pieņemti iekšējie datu apstrādes noteikumi un vai līgumos ar apstrādē iesaistītajām pusēm ir iekļautas nepieciešamās normas par personas datu apstrādi, t.sk. pienākumu un lomu sadalīšanu, kontroles mehānismiem.

Tādējādi pārzinim ir pienākums iesniegt Inspekcijai visu tā rīcībā esošo informāciju (t.sk. dokumentāciju vai citus materiālus pierādījumus), kas ļauj pārliecināties par veiktās apstrādes tiesiskumu un prasību ievērošanu. Inspekcija konstatē, ka Pašvaldība ir iesniegusi tās rīcībā esošo dokumentāciju saistībā ar tās veikto personas datu apstrādi VPS, notikušo Pārkaupumu un kā Pašvaldība pārliecinās par apstrādātāja ieviesto tehnisko un organizatorisko pasākumu un kontroļu atbilstību. Tikai izvērtējot šos dokumentus, Inspekcija var izdarīt secinājumus par to, vai Pašvaldība ir spējusi nodrošināt tādu procesu, kas pierāda Pašvaldības veiktās personas datu apstrādes atbilstību

¹¹ Inspekcijas 2025. gada 23. jūlija lēmums Nr. 01630000100325-3

¹² Fiziska vai juridiska persona, publiska iestāde, aģentūra vai cita struktūra, kas viena pati vai kopīgi ar citām nosaka personas datu apstrādes nolūkus un līdzekļus.

¹³ Apstrādātāja atbildība un prasības jo īpaši noteiktas Datu regulas 28. pantā, kas cita starpā paredz arī pārziņa pienākumus attiecībās ar apstrādātāju.

tiesiskajam regulējumam, tostarp Datu regulas 5. panta 1. un 2. punktā minētajiem principiem.

[3.3] Savukārt Datu regulas 5. panta 1. punkts nosaka personas datu apstrādes pamatprincipus, kas ikvienam pārzinim jāievēro. Jo īpaši Datu regulas 5. panta 1. punkta f) apakšpunkts paredz, ka pārzinim ir pienākums personas datus apstrādāt tādā veidā, lai tiktu nodrošināta atbilstoša personas datu drošība, tostarp aizsardzība pret neatļautu vai nelikumīgu apstrādi un pret nejaušu nozaudēšanu, iznīcināšanu vai sabojāšanu, izmantojot atbilstošus tehniskos vai organizatoriskos pasākumus. Lai gan šis princips ir ietverts arī vairākos citos Datu regulas pantos un apsvērumos, to konkretizējot, no tā nepārprotami izriet pārziņa vispārīgā atbildība apstrādājamo personas datu drošības nodrošināšanā, ieviešot un izmantojot nepieciešamus tehniskos vai organizatoriskos pasākumus, neatkarīgi no apstrādātājam vai citām apstrādē iesaistītajām pusēm uzliktajiem tiesiskajiem pienākumiem.

Ievērojot minēto, Inspekcija, izvērtējot visu tās rīcībā esošo informāciju, konstatē, ka Pārskatītāja rezultātā nepiederošām trešajām personām izdevās piekļūt VPS glabātajiem personas datiem, tostarp par Pašvaldībā deklarētajiem iedzīvotājiem. Līdz ar to secināms, ka konkrētajā gadījumā faktiski netika nodrošināta personas datu drošība saskaņā ar Datu regulas 5. panta 1. punkta f) apakšpunktu, par kuras īstenošanu atbildīgs ir arī pārzinis (Pašvaldība), nevis tikai konkrētajām apstrādes darbībām izvēlētais apstrādātājs vai sistēmas uzturētājs. Savukārt attiecībā uz pārziņa atbildības līmeni saistībā ar Pārskatītāju un tā apstākļiem norādāms, ka atbilstoši Datu regulas 5. panta 2. punktā minētajam pārskatatbildības principam pārzinim ir pienākums parādīt, ka viņa rīcība ir bijusi atbilstoša tiesiskajam regulējumam un viņš ir izpildījis visas Datu regulas prasības.

[3.4] Datu regulas 24. panta 1. punkts nosaka, ka, ņemot vērā apstrādes raksturu, apmēru, kontekstu un nolūkus, kā arī dažādas iespējamības un nopietnības pakāpes riskus attiecībā uz fizisku personu tiesībām un brīvībām, pārzinim ir pienākums īstenot atbilstošus tehniskus un organizatoriskus pasākumus, lai nodrošinātu un spētu uzskatāmi parādīt, ka apstrāde notiek saskaņā ar Datu regulu. Ja nepieciešams, minētos pasākumus pārskata un atjaunina. Šā panta 2. punkts skaidro, ka gadījumos, kad tas ir samērīgi attiecībā uz apstrādes darbībām, šajos pasākumos jāietver tas, ka pārzinis īsteno atbilstīgu politiku attiecībā uz datu aizsardzību.

Tādējādi Datu regulas 24. panta 1. punkts kopsakarā ar Datu regulas 5. panta 2. punktā noteikto pārskatatbildības principu konkrēti nosaka pārziņa pienākumu nodrošināt, ka personas datu apstrāde notiek saskaņā ar Datu regulu. No minētā izriet, ka Pašvaldība nevar atsaukties, piemēram, uz tiesiskās palāvības principu¹⁴, kas minēts Administratīvā procesa likuma (turpmāk – APL) 10. pantā, jo, pirmkārt, Pašvaldība nav uzskatāma par privātpersonu¹⁵ un, otrkārt, Pašvaldībai kā pārzinim ir pašai jānodrošina konkrētajai datu apstrādei piemērota un Datu regulas prasībām atbilstoša izpilde, nevis jāpaļaujas, ka šo prasību īstenošanu nodrošinās un regulāri pārbaudīs citas iestādes (piemēram, ISO sertifikācijas iestāde vai komisija, kas ievieto iepirkumu EIS). Inspekcija vērš uzmanību, ka ikviena iestāde darbojas tikai tai noteiktās kompetences un pilnvaru ietvaros, savukārt par personas datu aizsardzības prasību ievērošanu un īstenošanu atbildīgs ir tieši pārzinis, nevis citas sertifikācijas vai uzraugošās iestādes. Attiecīgi Inspekcija vērtē tieši Pašvaldības kā personas datu pārziņa rīcību un atbildības līmeni, nevis citu iestāžu kompetenci saistībā ar notikušo Pārskatītāju.

Saskaņā ar Pašvaldības iesniegto informāciju, Inspekcija konstatē, ka Pašvaldība ir veikusi esošās situācijas analīzi un uzskata, ka tā ir veikusi samērīgas un adekvātas darbības attiecībā uz

¹⁴ APL 10. pants paredz, ka privātpersona var paļauties, ka iestādes rīcība ir tiesiska un konsekventa. Tiesiskās palāvības princips aizsargā tikai tādas tiesības, uz kuru īstenošanu personai varēja rasties likumīga, pamatota un saprātīga palāvība, kas ir minēta vispārējā tiesību principa kodols. Skat. Satversmes tiesas 2020. gada 11. decembra sprieduma lietā Nr. 2020-26-0106 10.2. punktu un Satversmes tiesas 2021. gada 5. marta sprieduma lietā Nr. 2020-30-01 11.2. punktu.

¹⁵ Saskaņā ar APL 1. panta astoto daļu privātpersona ir fiziskā persona, privāto tiesību juridiskā persona vai šādu personu apvienība

apstrādātājam noteiktajām prasībām, pienākumiem, atbildību un pārraudzību, pamatā paļaujoties uz ZZ Dats kā sistēmas uzturētāja atbildību visām tiesiskā regulējuma prasībām saskaņā ar noslēgto līgumu, Vienošanos, Noteikumiem un ZZ Dats sertifikāciju.

Ievērojot minēto, izvērtējot visu tās rīcībā esošo informāciju, Inspekcija secina, ka attiecībā uz veikto personas datu apstrādi VPS infrastruktūrā noslēgtā līguma un Vienošanās ietvaros Pašvaldība nebija nodrošinājusi sev jebkādas patiesas iespējas veikt šīs sistēmas drošības pārbaudi un apstrādātāja ZZ Dats rīcības kontroli, lai savlaicīgi un regulāri pārliecinātos par Datu regulas prasību ievērošanu. Tādējādi secināms, ka Pašvaldība no savas puses nav veikusi nepieciešamos tehniskos un organizatoriskos pasākumus (piemēram, pirms personas datu apstrādes sākšanas vienojusies ar apstrādātāju par incidentu ziņošanas nepieciešamību, būtiskas informācijas apmaiņu saistībā ar personas datu apstrādes jautājumiem, lomu vai atbildības sadali u.c.), lai uzskatāmi parādītu, ka datu apstrāde notiek saskaņā ar Datu regulu, piemēram, apstrādātāja pārvaldīšana un apstrādes monitorēšana un drošības testēšana, datu apstrādes līguma noslēgšana, tādējādi pārkāpjot Datu regulas 24. panta 1. punktu.

[3.5] Saskaņā ar Datu regulas 25. panta 1. punktu, ņemot vērā tehnikas līmeni, īstenošanas izmaksas un apstrādes raksturu, apmēru, kontekstu un nolūkus, kā arī dažādas iespējamības un nopietnības pakāpes riskus attiecībā uz fizisku personu tiesībām un brīvībām, kurus rada apstrāde, pārzinim gan apstrādes līdzekļu noteikšanas, gan pašas apstrādes laikā ir pienākums īstenot atbilstošus tehniskus un organizatoriskus pasākumus, piemēram, pseidonimizāciju, kas ir paredzēti, lai efektīvi īstenotu datu aizsardzības principus, piemēram, datu minimizēšanu, un lai apstrādē integrētu vajadzīgās garantijas nolūkā izpildīt šīs regulas prasības un aizsargāt datu subjektu tiesības.

Pamatojoties uz Inspekcijas rīcībā esošo informāciju, konstatējams, ka Pašvaldība neveic ZZ Dats uzraudzību, bet gan paļaujas uz Noteikumos paredzētajām klauzulām, ZZ Dats izsniegtajiem un uzturētajiem ISO sertifikātiem, kā arī Pašvaldība atzīst, ka nav izveidotas piekļuves ZZ Dats informācijas sistēmām, lai tehniski pārraudzītu ieviesto tehnisko un organizatorisko pasākumu atbilstību.

Šajā ziņā Inspekcija norāda, ka tās ieskatā konkrētās datu apstrādes ietvaros nebūtu saprātīgi sagaidīt, ka ZZ Dats sniedz Pašvaldībai detalizētus paziņojumus par visiem tehniskajiem procesiem un uzlabojumiem, kas tiek veikti VPS infrastruktūrā, tomēr Pašvaldībai, ņemot vērā dažādas iespējamības un nopietnības pakāpes riskus datu subjektu tiesībām un brīvībām, būtu jābūt iespējai – vismaz pēc Pašvaldības pamatota pieprasījuma – saņemt pamatinformāciju par sistēmas uzturēto drošības līmeni vai līgumā atrunātos gadījumos, kad tiek veiktas nozīmīgas tehniskas izmaiņas, tos iepriekš savstarpēji saskaņot. Proti, Pašvaldības paļaušanās vien uz faktu, ka apstrādātājam ZZ Dats ir spēkā esoši ISO sertifikāti un ikgadēji veikti sistēmas drošības auditi, bez jebkādas iespējas Pašvaldībai piedalīties procesos, tos vajadzības gadījumā savstarpēji saskaņojot, nav atzīstams par pietiekamu, lai nodrošinātu Pašvaldības kā pārziņa rīcības atbildību Datu regulas prasībām. Tādējādi Inspekcija secina, ka Pašvaldība ZZ Dats uzraudzībā nenodrošina Datu regulas 25. panta 1. punkta prasības. Proti, ZZ Dats, apstrādājot Pašvaldības nodotos personas datus, ir rīkojusies patstāvīgi bez pārziņa iesaistes, ne tikai par apstrādes tehniskajiem aspektiem neinformējot pārziņi, bet arī savstarpēji nevienojoties par nepieciešamo rīcību un ieviešamajiem pasākumiem personas datu integritātes nodrošināšanai no apstrādātāja vai pārziņa puses, kā rezultātā Pašvaldība sev kā pārziņim nav nodrošinājusi patiesas kontroles iespējas par tās teritorijā deklarēto personu datu drošību.

[3.6] Datu regulas 28. pants noteic prasības attiecībā uz apstrādātāju. Proti, 28. panta 1. punkts paredz, ka gadījumos, kad apstrāde ir jāveic pārziņa vārdā, pārziņis izmanto tikai tādas apstrādātājus, kas sniedz pietiekamas garantijas, ka tiks īstenoti atbilstoši tehniskie un organizatoriskie pasākumi

tādā veidā, ka apstrādē tiks ievērotas šīs regulas prasības un tiks nodrošināta datu subjekta tiesību aizsardzība. Tas nozīmē, ka tieši pārzinis ir atbildīgs par apstrādātāja sniegto garantiju pietiekamības novērtēšanu, un viņam jāspēj pierādīt, ka ir nopietni ņēmis vērā visus Datu regulā paredzētos elementus.

Savukārt Datu regulas 28. panta 3. punkts noteic, ka apstrādi, ko veic apstrādātājs, ir nepieciešams reglamentēt ar līgumu vai ar citu juridisku aktu saskaņā ar Savienības vai dalībvalsts tiesību aktiem, kas ir saistošs apstrādātājam un pārzinim un kurā norāda līguma priekšmetu un apstrādes ilgumu, apstrādes raksturu un nolūku, personas datu veidu un datu subjektu kategorijas un pārziņa pienākumus un tiesības. Minētajā līgumā vai citā juridiskajā aktā jo īpaši jāparedz, ka apstrādātājs: a) personas datus apstrādā tikai pēc pārziņa dokumentētiem norādījumiem, tostarp saistībā ar nosūtīšanu uz trešo valsti vai starptautisku organizāciju, izņemot, ja tas ir jādara saskaņā ar Savienības vai dalībvalsts tiesību aktiem, kas piemērojami apstrādātājam, un šādā gadījumā apstrādātājs par minēto juridisko prasību informē pārzini pirms apstrādes, izņemot, ja ar attiecīgo tiesību aktu šāda informēšana ir aizliegta svarīgu sabiedrības interešu dēļ; c) īsteno visus pasākumus, kas nepieciešami saskaņā ar 32. pantu; f) palīdz pārzinim nodrošināt 32. līdz 36. pantā minēto pienākumu izpildi, ņemot vērā apstrādes veidu un apstrādātājam pieejamo informāciju; h) pārzinim dara pieejamu visu informāciju, kas nepieciešama, lai apliecinātu, ka tiek pildīti šajā pantā paredzētie pienākumi, un lai ļautu pārzinim vai citam pārziņa pilnvarotam revidentam veikt revīzijas, tostarp pārbaudes, un sniegtu tajās ieguldījumu¹⁶.

Turklāt Datu regulas 28. panta 9. punktā paredzēts, ka šā panta 3. un 4. punktā minētais līgums vai cits juridiskais akts ir jāsagatavo rakstiskā formā, tostarp elektroniski. Inspekcija vērš uzmanību, ka, lai gan Datu regula nenosaka, ka šiem nosacījumiem būtu obligāti jābūt ietvertiem vienā konkrētā dokumentā, attiecīgajam līgumam vai citam juridiskajam aktam (aktiem) ir jābūt nostiprinātiem rakstveidā, abām pusēm par tiem vienojoties pirms attiecīgās apstrādes veikšanas. Līgumā vai attiecīgajā juridiskajā aktā būtu jāiekļauj detalizēta informācija ne tikai par pārziņa un apstrādātāja lomu un pienākumu sadali, bet arī par to, cik bieži un kā jāvirzās informācijas plūsmai starp apstrādātāju un pārzini, lai pārzinis būtu pilnībā informēts par apstrādes detaļām, kas ir būtiskas, lai pierādītu atbilstību Datu regulas 28. pantā noteiktajiem pienākumiem¹⁷. Piemēram, apstrādātāja reģistrēto apstrādes darbību attiecīgās daļas var tikt kopīgotas ar pārzini, sniedzot informāciju par izmantoto sistēmu darbību, drošības pasākumiem, to, kā tiek ievērotas datu saglabāšanas prasības, datu atrašanās vietu, datu pārsūtīšanu, to, kam ir piekļuve datiem un kas ir datu saņēmēji, kādi apakšapstrādātāji tiek iesaistīti, utt.¹⁸

Izvērtējot Pašvaldības paskaidrojumus un iesniegtos pamatojošos dokumentus, Inspekcija konstatē, ka starp Pašvaldību un ZZ Dats nav noslēgts personas datu apstrādes līgums. Lai gan atsevišķi noteikumi ir minēti Vienošanās un Noteikumos, tie ir pārāk vispārīgi un nesatur konkrētu lomu sadalījumu, pušu tiesības un pienākumus, atbildību saistībā ar veicamo apstrādi, savstarpēji sniedzamās informācijas apjomu un kārtību vai citus konkrētajai apstrādei būtiskus apstākļus, lai nodrošinātu personas datu drošību, iespējamu revīziju veikšanu no pārziņa puses un efektīvu Datu regulas prasību izpildi. Turklāt Inspekcija secina, ka personas datu apstrādes līguma noslēgšanas

¹⁶ Attiecībā uz 28. panta 3. punkta pirmās daļas h) apakšpunktu apstrādātājam ir pienākums nekavējoties informēt pārzini, ja, viņaprāt, kāds norādījums pārkāpj Datu regulas prasības vai citus Eiropas Savienības vai dalībvalstu datu aizsardzības noteikumus.

¹⁷ Datu regulas 28. panta 3. punkta h) apakšpunkts paredz, ka apstrādātājam ir jādara pārzinim pieejama visa informācija, kas nepieciešama, lai apliecinātu, ka tiek pildīti 28. pantā paredzētie pienākumi, un lai ļautu pārzinim vai citam pārziņa pilnvarotam revidentam veikt revīzijas, tostarp pārbaudes, un sniegtu tajās ieguldījumu.

¹⁸ Eiropas Datu aizsardzības kolēģijas 2021. gada 7. jūlija Pamatnostādnes par pārziņa un apstrādātāja jēdzieniem VДАР, 143. punkts.

nepieciešamību Pašvaldība konstatēja tikai pēc Pārkāpuma iestāšanās, kad bija jāveic Pārkāpuma izmeklēšana un ziņošana kompetentajām iestādēm.

Tādējādi secināms, ka Pašvaldība, uzticot personas datu apstrādi apstrādātājam ZZ Dats, ir rīkojusies, neievērojot Datu regulas 28. panta 3. punkta prasības, ļaujoties uz vispārīgām frāzēm un citu iestāžu rīcību, bet pašai neuzņemoties atbildību par veiktās apstrādes atbilstību Datu regulas prasībām.

[3.7] Saskaņā ar Datu regulas 32. panta 1. punktu, ņemot vērā tehnikas līmeni, īstenošanas izmaksas un apstrādes raksturu, apmēru, kontekstu un nolūkus, kā arī dažādas iespējamības un smaguma pakāpes risku attiecībā uz fizisku personu tiesībām un brīvībām, pārzinis un apstrādātājs īsteno atbilstīgus tehniskus un organizatoriskus pasākumus, lai nodrošinātu tādu drošības līmeni, kas atbilst riskam, tostarp attiecīgā gadījumā cita starpā: b) spēju nodrošināt apstrādes sistēmu un pakalpojumu nepārtrauktu konfidencialitāti, integritāti, pieejamību un noturību; d) procesu regulārai tehnisko un organizatorisko pasākumu efektivitātes testēšanai, izvērtēšanai un novērtēšanai, lai nodrošinātu apstrādes drošību. Savukārt Datu regulas 32. panta 2. punkts paredz, ka, novērtējot atbilstīgo drošības līmeni, jo īpaši jāņem vērā riski, ko rada apstrāde, jo īpaši nejauša vai nelikumīga nosūtīto, uzglabāto vai citādi apstrādāto personas datu iznīcināšana, nozaudēšana, pārveidošana, neatļauta izpaušana vai piekļuve tiem.

Inspekcija norāda, ka, lai gan Pašvaldība nav tieši atbildīga par Pārkāpumu izraisījušo tehnisko kļūdu, pārbaudes Lietā konstatētais liecina, ka Pašvaldība, izmantojot ZZ Dats pakalpojumus, nav nodrošinājusi pietiekamu uzraudzību pār apstrādātāja ZZ Dats veiktajām darbībām Pašvaldībā deklarēto iedzīvotāju personas datu apstrādē, kā rezultātā ir iestājies Pārkāpums, kuru būtu bijis iespējams novērst, īstenojot atbilstošu pārziņa un apstrādātāja savstarpējo sadarbību.

Proti, izvērtējot Inspekcijas rīcībā esošo informāciju par Pārkāpuma (incidenta) apstākļiem, konstatējams, ka tā cēlonis bija kļūda sistēmas ugunsmūra konfigurēšanas laikā, ko – neatkarīgi no tā, vai kļūda ir saistīta ar darbinieka amata pienākumu nepienācīgu izpildi vai programmatūras bojājumu vai citiem ierobežojumiem, – būtu iespējams minimizēt vai novērst pavisam, ja attiecīgajā procesā būtu paredzēta papildu ugunsmūra konfigurācijas pārvaldības kontrole, piemēram: iepriekš veiktas pārbaudes simulētā testa vidē, automatizēta konfigurācijas validācija, izmaiņu pārskatīšanas process, ievērojot “četrus acu principu”, intrūzijas noteikšanas un novēršanas sistēmu (IDS/IPS) izmantošana vai uzvedības novērošana pēc programmatūras konfigurēšanas, izmantojot SIEM risinājumus u.c.

Ievērojot minētos apsvērumus, Inspekcija konstatē, ka Pašvaldība nav iesniegusi nekādus pierādījumus tam, ka Pašvaldība pirms Pārkāpuma būtu veikusi risku izvērtējumu vai noteikusi konkrētus un īstenojamus drošības pasākumus veicamajai personas datu apstrādei, tā nav veikusi savas pārbaudes vai auditus, kā arī Pašvaldība līgumiski nebija pietiekami precizējusi apstrādātāja pienākumus drošības jomā un netika izstrādāta incidentu atklāšanas procedūra vai komunikācijas kārtība. Ievērojot minēto secināms, ka Pašvaldība kā pārzinis nav pilnvērtīgi ievērojusi Datu regulas 32. panta 1. un 2. punkta prasības, bet gan paļāvusies uz ZZ Dats autonomu rīcību, atbilstību sertifikācijām un apstākli, ka līdz šim ZZ Dats veiktajā personas datu apstrādē nav bijuši konstatēti pārkāpumi.

[4] Ievērojot minēto attiecībā uz Lietas ietvaros izvērtēto Pašvaldības rīcību, Inspekcija konstatē, ka Pašvaldība tās administratīvajā teritorijā deklarēto iedzīvotāju veiktajā personas datu apstrādē VPS nav nodrošinājusi nepieciešamo tehnisko un organizatorisko pasākumu ieviešanu un īstenošanu sadarbībā ar apstrādātāju ZZ Dats, kā rezultātā jau kopš minētās apstrādes sākuma nebija un joprojām netiek nodrošināta tiesiskajam regulējumam atbilstoša personas datu drošība.

Tādējādi secināms, ka **Pašvaldības rīcība nav atbilstoša 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 un 28. panta 9. punkta, kā arī 32. panta 1. punkta b) un d) apakšpunkta un 32. panta 2. punkta prasībām.

[5] Saskaņā ar Datu regulas 58. panta 2. punkta b) apakšpunktu katrai uzraudzības iestādei ir pilnvaras izteikt rājienu pārzinim vai apstrādātājam, ja ar apstrādes darbībām ir tikuši pārkāpti šīs regulas noteikumi, savukārt Datu regulas 58. panta 2. punkta d) apakšpunkts paredz Inspekcijas pilnvaras izdot rīkojumu pārzinim vai apstrādātājam saskaņot apstrādes darbības ar Datu regulas noteikumiem, vajadzības gadījumā – konkrētā veidā un konkrētā laikposmā. Datu regulas 23. pants noteic, ka Inspekcija, pieņemot lēmumus attiecībā uz tiesiskā pienākuma uzlikšanu piemēro APL.

[5.1] Ievērojot minēto un to, ka Pašvaldības rīcībā ir konstatēti Datu regulas noteikumu pārkāpumi, Inspekcijai saskaņā ar APL 62. panta pirmo daļu, lemjot par tāda administratīvā akta izdošanu, kas varētu būt nelabvēlīgs adresātiem, iestādei (konkrētajā gadījumā Inspekcija) ir nepieciešams noskaidrot un izvērtēt adresātu viedokli un argumentus šajā lietā. Adresāts (Pašvaldība) Atbildes vēstulē sniedza savus paskaidrojumus lietā un tie ir ņemti vērā, pieņemot lēmumu.

[5.2] Saskaņā ar APL 66. panta pirmo daļu iestādei ir nepieciešams lemt par administratīvā akta izdošanas lietderību. Proti, pieņemot lēmumu par prettiesiskās personas datu apstrādes novēršanu, Inspekcijai jāvērtē iespēja lemt par mazāku personas tiesību ierobežojumu. Inspekcija secina, ka lēmuma pieņemšana ir nepieciešama un vajadzīga, lai sasniegtu mērķi – novērstu Datu regulas noteikumu pārkāpumus Pašvaldības rīcībā, apstrādājot personas datus VPS un izmantojot apstrādātāju šim nolūkam. Turklāt tiesiskā pienākuma uzlikšana ir vērsta uz datu subjektiem Datu regulā, Datu likumā un citos normatīvajos aktos paredzēto pamattiesību uz personas datu aizsardzību nodrošināšanu.

Administratīvais akts ir uzskatāms par piemērotu līdzekli šā mērķa sasniegšanai, jo rada tiesisku pienākumu Pašvaldībai novērst konstatētos pārkāpumus konkrētā procesuālā termiņā, kā arī novērš līdzīgu pārkāpumu rašanos nākotnē. Vienlaikus administratīvais akts ir uzskatāms par samērīgāko līdzekli mērķa sasniegšanai, jo salīdzinājumā ar lēmumu par administratīvā soda uzlikšanu ir uzskatāms par saudzīgāku.

Ievērojot minēto, Inspekcija, pamatojoties uz Datu regulas 58. panta 1. punkta e) apakšpunktu un 2. punkta b) un d) apakšpunktu, Datu likuma 5. panta pirmās daļas 3. un 6. punktu, Datu likuma 23. pantu un APL 63. panta pirmās daļas 2) punktu,

nolemj:

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 ZZ Dats 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 rakstveidā¹⁹ informēt Inspekciju, līdz 2025. gada 5. decembrim²⁰ iesniedzot informāciju par veiktajām darbībām.

Saskaņā ar APL 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 pirmā *prim* daļa noteic, ka dokuments, kas nosūtīts uz oficiālo elektronisko adresi, uzskatāms par paziņotu otrajā darba dienā pēc tā nosūtīšanas. Šo lēmumu saskaņā APL 76. panta pirmo un otro daļu, 79. panta pirmo daļu un Datu likuma 24. panta pirmo daļu var pārsūdzēt viena mēneša laikā no tā spēkā stāšanās dienas Datu valsts inspekcijas direktoram.

[6] Inspekcija informē, ka saskaņā ar Datu likuma 38. panta pirmo un otro daļu par jebkurām publisko tiesību juridiskās personas nelikumīgām darbībām ar personas datiem Inspekcija var piemērot brīdinājumu vai naudas sodu amatpersonai līdz divsimt naudas soda vienībām, savukārt par pārziņa vai apstrādātāja pienākumu nepildīšanu publisko tiesību juridiskās personas institūcijā – brīdinājumu vai naudas sodu amatpersonai līdz divsimt naudas soda vienībām.

Ievērojot minēto, Inspekcija informē, ka gadījumā, ja netiks pildīts šajā vēstulē minētais rīkojums, Inspekcija īstenos citas Datu regulā un Datu likumā Inspekcijai piešķirtās pilnvaras.

Direktora vietniece

L. Dilba

[..]

¹⁹ Inspekcija pieņem dokumentus, kas ir parakstīti pašrocīgi (sūtāmi pa pastu vai ievietojot Inspekcijas pastkastītē) vai ar drošu elektronisko parakstu uz Inspekcijas oficiālo elektroniskā pasta adresi *pasts@dvi.gov.lv* un oficiālajā elektroniskajā adresē (E-adresē), un noformētas atbilstoši Dokumentu juridiskā spēka likuma prasībām.

²⁰ Pēdējā diena rakstiskas atbildes iesniegšanai pastā vai nosūtīšanai elektroniski ar drošu elektronisko parakstu.