Datu valsts inspekcija

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

Gulbenes novada pašvaldībai
Nosūtīšanai e-adreses elektroniskajā sistēmā

Lēmums

Rīgā, 20.11.2025. Nr. 1-2.3/22-DVI

Par Datu valsts inspekcijas 2025. gada 22. septembra lēmumu Nr. 2-2.2/42 apstrīdēšanu

[1] Datu valsts inspekcijā (turpmāk – Inspekcija) saņemts Gulbenes novada pašvaldības (turpmāk – Pašvaldība) 2025. gada 22. oktobra iesniegums "Par Datu valsts inspekcijas 2025. gada 22. septembra lēmumu Nr. 2-2.2/42 "Par korektīvā līdzekļa piemērošanu" lietā Nr. L-2-6/5967[1] (*Inspekcijā reģistrēts 2025. gada 22. oktobrī ar Nr. 7-4.2/325-S*) (turpmāk – Sūdzība) ar kuru tiek apstrīdēts Inspekcijas 2025. gada 22. septembra lēmums Nr. 2-2.2/42 "Par korektīvā līdzekļa piemērošanu" (turpmāk – Lēmums).

[2] Izvērtējot Sūdzībā minēto un Inspekcijas rīcībā esošo informāciju, Inspekcija

konstatē:

[2.1.] 2024. gada 8. novembrī no Pašvaldības saņemts paziņojums par personas datu aizsardzības pārkāpumu. Saskaņā ar Sabiedrības ar ierobežotu atbildību "ZZ Dats", reģistrācijas numurs 40003278467 (turpmāk – SIA) sniegto informāciju Pašvaldībai, laika posmā no 2024. gada 29. oktobra līdz 2. novembrim nenoskaidrotām personām bija izdevies no vairākām interneta vietnēm nelikumīgi piekļūt Vienotās pašvaldību sistēmas (turpmāk – Sistēma) atsevišķām datubāzēm un iegūt šajās datubāzēs glabātos datus (turpmāk – Pārkāpums).

[2.2.] 2025. gada 29. janvārī Inspekcija Pašvaldībai nosūtīja vēstuli Nr. 2-4.2/110-N "*Par paziņojumu par personas datu aizsardzības pārkāpumu izskatīšanas virzību un pārbaudes uzsākšanu*", ar kuru Pašvaldība tika informēta par nolūku pārbaudīt SIA un pārziņu ieviesto tehnisko un organizatorisko pasākumu atbilstību Vispārīgās datu aizsardzības regulas[2] (turpmāk – Datu regula) prasībām un tika uzsākta personas datu apstrādes pārbaude[3], kuras ietvaros tika veikti uzraudzības pasākumi paziņojumos minēto notikumu apstākļu noskaidrošanai un vērtēta SIA un pārziņu sniegtā informācija par Pārkāpuma rašanās cēloņiem un rīcību pēc tā konstatēšanas.

[1] Gulbenes novada pašvaldības lietas Nr. 2-6/5957
[2] Eiropas Parlamenta un Padomes regula (ES) 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] Lieta Nr. L-2-6/5863

[2.3.] 2025. gada 12. februārī Inspekcija Pašvaldībai nosūtīja vēstuli Nr. 2-4.2/172-N "*Par pārbaudes uzsākšanu un informācijas pieprasījumu"*, ar kuru Pašvaldība informēta, ka pamatojoties uz Datu regulas 57. panta 1. punkta a) un h) apakšpunktu un Fizisko personu datu apstrādes likuma (turpmāk – Datu likuma) 4. panta 1. punktu ir uzsākusi pārbaudi[4] par Pārkāpumu, un SIA un pārziņu rīcības atbilstību Datu regulas 5. panta 2. punkta, 24., 28., 32. - 34. panta prasībām. Pamatojoties uz Datu regulas 58. panta 1. punkta e) apakšpunktu un Datu likuma 5. panta pirmās daļas 3. un 6. punktu, Inspekcija pieprasīja Pašvaldībai līdz 2025. gada 28. februārim rakstveidā izteikt savu viedokli par Pārkāpumu un sniegt atbildes uz uzdotajiem jautājumiem.

[2.4.] 2025. gada 28. februārī Inspekcijā saņemta Pašvaldības atbildes vēstule Nr. GND/4.21/25/642[5], ar kuru Pašvaldība sniedz atbildes uz Inspekcijas uzdotajiem jautājumiem.

[2.5.] Lietas materiālos atrodams 2025. gada 13. marta ziņojums Nr. 2-5.1/60 "Par pārbaudes lietas Nr. L-2-6/5863 sadalīšanu un slēgšanu", ar kuru konstatēts, ka 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.

[2.6.] 2025. gada 13. martā uzsākta pārbaudes lieta Nr. L-2-6/5957 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.

[2.7.] Izvērtējot lietā Nr. L-2-6/5957 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/atjaunināt 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.

[2.8.] 2025. gada 22. oktobrī Inspekcijā saņemta Sūdzība, kurā Pašvaldība nepiekrīt Lēmumā norādītajam, uzskata to par nepamatotu un lūdz:

1. Atcelt Datu valsts inspekcijas direktora vietnieces L. Dilbas 2025. gada 22. septembra lēmumu Nr. 2-2.2/42 "Par korektīvā līdzekļa piemērošanu", kurā nolemts Pašvaldībai izteikt rājienu.

[4] Pārbaudes Lieta Nr. L-2-6/5863
[5] Reģistrēta Inspekcijā 2025. gada 28. februārī ar Nr. 2-4.2/293-S

2. Izskaidrot Datu valsts inspekcijas direktora vietnieces L. Dilbas 2025. gada 22. septembra lēmuma Nr. 2-2.2/42 "Par korektīvā līdzekļa piemērošanu" nolemjošās daļas 2. punkta a) apakšpunktā Pašvaldībai uzlikto pienākumu.

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

secina:

[3.1.] Saskaņā ar Administratīvā procesa likuma (turpmāk – APL) 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 APL 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 lēmuma [1] punktā norādīto attiecībā uz Sūdzības saņemšanas dienu, Inspekcija secina, ka Sūdzība ir iesniegta termiņā, līdz ar to tās izskatīšana ir pieļaujama.

[3.3.] Pašvaldība nepiekrīt Inspekcijas Lēmumam un norāda šādus argumentus:

[3.3.1.] Pašvaldība norāda, ka Inspekcija Lēmuma 1.3.9. apakšpunktā un 3.7. apakšpunktos nepamatoti secinājusi, ka Pašvaldība nav nodrošinājusi pietiekamus uzraudzības un drošības pasākumus attiecībā uz apstrādātāja darbību.

[3.3.1.1.] Par prasībām attiecībā uz sistēmas drošību.

Pašvaldība norāda, ka gandrīz absolūti neievainojamas sistēmas izveide praksē nav iespējama – jebkura ar Sistēmu salīdzināmas sistēmas darbību nosaka tūkstošiem konfigurācijas elementu (operētājsistēmas, datu bāzes, aplikāciju servera, ugunsmūra, citu komponenšu konfigurācijas elementi), kas bieži ir savā starpā saistīti, tāpēc iespējamo konfigurāciju skaits, kurām būtu jāizveido "papildus kontrole", ir tuvs konfigurācijas elementu skaita faktoriālam. Šī iemesla dēļ nozīmīga konfigurāciju izlases pārbaudes neveikšana vai papildus pārbaužu neizveide nozīmīgam konfigurāciju skaitam nav Pašvaldības vai SIA darbība vai bezdarbība, bet gan objektīva situācija, savukārt savstarpējā līgumā noteikta prasība par kaut ko neiespējamu nav spēkā saskaņā ar Civillikuma 1543. pantu.

Direktores ieskatā Pašvaldības arguments par neiespējamu pilnību un konfigurāciju "faktoriāliem" ir tendenciozs un mēģina Inspekcijas prasības pasniegt kā ekstrēmas vai nesamērīgas. Taču, analizējot Lēmumu, konstatējams, ka Inspekcijas argumentācija ir balstīta uz riska – orientētu pieeju, kas ir Datu regulas pamatā, nevis uz absolūtisma principu. Arī visā Lēmuma tekstā tiek izmantots jēdziens "atbilstošs", kas ir nesavietojams ar jēdzienu "absolūts". Lēmumā arī atbilstības nodrošināšanai ir minētas standarta procedūras, kuras ir iespējams īstenot jebkuram: svarīgas izmaiņas (piemēram, ugunsmūra noteikumu maiņa) tiek plānotas un testētas kontrolētā veidā; "četru acu princips"; automatizētas konfigurācijas pārbaudes.

Direktore norāda, ka Lēmumā ir atsauce uz Datu regulas 32. panta 1. punktu, saskaņā ar kuru pārzinim un apstrādātājam ir pienākums ieviest atbilstošus tehniskos un organizatoriskos pasākumus, lai nodrošinātu drošības līmeni, kas atbilst riskam, ņemot vērā tehnikas līmeni, īstenošanas izmaksas, apstrādes raksturu, apmēru, kontekstu un nolūkus, kā arī riskus fizisku personu tiesībām un brīvībām. Proti, Datu regula neparedz pilnīgi absolūti nevainojamas sistēmas izveidi, bet gan paredz samērīgu drošību, kas atbilst riska līmenim. Pārzinim ir noteikts pienākums veikt tehniskus un organizatoriskus pasākumus, lai, cik vien iespējams, novērstu personas datu aizsardzības pārkāpumu. Šādu pasākumu piemērotība ir konkrēti jāizvērtē, pārbaudot, vai šis pārzinis pasākumus ir veicis, ņemot vērā minētajos pantos paredzētos dažādos kritērijus un ar attiecīgo apstrādi saistītās datu aizsardzības vajadzības, kā arī ar šo apstrādi saistītos riskus.[6] Proti, gan pārzinim, gan apstrādātajam ir jāspēj pamatot, ka ir veikti pasākumi, kas objektīvi samazina riskus līdz saprātīgam līmenim, ņemot vērā tehnoloģiju attīstības līmeni, datu veidu, to apstrādes raksturu u.tml.

Inspekcijas Lēmuma mērķis bija nevis norādīt, ka pašvaldībām ir jāizdara kaut kas neiespējams, proti, jāizveido informācijas sistēma, kas ir absolūti bez kļūdām, bet gan norādīt uz sistēmiskas un regulāras pārbaudes un uzraudzības trūkumu, kas jānodrošina pārzinim, uzraugot apstrādātāja darbību. Nenoliedzami, nav iespējams izveidot nevainojamu informācijas sistēmu un katra sistēma var saturēt noteiktu kļūdu skaitu, kas netraucē tās būtisko funkciju izpildi. Taču Lēmums par rājiena izteikšanu Pašvaldībai nav saistīts ar to, ka Pašvaldība neizveidoja absolūti drošu sistēmu, bet gan par to, ka Pašvaldība neizpildīja tai Datu regulā noteiktās pārziņa funkcijas.

[3.3.1.2.] Par Civillikuma 1543. panta piemērošanu.

Pašvaldības atsauce uz Civillikuma 1543. pantu, kas attiecas uz neiespējama pienākuma saistību spēkā neesamību, šajā gadījumā nav piemērojama. Inspekcija Pašvaldībai nav uzlikusi pienākumu nodrošināt absolūtu sistēmas drošību vai veikt pilnīgu konfigurāciju pārbaudi. Inspekcija noteica samērīgus pienākumus – pārskatīt un uzlabot uzraudzības mehānismus un aktualizēt risku novērtējumu, kas atbilst Datu regulas 24. un 32. pantam. Līdz ar to Pašvaldības atsauce uz Civillikumu kļūdaini interpretē Lēmuma būtību un ir noraidāma kā nepamatota.

[3.3.1.3.] Par resursu trūkumu.

Pašvaldība norāda, ka tai nav tehnisko un administratīvo resursu Inspekcijas norādītās uzraudzības veikšanai. Tāpēc Pašvaldībai faktiski nav citu iespēju, kā paļauties uz attiecīgu speciālistu, kuri veikuši SIA drošības auditus un ISO sertifikāciju, novērojumiem.

Ar šo argumentu Pašvaldība būtībā nonāk pretrunās, jo no vienas puses apgalvo, ka uzraudzība vispār nav iespējama, no otras – tā nav iespējama resursu trūkuma dēļ. Saskaņā ar Datu regulas 5. panta 2. punktu tieši pārzinis ir atbildīgs par personas datu aizsardzību, pat ja apstrādi veic cits uzņēmums (*apstrādātājs*). Resursu vai tehnisko zināšanu trūkums nevar būt pamats, lai pārzini atbrīvotu no atbildības. Gluži pretēji, ja pārzinis apzinās savu nekompetenci, tam ar vēl lielāku rūpību ir jāizvēlas apstrādātājs un jāveltī uzmanība atbilstoša līguma noslēgšanai.

Eiropas Savienības Tiesa (turpmāk – Tiesa) lietās Nr. C-340/21 un Nr. C-683/21 atzinusi, ka pārzinis saglabā atbildību arī tad, ja apstrādi faktiski veic cits subjekts (piemēram, apstrādātājs), ja vien pārzinis ir noteicis apstrādes nolūkus un līdzekļus vai var tos ietekmēt. Pārzinim ir jāpierāda, ka tas ir ieviesis un uztur efektīvu uzraudzības mehānismu pār apstrādātāju, nevis tikai formāli paļāvies uz apstrādātāja sniegtajām garantijām. Šī judikatūra apstiprina, ka pārziņa atbildība nevar tikt izslēgta ar norādi uz tehniskām grūtībām vai sistēmas sarežģītību.

[6] Skat. EST spriedums lietā Nr. C-340/21 "VB pret *Natsionalna agentsia za prihodite",* 30. punkts

Pašvaldības arguments, ka tai nav citu iespēju kā paļauties, ir pretrunā Datu regulā noteiktajai pārziņa lomai. Pārziņa pienākums ir ievērot principu "uzticies, bet pārbaudi", kurpretim Pašvaldība ir piemērojusi principu "uzticies akli", kas ir tiešs pārskatatbildības principa pārkāpums.

[3.3.2.] Pašvaldība norāda, ka Lēmumā nav norādīts, vai Inspekcijas 2025. gada 23. jūlija lēmums Nr. 01630000100325-3 pārbaudes lietā Nr. L-2-6/5930 ir kļuvis neapstrīdams. Saskaņā ar publiski pieejamo informāciju Inspekcijas mājas lapā[7] informācija par iepriekš minēto Inspekcijas lēmumu nav publicēta, līdz ar to Pašvaldība pieņem, ka šāds lēmums nav kļuvis neapstrīdams, bet ir ticis apstrīdēts un/vai pārsūdzēts. Ņemot vērā, ka šis lēmums var tikt atcelts, Inspekcijai nav tiesiska pamata Lēmumā atsaukties uz administratīvo aktu, kurš nav kļuvis neapstrīdams.

Visupirms Inspekcijas direktore paskaidro, ka Inspekcijas 2025. gada 23. jūlija lēmums Nr. 01630000100325-3 pārbaudes lietā Nr. L-2-6/5930 nav administratīvais akts administratīvā procesa ietvaros, bet gan lēmums administratīvā pārkāpuma procesa ietvaros.

Neatkarīgi no minētā lēmuma spēkā stāšanās, nav apstrīdams fakts, ka ir noticis datu aizsardzības pārkāpums. Inspekcija uz SIA Lēmumu atsaucās, lai norādītu, ka ir pierādīts fakts, ka incidents vispār ir noticis. Neviena no iesaistītajām pusēm līdz šim nav noliegusi to, ka šāds incidents tiešām ir noticis, un kura rezultātā laika posmā no 2024. gada 29. oktobra līdz 2. novembrim nenoskaidrotām personām bija izdevies no vairākām interneta vietnēm nelikumīgi piekļūt SIA informācijas sistēmu datu bāzēm. Attiecīgi atsauce uz šo lēmumu tika veikta, lai norādītu uz konkrētu faktu, kas ir noticis un ko nav iespējams atcelt, nevis uz lēmumā izdarīto juridisko analīzi. Līdz ar to iebildums, ka Inspekcija nevarēja atsaukties uz minēto lēmumu, nav pamatots, jo konkrētais lēmums netika izmantots kā pierādījums pašvaldības rīcībai, bet gan kā atsauce uz faktu, kas ir noticis.

Tāpēc Inspekcijas direktore secina, ka šis arguments nav pamatots, jo Pašvaldībai korektīvais līdzeklis tika piemērots tāpēc, ka Pašvaldība neizpildīja attiecīgus kontroles un uzraudzības pasākumus, kas tai bija jānodrošina atbilstoši Datu regulai.

[3.3.3.] Pašvaldība norāda, ka, izvēloties SIA kā apstrādātāju, tā ir ievērojusi Datu regulas 28. panta 1. punktu, jo apstrādātājs sniedz pietiekamas garantijas, kas apliecinātas ar spēkā esošajiem ISO 9001 un ISO/IEC 27001 sertifikātiem. Šie sertifikāti, Pašvaldības ieskatā, nodrošina, ka apstrādātājs ir veicis risku novērtēšanu, ieviesis atbilstošus tehniskos un organizatoriskos pasākumus un tiek regulāri auditēts. Tādēļ Inspekcijas secinājums, ka Pašvaldība neesot nodrošinājusi apstrādātāja uzraudzību, esot nepamatots.

Nenoliedzami, ka ISO 27001 sertifikāts ir starptautiski atzīts standarts informācijas drošības pārvaldības sistēmām, kas apliecina, ka organizācija ir ieviesusi sistēmisku un efektīvu pieeju informācijas drošības riska pārvaldībai, kas nodrošina konfidencialitāti, integritāti un pieejamību tās pārvaldītajai informācijai[8]. Vienlaikus šāda sertifikāta esamība pakalpojuma sniedzējam tikai norāda uz viņa ieviestajiem informācijas pārvaldības sistēmas drošības risinājumiem, taču neatceļ pārziņa pienākumus uzraudzīt apstrādātāja darbību, kā arī nenozīmē, ka apstrādātājs izpilda visas Datu regulā noteiktās prasības. Papildus jāņem vērā, ka ISO sertifikāts apliecina, ka apstrādātājam ir izveidota sistēma un pastāv procesi, bet tas negarantē, ka darbinieki šos procesus izpilda. Konkrētajā gadījumā pārkāpums ir radies, nevis tāpēc, ka nepastāvēja procesi, ko garantē ISO sertifikāts, bet gan izpildes kļūdas, kontroles trūkuma rezultātā.

Turklāt pašvaldības arguments par to, ka sertifikācija pati par sevi dod pārliecību, ka apstrādātājs ir uzticams un nodrošina datu aizsardzību, neiztur kritiku, jo pārkāpums notika, neskatoties uz sertifikāta esamību. Līdz ar to atsaukšanās uz ISO sertifikātu kā pietiekamu garantiju

[7] https://www.dvi.gov.lv/lv/lemumi
[8] Informācija pieejama - https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27001:ed-3:v1:en

neatbilst riskā balstītas pieejas principam un neatbilst Datu regulas mērķim nodrošināt faktisku, nevis formālu atbilstību.

Lai arī Pašvaldība pati atsaucas uz Datu regulas 81. apsvērumu, kas paredz, ka sertifikāciju var izmantot kā elementu, ar ko uzskatāmi parāda pienākumu izpildi, pašā argumentācijā šī apsvēruma punkta atslēgas vārds "kā elementu" tiek ignorēts. Proti, sertifikācija var būt viens no pierādījumiem, nevis pilnīgs pārziņa atbrīvojums no atbildības. Sertifikācija automātiski nepadara pārziņa rīcību par atbilstošu Datu regulas prasībām. Turklāt būtu norādāms, ka Datu regulas 81. apsvērums paskaidro Datu regulas 28. panta 5. punktu, kurā ir skaidras norādes uz Datu regulas 40. pantu un 42. pantu. Līdz ar to termins "sertifikācijas mehānisms" attiecās uz Datu regulas 42. pantā noteikto sertifikācijas mehānismu. Un minētais mehānisms nav ISO sertifikāts.

No Datu regulas 28. panta 1. punkta izriet pārziņa pienākums izmantot tikai tādus apstrādātājus, kas sniedz pietiekamas garantijas, ka tiks īstenoti atbilstoši tehniskie un organizatoriskie pasākumi tādā veidā, ka apstrādē tiks ievērotas Datu regulas prasības. Eiropas Datu aizsardzības kolēģijas (turpmāk – EDPB) Pamatnostādnēm 07/2020[9] ir noteikts, ka "pienākums izmantot tikai tādus apstrādātājus, kuri "sniedz pietiekamas garantijas", kas iekļauts Datu regulas 28. panta 1. punktā, ir pastāvīgs pienākums. Tas nebeidzas brīdī, kad pārzinis un apstrādātājs noslēdz līgumu vai citu juridisku dokumentu. Pārzinim drīzāk ir atbilstīgos intervālos jāpārbauda apstrādātāja sniegtās garantijas, tostarp vajadzības gadījumā veicot revīzijas un pārbaudes."[10] Šo pieeju apliecina arī Tiesas spriedumi, kuros Tiesa norāda, ka pārzinim ir jāspēj pierādīt, ka tas reāli ietekmē un kontrolē apstrādes līdzekļus un apstākļus[11].

Inspekcijas Lēmuma 3.4. un 3.5. apakšpunktā jau norādīts, ka Pašvaldība nav paredzējusi līgumiskus vai organizatoriskus mehānismus, kas ļautu tai faktiski pārliecināties par apstrādātāja darbību (piemēram, audita rezultātu pieprasīšanu, atskaišu saņemšanu par ugunsmūra konfigurāciju vai izmaiņām sistēmā). Līdz ar to Inspekcijas direktore secina, ka apstrādātāja uzraudzība tika aizstāta ar formālu paļaušanos uz ISO sertifikātiem, kas neatbilst Datu regulas 5. panta 2. punktā nostiprinātajam pārskatatbildības principam, kā arī Datu regulas 28. panta 1. un 2. punktā pārzinim noteiktajām prasībām.

[3.3.4.] Attiecībā par Pašvaldības norādi, ka apstrādātāja auditus un risku analīzi veikušas citas pašvaldības (piemēram, Liepājas un Jūrmalas), Inspekcijas direktore norāda, ka šāda pieeja neatbrīvo no pārziņa pienākuma personīgi pārliecināties par apstrādes atbilstību. Katra pašvaldība ir patstāvīgs pārzinis attiecībā uz saviem datiem (Datu regulas 4. panta 7. punkts), līdz ar to arī ir individuāli atbildīga par savu apstrādes procesu. Citi pārziņi var sniegt informatīvu pamatojumu, bet viņu veiktais audits nevar aizstāt pārziņa paša veikto izvērtējumu. Turklāt, Jūrmalas pašvaldības 2023.gadā veiktajā auditā tika identificēti vērā ņemami informācijas drošības riski, savukārt no Pašvaldības nav informācijas kā un vai ir sekojusi kāda rīcība šo risku mazināšanai.

Papildus tam katra pašvaldība var veikt VPS konfigurāciju, pielāgojot to atbilstoši savām vajadzībām un saviem apstrādes nolūkiem, piemēram, izvēlētos attiecīgos sistēmas moduļus, pašvaldībām var būt piešķirtas atšķirīgas piekļuves tiesības noteikta veida personālam, kā arī sistēmas lietotāju skaits katrā pašvaldībā var būtiski atšķirties. Tāpēc pat, ja dažādas pašvaldības izmanto vienu un to pašu sistēmu, to organizatoriskie procesi, risinājumi un riska līmeņi var atšķirties. Arī Datu regulas 32. panta 1. punkts kopsakarā ar Datu regulas 5. panta 2. punktu

---

[9] Eiropas Datu aizsardzības kolēģijas 2020. gada jūlija pamatnostādnes 07/2020 par pārziņa un apstrādātāja jēdzieniem VDAR (turpmāk – Pamatnostādnes 07/2020)

[10] Skat. Eiropas Datu aizsardzības kolēģijas 2020. gada jūlija pamatnostādnes 07/2020 par pārziņa un apstrādātāja jēdzieniem VDAR. Pieejamas: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_en

[11] Skatīt Tiesas 2023. gada 14. decembra spriedums lietā Nr. C-340/21 un 2023. gada 5. decembra spriedums lietā Nr. C-683/21

nosaka, ka pienākums īstenot personas datu aizsardzības pasākumus ir attiecināms uz katru pārzini atsevišķi.

Informācija, kas neformāli iegūta asociācijas sanāksmē par to, ka cita juridiska persona ir veikusi auditu, nav juridiski saistošs pierādījums, ko Pašvaldība var uzrādīt, lai pierādītu savu pienākumu izpildi. Ja sekotu Pašvaldības loģikai, līdzīgi varētu secināt, ka nav nepieciešams iziet tehnisko apskati automašīnai, ja tās pašas markas, modeļa un izlaiduma automašīnai tehnisko apskati nesenā pagātnē izgājis kaimiņš.

Direktore piekrīt, ka neviens normatīvais akts nenosaka konkrētu audita biežumu, tieši tādēļ pārzinim pašam jāspēj pamatot, kāpēc tā izvēlētais audita biežums ir atbilstošs riskam. Lēmums neveikt nekādu kontroli, jo kāds cits to ir darījis, nav uzskatāms par riskā balstītu un atbilstošu Datu regulai.

Ņemot vērā minēto, direktore uzskata, ka Pašvaldība, paļaujoties tikai uz ISO sertifikātiem un citu pašvaldību veikto auditu rezultātiem, kuros tika konstatēti drošības riski, nav veikusi pietiekamus pasākumus, lai uzskatāmi pierādītu savu atbildību par apstrādi, kā to prasa Datu regulas 5. panta 2. punkts un 24. panta 1. punkts.

[3.3.5.] Pašvaldība norāda, ka nav nozīmes tam, vai apstrādātāja pārbaudi veic pats pārzinis vai kāda cita persona, ja vien pārbaudes gaitā tiek konstatēta apstrādes atbilstība Datu regulas prasībām. Pašvaldības ieskatā būtisks ir pārbaudes saturs un secinājumi, nevis tās veicējs.

Saskaņā ar Datu regulas 28. panta 3. punkta h) apakšpunktu, pārziņa tiesības pārbaudīt apstrādātāju var īstenot ne tikai pats pārzinis, bet arī jebkurš pārziņa pilnvarots revidents. Tas nozīmē, ka pārbaudes veikšanai jābūt juridiski pamatotai ar pilnvaru vai līgumu, kas apliecina, ka konkrētā persona darbojas pārziņa vārdā un uzdevumā.

Inspekcijas direktore norāda, ka Pašvaldības argumentācija ir pretrunīga, jo tā vienlaikus atzīst nepieciešamību nodrošināt atbilstošu kontroli pār apstrādātāju, bet tajā pašā laikā atsaucas uz citu iestāžu vai juridisku personu veiktajām pārbaudēm, nesniedzot pierādījumus, ka šie subjekti būtu rīkojušies kā pārziņa pilnvaroti revidenti.

Lai Pašvaldība varētu atsaukties uz citu iestāžu veiktajiem auditiem kā pierādījumu savas uzraudzības pienākuma izpildei, tai būtu jāuzrāda dokumenti, kas apliecina, ka šīm personām ir deleģētas tiesības pārbaudīt apstrādātāju Pašvaldības vārdā. Ja šāds pilnvarojums nav sniegts, tad šie auditi nav uzskatāmi par pārziņa veikto pārbaudi Datu regulas izpratnē un nevar kalpot kā pierādījums pārziņa atbildības izpildei.

[3.3.6.] Pašvaldība norāda, ka SIA personas datu apstrādes procesā rīkojies neatkarīgi un faktiski noteicis apstrādes līdzekļus, tādēļ uzskatāms par pārzini Datu regulas izpratnē.

[3.3.6.1.] Par personas datu apstrādes nolūku.

Saskaņā ar Datu regulas 4. panta 7. punktu, par pārzini uzskatāma persona, kas nosaka apstrādes nolūkus un līdzekļus, savukārt, atbilstoši 4. panta 8. punktam, apstrādātājs apstrādā datus pārziņa uzdevumā. No lietas materiāliem neizriet, ka SIA būtu izmantojis personas datus saviem nolūkiem vai noteicis jaunu apstrādes mērķi. SIA darbība bija vērsta uz esošās Sistēmas uzturēšanu un tehnisko darbību nodrošināšanu. Arī meklēšanas indeksa ieviešana un konfigurēšana tika veikta nolūkā nodrošināt sistēmas funkcionalitāti un datu pieejamību Pašvaldības funkciju īstenošanai — tas ir Pašvaldības noteiktais apstrādes nolūks.

Kā izriet no EDPB Pamatnostādnēm 07/2020[12], izšķirošais kritērijs ir apstrādes nolūks, nevis apstrādes tehniskā realizācija — ja apstrādātājs veic darbības, lai īstenotu pārziņa noteiktu mērķi, tas saglabā apstrādātāja statusu pat tad, ja izvēlas konkrētus tehniskus risinājumus apstrādes nodrošināšanai

Tādējādi SIA rīcība atspoguļo tehnisku kļūdu pārziņa uzdevuma ietvaros, nevis patstāvīgu datu apstrādi ar neatkarīgu mērķi. Konkrētajā situācijā SIA neveica personas datu apstrādi saviem nolūkiem, bet gan atbilstoši Pašvaldības noteiktajiem personas datu apstrādes nolūkiem, izvēlējās jaunus tehniskos risinājumus personas datu apstrādei, taču joprojām apstrādāja datus Pašvaldības noteiktajā nolūkā, tāpēc saglabājas Pašvaldības kā pārziņa atbildība par notikušo Pārkāpumu. Datu regulas 28. panta 10. punkts, uz kuru atsaucas Pašvaldība, paredz, ka apstrādātājs kļūst par pārzini tikai tad, ja pats nosaka apstrādes nolūkus un līdzekļus, rīkojoties ārpus pārziņa deleģētā uzdevuma. Šajā gadījumā šādu apstākļu nav, jo apstrāde joprojām tika veikta Pašvaldības definētā nolūka ietvaros.

[3.3.6.2.] Par apstrādes līdzekļiem.

Attiecībā uz apstrādes līdzekļiem norādāms, ka atbilstoši EDPB Pamatnostādnēs 07/2020 norādītajam var izšķirt būtiskos un nebūtiskos līdzekļus. "Būtiskie līdzekļi" tradicionāli un pēc būtības tiek rezervēti pārzinim. Nebūtiskos līdzekļus var noteikt arī apstrādātājs. "Būtiskie līdzekļi" ir līdzekļi, kas ir cieši saistīti ar apstrādes nolūku un apjomu, piemēram, apstrādājamo personas datu veids ("kādi dati tiks apstrādāti?"), apstrādes ilgums ("cik ilgi tie tiks apstrādāti?"), saņēmēju kategorijas ("kam būs piekļuve tiem?") un datu subjektu kategorijas ("kuru subjektu personas dati tiek apstrādāti?"). Būtiskie līdzekļi, tāpat kā apstrādes nolūks, ir cieši saistīti arī ar jautājumu par to, vai apstrāde ir likumīga, nepieciešama un samērīga. "Nebūtiskie līdzekļi" attiecas uz praktiskākiem īstenošanas aspektiem, piemēram, uz konkrēta aparatūras vai programmatūras veida izvēli vai detalizētiem drošības pasākumiem, kurus var atstāt apstrādātāja ziņā.[13]

Tā kā SIA nodrošina sistēmas uzturēšanas pakalpojumu pašvaldībām, no iepriekš minētā var secināt, ka tā nosaka nebūtiskos līdzekļus, tostarp arī meklēšanas indeksa risinājuma ieviešanu.

[3.3.6.3.] Par pārziņa pienākumiem attiecībās ar apstrādātāju.

Inspekcijas direktore uzsver, ka pārziņa atbildība par apstrādes atbilstību neizbeidzas ar līguma noslēgšanu ar apstrādātāju. Atbilstoši Datu regulas 5. panta 2. punktam un 24. panta 1. punktam, pārzinim ir pienākums spēt pierādīt, ka apstrāde notiek saskaņā ar Datu regulu, tostarp nodrošinot atbilstošu uzraudzību pār apstrādātāja darbībām. Tas ietver arī pienākumu pārliecināties par apstrādātāja īstenotajiem tehniskajiem un organizatoriskajiem pasākumiem un par to, vai līguma ietvaros paredzētas pietiekami efektīvas kontroles un ziņošanas procedūras.

Vienreizējs drošības risku novērtējums nenodrošina pastāvīgu kontroli. Proti, Datu regulas 28. pants paredz, ka pārzinim jāizvēlas apstrādātājs, kas "sniedz pietiekamas garantijas". Kopsakarā ar pārziņa pārskatatbildības principu, pārzinim jāpārliecinās par apstrādātāja atbilstību regulāri – ne tikai līguma noslēgšanas brīdī. Vienreizējs drošības novērtējums, kas veikts līguma noslēgšanas sākumā vai konkrētā brīdī, neatspoguļo apstrādātāja turpmāko darbību, izmaiņas sistēmās vai riska līmeni. Tādēļ šādu novērtējumu nevar uzskatīt par pietiekamu pastāvīgas kontroles un uzraudzības mehānisma pierādījumu. Minēto apliecina arī EDPB Pamatnostādnēs 07/2020 norādītais, proti, ka pienākums izmantot tikai tādus apstrādātājus, kuri "sniedz

[12] Skat. Eiropas Datu aizsardzības kolēģijas 2020. gada jūlija pamatnostādnes 07/2020 par pārziņa un apstrādātāja jēdzieniem VDAR. Pieejamas: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_en

[13] Skat. Eiropas Datu aizsardzības kolēģijas 2020. gada jūlija pamatnostādnes 07/2020 par pārziņa un apstrādātāja jēdzieniem VDAR. Pieejamas: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_en

pietiekamas garantijas", kas iekļauts Datu regulas 28. panta 1. punktā, ir pastāvīgs pienākums. Tas nebeidzas brīdī, kad pārzinis un apstrādātājs noslēdz līgumu vai citu juridisku dokumentu. Pārzinim drīzāk ir atbilstīgos intervālos jāpārbauda apstrādātāja sniegtās garantijas, tostarp vajadzības gadījumā veicot revīzijas un pārbaudes.

Līdz ar to Inspekcijas direktore nevar piekrist Pašvaldības norādījumam, ka tā nevar uzņemties katra darbinieka fizisku uzraudzību, jo tas būtu pretrunā lomu sadalījumam.

Lēmumā netika ietverta prasība veikt fizisku uzraudzību vai nodarboties ar mikromenedžmentu. Ar Lēmumu tika konstatēts, ka Pašvaldība nebija ieviesusi standarta procedūras – noslēgusi Datu regulai atbilstošu līgumu, kurā būtu skaidri aizliegts apstrādātājam ieviest jebkādus jaunus, būtiskus apstrādes līdzekļus bez rakstiskas pārziņa piekrišanas, kā arī nodrošinājusi sev audita un pārbaudes tiesības, lai periodiski pārbaudītu, kādus tehniskos līdzekļus apstrādātājs izmanto.

Ņemot vērā [3.3.6.] punktā iekļauto informāciju, Inspekcijas direktore norāda, ka pārbaudē pret SIA notikušo personas datu apstrādes pārkāpumu netika konstatēts, ka SIA būtu darbojies kā pārzinis, tādēļ Pašvaldības argumentācija par apstrādātāja statusa pārtapšanu par pārzini ir nepamatota, un Inspekcijas direktore atzīst korektīvā līdzekļa piemērošanu par tiesisku un samērīgu, jo tā vērsta uz pārziņa pienākumu pienācīgu izpildi nākotnē. Apstrāde notika Pašvaldības uzdevumā, lai nodrošinātu informācijas sistēmas darbību, un kļūda radās tehniskas neprecizitātes dēļ, nevis nolūkā izmantot datus neatkarīgi.

Ņemot vērā minētos faktiskos un tiesiskos apstākļus, pamatojoties uz Datu regulas 4. panta 7., 8. punktu, 5. panta 2. punktu, 24. panta 1. punktu, 28. panta 1., 2. un 3. punkta h) apakšpunktu, 32. panta 1. punktu, Civillikuma 1543. pantu, 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. 2-2.2/42.

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].

Par Sūdzībā ietverto lūgumu skaidrot Lēmuma nolemjošās daļas 2. punkta a) apakšpunktu

[1] Attiecībā uz Pašvaldības Sūdzībā minēto lūgumu izskaidrot Lēmuma nolemjošās daļas 2. punkta a) apakšpunktā Pašvaldībai uzlikto pienākumu, Inspekcija paskaidro, ka šāds uzlikts tiesiskais pienākums nozīmē, ka Pašvaldības kā pārziņa, kas veic personas datu apstrādi, rīcībā tika

konstatēti trūkumi personas datu aizsardzības efektīvā nodrošināšanā, un šos trūkumus nepieciešams novērst, ieviešot iekšējos personas datu apstrādes procesus un noteikumus vai pārskatot un veicot nepieciešamās korekcijas jau esošajos procesos un noteikumos, kā arī noslēdzot līgumu (vienošanos) ar apstrādātāju par personas datu apstrādes jautājumiem, lai Pašvaldības rīcībā tiktu īstenotas Datu regulas prasības. Šis pienākums pēc būtības sevī ietver gan preventīvus, gan korektīvus pasākumus, kas vērsti uz atbilstības atjaunošanu, lai novērstu ne tikai konstatētos pārkāpumus, bet arī samazinātu riskus nākotnē, jo īpaši ņemot vērā, ka dažādas publiskās varas iestādes un privāti uzņēmumi (t.sk. apstrādātāji vai citi pašvaldības funkciju izpildei piesaistītie partneri) arvien vairāk ik dienas tiek pakļauti dažādiem kibernoziegumu riskiem.

[2] Šajā ziņā Inspekcija norāda, ka tikai un vienīgi **pati Pašvaldība – kā pārzinis, kas patstāvīgi nosaka personas datu apstrādes nolūkus un līdzekļus** – zina, kādu personas datu apstrādi tai nepieciešams veikt, kādā nolūkā, uz kāda tiesiskā pamata un ar kādiem pasākumiem, piemēram, konkrētiem iekšējiem dokumentiem vai procesu aprakstiem tā spēj praktiski un efektīvi nodrošināt šo procesu atbilstību Datu regulas prasībām. Inspekcija vērš uzmanību, ka tā nav Pašvaldības veiktās personas datu apstrādes pārzinis, un tādēļ Inspekcija nevar Pašvaldības vietā noteikt piemērotākos pasākumus, kas Pašvaldībai būtu faktiski īstenojami, vai konkrētus izstrādājamos dokumentus.

Proti, Inspekcija kā personas datu uzraudzības iestāde nevar noteikt pārziņa vietā, kas ir vai nav pietiekami, tomēr ir būtiski, ka Pašvaldībai ir izstrādāti tai nepieciešamie procesu apraksti, no kuriem loģiski saprotams, kā notiek personas datu apstrāde un ir jābūt skaidrai kārtībai, kā rīkoties dažādās situācijās vai, ja iestājas riski. Pašvaldībai arī jānodrošina, ka darbinieki praksē un realitātē zina noteiktas prasības un procesus un izpilda tos. Tādējādi, piemēram, pārzinim ir pienākums vest datu apstrādes reģistru, kurā iekļauta Datu regulas 30. pantā minētā informācija, taču reģistra formai nav izšķirošas nozīmes (tas var būt elektroniskais rīks, Excel tabula u.tml.), kā arī pārliecināties, ka tās iekšējās kārtībās ir paredzēts, kā Pašvaldība praktiski īsteno un nodrošina atbilstību Datu regulas 24., 25., 28., 32., 33., 34. panta prasībām.

Lai izpildītu Lēmumā uzlikto tiesisko pienākumu, Pašvaldībai pašai ir jāizvērtē un jāsaprot, **konsultējoties ar savu datu aizsardzības speciālistu**, kādas darbības tai būtu jāveic un ko tā uzskata par atbilstošu, lai novērstu Lēmumā konstatētos pārkāpumus un saprātīgā apjomā nodrošinātu, ka tie neatkārtojas nākotnē un līdz minimumam tiek samazināts datu subjektu tiesībām un brīvībām radītais kaitējums. Kā jau minēts, Inspekcija šajā gadījumā **nevar sniegt visaptverošu un konkrētu skaidrojumu par Pašvaldībai īstenojamiem pasākumiem saistībā ar tās veikto datu apstrādi kopumā vai, cik detalizētiem jābūt noslēgtajiem personas datu apstrādes līgumiem ar apstrādātājiem vai citiem koppārziņiem vai sadarbības partneriem**.

[3] Vienlaikus, lai sniegtu lielāku skaidrību Pašvaldībai, attiecībā uz aspektiem, kas jāņem vērā, izpildot Lēmumā noteikto pienākumu, norādām turpmāko.

[3.1.] Inspekcijas uzliktais pienākums pārskatīt personas datu apstrādes noteikumus nozīmē, ka Pašvaldībai ir jāizvērtē un jāatjauno (jāprecizē vai jāpapildina) iekšējie dokumenti un procesi, kas ir saistīti ar personas datu apstrādi. Tas jo īpaši ietver pienākumu Pašvaldībai pārbaudīt, vai ir izstrādāti visi nepieciešamie iekšējie noteikumi (piemēram, personas datu apstrādes noteikumi, personas datu drošības politika, IT drošības noteikumi un incidentu reaģēšanas procedūra, novērtējums par ietekmi uz riskiem personas tiesībām un brīvībām, personas datu pārkāpumu pārvaldības procedūra, datu subjekta tiesību īstenošanas kārtība u.c.[14]) un tie atbilst Datu regulas prasībām, un vai Pašvaldībai ir skaidrs, kā ikdienā un jo īpaši konstatētu incidentu gadījumos tie tiek praktiski īstenoti.

Ja šie dokumenti un procesu apraksti ir novecojuši vai nepilnīgi (piemēram, neietver

[14] Minētais piemēru uzskaitījums nav obligāts, bet gan atkarīgs no pašas Pašvaldības lēmuma, kādus noteikumus tai nepieciešams izstrādāt, un kādā formā vai dokumentā tie ietverami.

faktiskai situācijai atbilstošu informāciju par iekšējo informācijas sistēmu, mākoņpakalpojumu vai mākslīgā intelekta izmantošanu), tie jāatjauno, lai skaidri un precīzi noteiktu datu apstrādes mērķus, tiesiskos pamatus, definētu darbinieku piekļuves tiesības, atbildības apjomu un lomu sadalījumu starp darbiniekiem vai attiecīgos gadījumos trešām pusēm (piemēram, apstrādātājiem, audita uzņēmumiem, citām struktūrvienībām), un paredzētu Pašvaldības regulāri, ikgadēji vai pēc nepieciešamības veicamos preventīvos drošības pasākumus – gan tehniskus, gan organizatoriskus, piemēram, darbinieku apmācības, sistēmu auditi, drošības testu un pārbaužu veikšana u.c.

[3.2.] Ja Pašvaldībai vēl nav izstrādāts (vai ir nepilnīgs), tad jāizstrādā process, kādā ir veicams personas datu apstrādes risku novērtējums un/vai novērtējums par ietekmi uz riskiem personas tiesībām un brīvībām, kā arī attiecībā uz personas apstrādi, kas ir norādīta Datu regulas 35.pantā, būtu jāizstrādā novērtējums par ietekmi (turpmāk – NIDA). Katrā NIDA jāapraksta, kāda veida dati tiek apstrādāti (piemēram, iedzīvotāju dati, veselības dati, skolēnu/nepilngadīgu personu dati, biometrijas dati vai citi sensitīvi dati), kādi apdraudējumi pastāv (nesankcionēta piekļuve, datu zudums, ļaunprātīga izmantošana utt.), vai šie riski ir uzskatāmi par maznozīmīgiem vai nozīmīgiem (augstiem), un kādi pasākumi ir veicami, lai šos riskus mazinātu. Šim nolūkam iespējams izmantot Inspekcijas izstrādātās vadlīnijas par NIDA izstrādi vai citu iestāžu sniegtās vadlīnijas, piemēram, Eiropas Savienības Kiberdrošības aģentūras vadlīnijas "*Recommendations for a methodology of the assessment of severity of personal data breaches*"[15]. Attiecīgi Pašvaldībai ir jābūt izstrādātai un noteiktai kārtībai jeb noteikumiem, kuros paredzēti un izdalīti dažādi riski, un skaidrots, kā tos izvērtēt, kādas ir potenciālās sekas un kā tās iespējams mazināt.

[3.3.] Tāpat Pašvaldībai jāpārliecinās, vai ir izstrādāta skaidra incidentu reaģēšanas kārtība vai procedūra, nosakot katra atbildīgā darbinieka pienākumus un atbildību, kā rīkoties, ja ir noticis incidents vai **personas datu aizsardzības pārkāpums**. Šajā kārtībā jo īpaši jāparedz: kā notiek incidenta identificēšana un dokumentēšana; kurš un kam ziņo organizācijas iekšienē vai sadarbības partneriem, un kurš un kad ziņo Inspekcijai; un kā tiek novērtētas pārkāpuma sekas un informēti datu subjekti, ja tas nepieciešams.

[3.4.] Attiecībā uz Lēmumā noteikto pienākumu noslēgt atbilstošu datu apstrādes līgumu ar apstrādātāju ZZ Dats, Inspekcija norāda, ka šis pienākums izriet no Datu regulas 28. panta, kas būtībā paredz, ka pārziņa un apstrādātāja attiecības regulē līgums vai cits juridisks akts, kas ir saistošs abām līgumslēdzēja pusēm. Inspekcija norāda, ka tā nevērtē noslēgtā līguma atbilstību pēc būtības Pašvaldības faktiskajai situācijai, bet gan tikai Lietas tvēruma kontekstā vērtējot, vai šāds līgums pastāv un vai tajā ir ietverts viss Datu regulas 28. pantā minētais, ņemot vērā, ka konkrētajā gadījumā dokuments, uz ko Pašvaldība atsaucās paskaidrojumos, nesaturēja visu nepieciešamo informāciju, ko prasa Datu regula. Pašvaldības ziņā ir izvērtēt, kur tās apstrādē un sadarbībā ar ārējiem pakalpojumu sniedzējiem ir konstatējami trūkumi un kā tos novērst, un cik detalizētam jābūt līgumam, ievērojot riskus un esošo pieredzi saistībā ar notikušo Pārkāpumu.

Inspekcija norāda, ka šajā līgumā (vienošanās dokumentā) ir obligāti jābūt ietvertiem tādiem nosacījumiem, kas ļauj pārliecināties par Pašvaldības kā pārziņa (un ZZ Dats kā apstrādātāja) Datu regulā paredzēto pienākumu izpildi, jo īpaši nosakot: 1) līguma un apstrādes priekšmetu, 2) apstrādes ilgumu, 3) apstrādes raksturu un nolūku, 4) personas datu veidu un datu subjektu kategorijas, 5) pārziņa pienākumus un tiesības, piemēram, apstrādāt datus tikai saskaņā ar pārziņa norādījumiem, nodrošināt konfidencialitāti, īstenot atbilstošus drošības pasākumus (Datu regulas 32. pants), palīdzēt pārzinim izpildīt datu subjektu tiesību pieprasījumus, ziņot par datu aizsardzības pārkāpumiem, dzēst vai atdot datus pēc līguma beigām, neiesaistīt citus apstrādātājus vai apakšapstrādātājus bez pārziņa atļaujas, 6) drošības pasākumu aprakstu, kas nodrošina datu aizsardzībai atbilstošu līmeni (tehniski un organizatoriski).

[15] https://www.enisa.europa.eu/publications/dbn-severity

Šāda līguma vai vienošanās mērķis ir panākt, ka Pašvaldība zina, izpilda un nepārkāpj savas kā pārziņa saistības un varētu pārliecināties, ka ārējais pakalpojumu sniedzējs (apstrādātājs) apstrādā datus likumīgi, droši un tikai tam paredzētajiem nolūkiem. Šajā dokumentā atkarībā no faktiskās situācijas un līguma priekšmeta būtu atrunājams, piemēram, vai apstrādātājs veic datu nosūtīšanu uz citu Eiropas Savienības vai trešo valsti vai starptautisku organizāciju, vai apstrādātājs apliecina, ka personas, kuras ir pilnvarotas apstrādāt datus, ievēro konfidencialitāti un drošības prasības un kādos gadījumos un termiņos dzēš datus un to kopijas, kā arī, vai un kā apstrādātājs, ciktāl tas ir iespējams ņemot vērā apstrādes būtību, palīdz pārzinim ar atbilstīgiem tehniskiem un organizatoriskiem pasākumiem, kas nodrošina, ka pārzinis var izpildīt savu Datu regulas 32. – 36. pantā paredzēto pienākumu izpildi. Ne mazāk būtiski šādā dokumentā ir paredzēt pasākumus un procedūru, kā apstrādātājs dara pārzinim pieejamu visu informāciju, kas tam nepieciešama, lai apliecinātu, ka tiek pildīti Datu regulā paredzētie pienākumi, un lai ļautu pārzinim vai citam pārziņa pilnvarotam revidentam veikt revīzijas, tostarp pārbaudes, un sniegtu tajās ieguldījumu.

[3.5.] Attiecībā uz to, kā veikt paša apstrādātāja atbilstības Datu regulas prasībām izvērtējumu, Inspekcija papildus norāda, ka Datu regula nenosaka konkrētus veicamos pasākumus vai ierobežojumus. Proti, ņemot vērā efektivitātes un resursu lietderības apsvērumus, Pašvaldība var lemt pati veikt individuālus auditus vai izvērtējumu, kā arī tai ir tiesības pilnvarot citu Pašvaldību vai trešās puses ārpakalpojumu sniedzēju, slēdzot sadarbības līgumus vai vienošanās sadarbības platformās, pilnvarojot šo struktūru veikt neatkarīgu izvērtējumu. Pēc būtības, ja apstrādātājs sniedz vienādus (līdzvērtīgus) pakalpojumus vairākiem pārziņiem (Pašvaldībām), no Datu regulas prasību ievērošanas nav starpības, vai to dara Pašvaldība vai kāda trešā persona, ar ko visas vai attiecīgās pašvaldības ir noslēgušas līgumu tiktāl, ciktāl Pašvaldība var pamatot šāds audita veikšanu tās interesēs, kādas sistēmas vai citi procesi tika pārbaudīti, kādi ir secinājumi un kā tie attiecas uz Pašvaldības pienākumu pārliecināties par apstrādātāja atbilstību Datu regulas prasībām. Inspekcija atzīst, ka ir saprātīgi un pamatoti konkrētās situācijās šos procesus (gan auditu un pārbaužu veikšanu, gan turpmāku apstrādātāja uzraudzību) veikt centralizēti, ja tie pēc sava satura un rezultātiem ir atbilstoši, ņemot vērā, ka Pašvaldībai kā pārzinim ir izvēles iespējas, nosakot piemērotākos līdzekļus, lai nodrošinātu apstrādes atbilstību Datu regulai.

Direktore J.Macuka

[..]