Datu valsts inspekcija

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

Lieta Nr. L-2-6/5980

Sabiedrībai ar ierobežotu atbildību
"LIEPĀJAS REĢIONĀLĀ SLIMNĪCA"

Lēmums

Rīgā, 22.09.2025. Nr. 2-2.2/63

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 Sabiedrības ar ierobežotu atbildību "LIEPĀJAS REĢIONĀLĀ SLIMNĪCA", vienotais reģistrācijas numurs 42103041306 (turpmāk – Slimnīca) darbiniekiem un klientiem.

[1.1] Saistībā ar notikušo Pārkāpumu Inspekcija saņēma Slimnīcas 2025. gada 15. novembra paziņojumu[1] (turpmāk – Paziņojums), kurā tika norādīts, ka Slimnīca konstatēja Pārkāpumu 2024. gada 11. novembrī un paskaidrots, ka Liepājas valstspilsētas pašvaldības (turpmāk – Pašvaldība) apstrādātājam ZZ Dats noticis kiberdrošības incidents. Pārkāpums skar visas Latvijas pašvaldības, kuras izmanto Vienotās pašvaldību sistēmas (turpmāk – VPS). Pārkāpumā nav ietekmēta datu integritāte (nekas nav mainīts vai izdzēsts) un konkrētās personas nav piekļuvušas dokumentiem, kas ir datņu formātā. Uz Paziņojuma iesniegšanas dienu nav zināms tieši Slimnīcas datu ierakstu un datu subjektu skaits, kuru skar pārkāpums.

Paziņojumā norādīts, ka Slimnīcas un Pašvaldības starpā ir noslēgts līgums par IS Lietvaris lietošanu, kur tiek iesaistīts apakšapstrādātājs ZZ Dats. ZZ Dats informācijas sistēmu izstrādes un uzturēšanas pakalpojumi ir sertificēti atbilstoši starptautiski atzītiem kvalitātes un informācijas drošības standartiem: ISO 9001:2015 "Kvalitātes pārvaldības sistēmas. Prasības" un ISO/IEC 27001:2013 "Informācijas tehnoloģijas. Drošības paņēmieni. Informācijas drošības pārvaldības sistēmas. Prasības". ZZ Dats informācijas drošības pārvaldības sistēmai, gan iekšējos, gan ārējos auditos tiek regulāri pārbaudīta atbilstība: uzņēmuma procedūrām, industrijas labajai praksei, normatīvo dokumentu prasībām un minēto starptautisko standartu prasībām un vadlīnijām.

[1] Inspekcijā saņemts un reģistrēts 2024. gada 15. novembrī ar Nr. 2-5.2/164

Papildus norādīts, ka ZZ Dats veicis pasākumus, lai pārtrauktu nesankcionēto piekļuvi personas datiem. Ziņojis CERT.LV un Inspekcijai. Saglabāta datu integritāte.

[1.2] Nolūkā pārliecināties par Slimnīcas 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 regulas[2] (turpmāk – Datu regula) 58. panta 1. punkta e) apakšpunktu 2025. gada 12. februārī aicināja Slimnīcu sniegt papildu informāciju[3]: 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 Slimnīcu par izmaiņām ZZ Dats īstenotajos tehniskajos un organizatoriskajos pasākumos pārziņu personas datu apstrādē, par kārtību, kādā ZZ Dats informē Slimnīcu par notikušiem personas datu aizsardzības pārkāpumiem, kā arī aicināja Slimnīcu iesniegt ziņojumu par Pārkāpuma izmeklēšanu.

[1.3] Slimnīca 2025. gada 28. februāra atbildes vēstulē Nr. 186/1.10[4] (turpmāk – Atbildes vēstule) sniedza turpmāk norādīto informāciju uz Inspekcijas jautājumiem.

[1.3.1] Attiecībā uz ZZ Dats kā apstrādātāja izvēli, Slimnīca paskaidroja, ka ZZ Dats informācijas sistēmas "Lietvaris" (turpmāk – Lietvaris) lietošanu uzsāka 2018. gada 23. novembrī, pamatojoties uz Pašvaldības izpilddirektora 2018. gada 23. novembra rīkojumu Nr. 244, līdz ar to Slimnīcai praktiski bija jāuzsāk Lietvaris lietošana pamatojoties uz Pašvaldības kā Slimnīcas kapitāldaļu turētāja rīkojumu.

[1.3.2] Attiecībā uz personas datu apstrādes līguma noslēgšanu, Slimnīca paskaidroja, tai ar ZZ Dats nav noslēgts līgums, bet Slimnīcai kā pārzinim ir noslēgta Vienošanās ar Pašvaldību kā apstrādātāju, kura ZZ Dats ir piesaistījusi kā apakšapstrādātāju.

[1.3.3] Attiecībā uz ZZ Dats kā apstrādātāja uzraudzību, t.sk., vai ir izstrādāti apstrādātāja uzraudzības noteikumi, Slimnīca paskaidro, ka apstrādātāju piesaisti un uzraudzības kārtību ir noteikusi savos iekšējos Personas datu apstrādes un aizsardzības noteikumos un Vienošanās ar Pašvaldību, kur ir noteiktas tiesības pieprasīt informāciju no Pašvaldības kā apstrādātāja. Tāpat Pašvaldība katru gadu pārslēdzot jaunu līgumu ar ZZ Dats regulāri veic ZZ Dats piegādāto informācijas sistēmu pārvērtēšanu.

Tāpat kā būtisks aspekts norādīts, ka ZZ Dats pastāvīgi uztur starptaustisku informācijas drošības Pārvaldības standaru ISO/IEC 27001, kas apliecina ZZ Dats kā Lietvaris uzturētāju atbilstību nozares labās prakses pieņemtajiem standartiem.

Slimnīca norāda, ka Slimnīca nav izstrādājusi atsevišķu personas datu apstrādātāja uzraudzības kārtību, taču pastāvīgi tiek sekots līdz apstrādātāju darbībām un uzturēta savstarpējā informācijas apmaiņa.

[1.3.4] Attiecībā uz ZZ Dats kā apstrādātāja risku analīzi, Slimnīca paskaidroja, ka risku analīzi informācijas sistēmai Lietvaris ir veikusi Pašvaldība, kas pēc Pašvaldības sniegtās informācijas iesniegta Inspekcijā.

[1.3.5] Attiecībā uz to, kā ZZ Dats informē Slimnīcu par izmaiņām ZZ Dats īstenotajos tehniskajos un organizatoriskajos pasākumos pārziņu personas datu apstrādē, Slimnīca paskaidroja, ka Pašvaldība Slimnīcai informāciju par īstenotajiem tehniskajiem un organizatoriskajiem

---

[2] 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.
[3] Inspekcijas 2025. gada 12. februāra vēstule Nr. 2-4.2/172-N *Par pārbaudes uzsākšanu un informācijas pieprasījumu.*
[4] Inspekcijā saņemta un reģistrēta 2025. gada 3. martā ar Nr. 2-4.2/318-S.

pasākumiem saņem pēc tam, kad Pašvaldība tos atbilstoši VPS uzturēšanas Noteikumiem[5] saņem no ZZ Dats.

Saskaņā ar Noteikumiem ne vēlāk kā piecas darba dienas iepriekš Pašvaldības atbildīgie pārstāvji tiek informēti par plānotajām būtiskajām izmaiņām sistēmas funkcionalitātē, lietošanas kārtībā vai pieejamībā. 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 Slimnīcu par notikušiem personas datu aizsardzības pārkāpumiem, Slimnīca paskaidroja, ka ņemot vēra to apstākli, ka Slimnīcai tiešās pārziņa apstrādātāja attiecības ir ar Pašvaldību, tad pārkāpuma paziņošanas kārtība paredzēta Vienošanās, kurā noteikts, ka Pašvaldība dokumentē visus personas datu aizsardzības pārkāpumus, norādot faktus, kas saistīti ar personas datu pārkāpumu, tā sekas un veiktās koriģējošās darbības. Ja ir iestājies personas datu aizsardzības pārkāpums, Pašvaldība pēc iespējas ātri, bet ne vēlāk kā 72 stundas no drošības incidenta vai personas datu aizsardzības pārkāpuma konstatēšanas brīža, nosūta informāciju par to Slimnīcai, norādot personas datu aizsardzības pārkāpuma aprakstu, tostarp, ja iespējams, ietekmēto datu subjektu kategorijas un aptuveno skaitu, ietekmēto personas datu ierakstu kategorijas un aptuvenais skaitu, datu aizsardzības speciālista vārdu un uzvārdu, un kontaktinformāciju vai norāda citu kontaktpersonu ar mērķi iegūt papildus informāciju par personas datu pārkāpumu, personas datu aizsardzības pārkāpuma iespējamo seku aprakstu, pasākumu, ko Pašvaldība veikusi vai ierosinājusi veikt, lai novērstu personas datu aizsardzības pārkāpumu, aprakstu, tostarp pasākumus, lai mazinātu iespējamās nelabvēlīgās sekas, un lai Slimnīca varētu izpildīt savu pienākumu ziņot par šo pārkāpumu Inspekcijai.

[1.3.7] Attiecībā uz Slimnīcas ziņojuma par Pārkāpuma izmeklēšanu iesniegšanu, Slimnīca norādīja, ka ir veikusi incidenta izvērtēšanu, kā ietvaros ir pieprasīta papildus informācija no Pašvaldības un vērtēts iespējams risks uz datu subjektu tiesībām.

Papildus notiek saziņa ar Pašvaldības datu aizsardzības speciālistu, kurš informē Slimnīcu par situācijas attīstību, tostarp, arī Slimnīca ir uzsākusi veikt jaunu novērtējumu par ietekmi uz datu aizsardzību Lietvedības procesiem, kas tieši saistīta ar Lietvaris lietošanu.

[1.3.8] Atbildes vēstules pielikumā Slimnīca iesniedza šādus dokumentāros pierādījumus un materiālus, kas pamato tās sniegtās atbildes uz Inspekcijas jautājumiem: 1) Pašvaldības 2018.gada 23. novembra rīkojuma Nr. 244 kopiju; 2) Vienošanās par VPS lietošanu un personu datu apstrādes noteikumiem kopiju; 3) Slimnīca Personas datu apstrādes un aizsardzība noteikumi sadaļa "Personas datu apstrādātāju prasības" (noraksts); 4) Slimnīcas Pārkāpuma izvērtējums; 5) Slimnīcas vēstule Pašvaldībai papildus informācijas pieprasīšanai; 6) Pašvaldības atbildes vēstule uz Slimnīcas pieprasījumu.

[1.3.9] Ar Inspekcijas amatpersonas lēmumu[6] Inspekcijas pārbaudes lietā Nr. L-2-6/5930 konstatēts, ka Pārkāpuma cēlonis bija ZZ Dats darbinieka pieļauta kļūda ugunsmūra konfigurācijas izmaiņu ieviešanā, kā rezultātā ugunsmūra noteikumi ļāva trešajām personām nesankcionēti piekļūt VPS esošiem personas datiem. Inspekcija secināja, ka ZZ Dats pirms Pārkāpuma 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

[5] https://www.zzdats.lv/vps-uzturesanas-noteikumi
[6] Inspekcijas 2025. gada 23. jūlija lēmums Nr. 01630000100325-3

kontroli un tā tiktu savlaicīgi novērsta, nepieļaujot Pārkāpuma 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 Slimnīcas 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 Slimnīcas 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 Slimnīcas.

[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 pārzinis[7]. Konkrētajā gadījumā Inspekcija konstatē, ka attiecībā uz Slimnīcas darbinieku/klientu veikto personas datu apstrādi VPS Lietvaris Slimnīca ir uzskatāma par pārzini,

Datu regulas 4. panta 8) apakšpunkts noteic, ka apstrādātājs ir fiziska vai juridiska persona, publiska iestāde, aģentūra vai cita struktūra, kura *pārziņa vārdā apstrādā personas datus*. Atbilstoši minētajai definīcijai, Pašvaldība nevar tikt uzskatīta par apstrādātāju, jo tā saskaņā ar Vienošanās norādīto sniedz Slimnīcai atbalstu VPS lietošanā, nodrošinot lietotāju tiesību piešķiršanu un lietotāju konsultēšanu, Pašvaldība pati neveic VPS uzturēšanu un jebkādu Slimnīcas darbinieku/klientu personas datu apstrādi VPS. VPS uzturēšanu un datu apstrādi VPS nodrošina ZZ Dats, tādējādi ZZ Dats ir uzskatāma par apstrādātāju Datu regulas izpratnē[8], bet Pašvaldība darbojas šajā gadījumā kā starpnieks starp pārzini (Slimnīcu) un apstrādātāju (ZZ Dats). Līdz ar to Slimnīcai kā personas datu apstrādes pārzinim ir jānodrošina Datu regulas prasību ievērošana, tostarp attiecībās ar izvēlēto apstrādātāju ZZ Dats.

[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 Slimnīca ir iesniegusi tās rīcībā esošo dokumentāciju saistībā ar tās veikto personas datu apstrādi VPS, notikušo Pārkāpumu un kā Slimnīca pārliecinās par apstrādātāja ieviesto tehnisko un organizatorisko pasākumu un kontroļu atbilstību. Tikai izvērtējot šos dokumentus, Inspekcija var izdarīt secinājumus par to, vai Slimnīca ir spējusi nodrošināt tādu procesu, kas pierāda Slimnīcas veiktās personas datu apstrādes atbilstību tiesiskajam

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

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

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 Pārkāpuma rezultātā nepiederošām trešajām personām izdevās piekļūt VPS glabātajiem personas datiem, tostarp par Slimnīcas darbiniekiem/klientiem. 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 (Slimnīca), nevis tikai konkrētajām apstrādes darbībām izvēlētais apstrādātājs vai sistēmas uzturētājs. Savukārt attiecībā uz pārziņa atbildības līmeni saistībā ar Pārkāpumu 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 nevar atsaukties, piemēram, uz tiesiskās paļāvības principu[9], kas minēts Administratīvā procesa likuma (turpmāk – APL) 10. pantā, jo Slimnīcai 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, Pašvaldība, 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 Slimnīcas kā personas datu pārziņa rīcību un atbildības līmeni, nevis citu iestāžu kompetenci saistībā ar notikušo Pārkāpumu.

Ievērojot minēto, izvērtējot visu tās rīcībā esošo informāciju, Inspekcija secina, ka attiecībā uz veikto personas datu apstrādi VPS infrastruktūrā Slimnīca 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 Slimnīca no savas

[9] APL 10. pants paredz, ka privātpersona var paļauties, ka iestādes rīcība ir tiesiska un konsekventa. Tiesiskās paļāvības princips aizsargā tikai tādas tiesības, uz kuru īstenošanu personai varēja rasties likumīga, pamatota un saprātīga paļāvība, kas ir minētā 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.

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 Slimnīca neveic ZZ Dats uzraudzību, bet gan paļaujas uz Noteikumos paredzētajām klauzulām, ZZ Dats izsniegtajiem un uzturētajiem ISO sertifikātiem, Pašvaldības veikto izvērtējumu, kā arī Slimnīca atzīst, ka par tehniskajiem uzlabojumiem VPS infrastruktūrā tā nesaņem no ZZ Dats nekādas atskaites, ziņojumus vai auditācijas pierakstus (tostarp, par ugunsmūra konfigurācijām vai citiem personas datu drošību ietekmējošiem procesiem).

Šajā ziņā Inspekcija norāda, ka tās ieskatā konkrētās datu apstrādes ietvaros nebūtu saprātīgi sagaidīt, ka ZZ Dats sniedz Slimnīcai detalizētus paziņojumus par visiem tehniskajiem procesiem un uzlabojumiem, kas tiek veikti VPS infrastruktūrā, tomēr Slimnīcai, ņemot vērā dažādas iespējamības un nopietnības pakāpes riskus datu subjektu tiesībām un brīvībām, būtu jābūt iespējai – vismaz pēc Slimnīcas pamatota pieprasījuma – saņemt pamatinformāciju par sistēmas uzturēto drošības līmeni vai līgumā atrunātos gadījumos, kad tiek veiktas nozīmīgas tehniskas izmaiņas, tos iepriekš savstarpēji saskaņot. Proti, Slimnīcas paļaušanās vien uz faktu, ka apstrādātājam ZZ Dats ir spēkā esoši ISO sertifikāti un ikgadēji veikti sistēmas drošības auditi, bez jebkādas iespējas Slimnīcai piedalīties procesos, tos vajadzības gadījumā savstarpēji saskaņojot, nav atzīstams par pietiekamu, lai nodrošinātu Slimnīcas kā pārziņa rīcības atbilstību Datu regulas prasībām. Tādējādi Inspekcija secina, ka Slimnīca ZZ Dats uzraudzībā nenodrošina Datu regulas 25. panta 1. punkta prasības. Proti, ZZ Dats, apstrādājot Slimnīcas nodotos personas datus, ir rīkojusies patstāvīgi bez pārziņa iesaistes, ne tikai par apstrādes tehniskajiem aspektiem neinformējot pārzini, bet arī savstarpēji nevienojoties par nepieciešamo rīcību un ieviešamajiem pasākumiem personas datu integritātes nodrošināšanai no apstrādātāja vai pārziņa puses, kā rezultātā Slimnīca sev kā pārzinim nav nodrošinājusi patiesas kontroles iespējas par tās apstrādājamo 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, pārzinis izmanto tikai tādus 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 ieguldījumu[10].

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 pienākumiem[11]. 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.[12]

Izvērtējot Slimnīcas paskaidrojumus un iesniegtos pamatojošos dokumentus, Inspekcija konstatē, ka starp Slimnīcu un ZZ Dats nav noslēgts personas datu apstrādes līgums vai vienošanās. Tam apstāklim, ka Slimnīcai nebija izvēles brīvības, un bija jāuzsāk VPS moduļu lietošana, pamatojoties uz Pašvaldības rīkojumu, nav nozīmes no datu apstrādes viedokļa, jo tas neatbrīvo Slimnīcu no Datu regulā paredzētiem pārziņa pienākumiem, tostarp, no pienākuma noslēgt līgumu ar tiešu apstrādātāju, paredzot tajā 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.

Tādējādi secināms, ka Slimnīca, uzticot personas datu apstrādi apstrādātājam ZZ Dats, ir rīkojusies, neievērojot Datu regulas 28. panta 3. punkta prasības, paļaujoties 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

---

[10] 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.

[11] 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.

[12] Eiropas Datu aizsardzības kolēģijas 2021. gada 7. jūlija Pamatnostādnes par pārziņa un apstrādātāja jēdzieniem Datu regulas, 143. punkts.

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 Slimnīca nav tieši atbildīga par Pārkāpumu izraisījušo tehnisko kļūdu, pārbaudes Lietā konstatētais liecina, ka Slimnīca, izmantojot ZZ Dats pakalpojumus, nav nodrošinājusi pietiekamu uzraudzību pār apstrādātāja ZZ Dats veiktajām darbībām Slimnīcas darbinieku 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 "četru 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 Slimnīca nav iesniegusi nekādus pierādījumus tam, ka Slimnīca būtu veikusi risku izvērtējumu vai noteikusi konkrētus un īstenojamus drošības pasākumus veicamajai personas datu apstrādei, tā nav veikusi savas pārbaudes vai auditus, kā arī Slimnīca līgumiski nebija pietiekami precizējusi apstrādātāja pienākumus drošības jomā un netika izstrādāta incidentu atklāšanas procedūra vai komunikācijas kārtība. Ievērojot minēto secināms, ka Slimnīca 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.

[3.8] Personas datu apstrādes pārkāpumu gadījumos Datu regulas 33. panta 1. punkts paredz, ka pārzinim ir pienākums bez nepamatotas kavēšanās un, ja iespējams, 72 stundu laikā no pārkāpuma konstatēšanas, paziņot par to kompetentajai uzraudzības iestādei, sniedzot visu šā panta 3. punktā norādīto informāciju, izņemot gadījumus, kad ir maz ticams, ka minētais pārkāpums varētu radīt risku fizisku personu tiesībām un brīvībām, kā arī saskaņā ar minētā panta 5. punktu dokumentēt visus faktus un veiktos pasākumus saistībā ar notikušo pārkāpumu.

Ja paziņošana uzraudzības iestādei nav notikusi 72 stundu laikā, paziņojumam pievieno kavēšanās iemeslus. Savukārt gadījumos, ja visu informāciju nav iespējams sniegt vienlaikus un nepieciešams veikt papildu pārbaudi/informācijas apkopošanu, lai konstatētu visus ar incidentu saistītos faktus, Datu regulas 33. panta 4. punkts ļauj informāciju par Pārkāpumu sniegt pa posmiem, t.i. paziņojot par notikušo pārkāpumu, pārzinim ir iespēja informēt Inspekciju, ka viņa rīcībā vēl nav visa nepieciešamā informācija un ka sīkāka informācija tiks sniegta vēlāk. Ievērojot minēto, precīzas informācijas trūkums vai nepieciešamība veikt papildu izmeklēšanu vai informācijas apkopošanu nav uzskatāma par objektīvu iemeslu savlaicīgai paziņošanai par pārkāpumu.

Pamatojoties uz Inspekcijas rīcībā esošo informāciju, tika konstatēts, ka Slimnīca nav iesniegusi Inspekcijai sākotnējo paziņojumu par Pārkāpumu Datu regulas noteiktajā termiņā.

Turklāt, ņemot vērā iepriekš Inspekcijas izdarītos secinājumus, ka Slimnīcai kā pārzinim nav bijušas patiesas iespējas monitorēt un pārliecināties par datu subjektu personas datu aizsardzību ZZ Dats uzturētajā VPS infrastruktūrā, tostarp nodrošināt, ka gadījumā, ja ZZ Dats konstatē incidentu (Pārkāpumu) sistēmā, tiek īstenota iepriekš abu pušu apstiprināta datu aizsardzības pārkāpumu reaģēšanas kārtība un nekavējoties informēta Pašvaldība, iesniedzot tai visu nepieciešamo informāciju. Tas savukārt novērstu iespējamību, ka šādi incidenti tiek paziņoti ar termiņa kavējumu attiecīgajām uzraudzības iestādēm ne tikai no apstrādātāja, bet arī no pārziņa puses.

[4] Ievērojot minēto attiecībā uz Lietas ietvaros izvērtēto Slimnīcas rīcību, Inspekcija konstatē, ka Slimnīca tās darbinieku 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 **Slimnīcas 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 un 33. panta 1. 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 Slimnīcas 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 (Slimnīca) 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 Slimnīcass 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 Slimnīcai 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 Slimnīcai rājienu;

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

a) pārskatīt tās iekšējos personas datu apstrādes noteikumus, tostarp izstrādāt Slimnīcas 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 rakstveidā[13] informēt Inspekciju, līdz 2025. gada 5. decembrim[14] 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 lēmumā minētais rīkojums, Inspekcija īstenos citas Datu regulā un Datu likumā Inspekcijai piešķirtās pilnvaras.

Direktora vietniece L. Dilba

[..]

[13] 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.

[14] Pēdējā diena rakstiskas atbildes iesniegšanai pastā vai nosūtīšanai elektroniski ar drošu elektronisko parakstu.