Datu valsts inspekcija

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

Lietā Nr. 01630000100826 (L-2-6/6235)

Sabiedrībai ar ierobežotu atbildību "RIDE"
nosūtīšanai e-adreses informācijas sistēmā

Lēmums

Rīgā, 13.11.2026.

Dokumenta reģistrācijas numurs
skatāms pievienotajā teksta datnē

Nr. 01630000100826-4

Par pārsūdzēto lēmumu

[1] Datu valsts inspekcija (turpmāk – Inspekcija) 2026. gada 12. oktobrī pieņēma lēmumu Nr. 01630000100826-3 "Par soda piemērošanu" (turpmāk – Lēmums) administratīvā pārkāpuma lietā Nr. 01630000100826 (L-2-6/6235) (turpmāk – Lieta), atzīstot sabiedrību ar ierobežotu atbildību "RIDE", vienotais reģistrācijas numurs 40203212928, juridiskā adrese: Sēļu iela 10, Mārupe, Mārupes novads, LV-2167 (turpmāk – Sabiedrība) par vainīgu Vispārīgās datu aizsardzības regulas[1] (turpmāk – Datu regula) 83. panta 4. punkta a) apakšpunktā un 83. panta 5. punkta a) apakšpunktā paredzētā administratīvā pārkāpuma izdarīšanā, piemērojot Sabiedrībai administratīvo naudas sodu EUR 21 000.00 (divdesmit viens tūkstotis euro 00 centi) apmērā.

[2] Lēmumā konstatēti šādi apstākļi:

[2.1] Lietas materiālos atrodas Inspekcijas Uzraudzības nodaļas juriskonsultes (turpmāk – Amatpersona) 2026. gada 7. maija ziņojums Nr. 2-5.1/104 "*Par sabiedrības ar ierobežotu atbildību "RIDE" rīcību un administratīvā pārkāpuma procesa uzsākšanu*" (turpmāk – Ziņojums).

Ziņojumā norādīts, ka:

[2.1.1] pamatojoties uz Patērētāju tiesību aizsardzības centra (turpmāk – PTAC) 2025. gada 2. decembra vēstulē[2] sniegto informāciju, saskaņā ar Datu regulas 57. panta 1. punkta a), f) un

[1] Eiropas Parlamenta un Padomes 2016. gada 27. aprīļa Regula Nr.2016/679 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula)

[2] PTAC 2025. gada 2. decembra vēstule Nr. 8-6./11526 *Par iespējamiem personas datu aizsardzības pārkāpumiem komersantu mobilajās lietotnēs* ar pielikumu (CD) (reģ. Inspekcijā 04.12.2025. ar Nr. 2-4.2/1906-S)

h) apakšpunktu un Datu likuma 5. panta pirmās daļas 1. punktu, 2026. gada 21. janvārī uzsākta pārbaude par Sabiedrības veikto personas datu apstrādi mobilajā lietotnē "RIDE App"[3] (turpmāk – Lietotne);

[2.1.2] no pārbaudes ietvaros iegūtās informācijas secināms, ka Sabiedrība, savas pamatdarbības – vieglo elektrisko transportlīdzekļu nomas – ietvaros, nodrošinot Lietotnes darbību un pakalpojuma saņēmēju autentifikāciju, izmantoja vienīgi uz mobilā tālruņa numuru nosūtītu vienreizēju piekļuves kodu (SMS OTP), nenodrošināja papildu identitātes pārbaudes mehānismus gadījumos, kad mobilā tālruņa numurs tiek atkārtoti piešķirts citai fiziskai personai, kā rezultātā jaunais numura lietotājs iegūst piekļuvi iepriekšējā Lietotnes lietotāja profilam un tajā esošajiem personas datiem – vārdam, elektroniskā pasta adresei, braucienu vēsturei, maršrutiem, laikiem, kā arī iemaksātājiem naudas līdzekļiem Lietotnes sadaļā "Mans e-maks", tādējādi pieļaujot nepamatotu un neatļautu personas datu izpaušanu trešajām personām un neievērojot pienākumu nodrošināt atbilstošus tehniskos un organizatoriskos pasākumus personas datu aizsardzībai;

[2.1.3] Ar minētajām darbībām Sabiedrība pārkāpusi Datu regulas 5. panta 1. punkta a) un f) apakšpunktā noteiktos personas datu apstrādes pamatprincipus, kā arī 5. panta 2. punktu un Datu regulas 24. panta 1. punktā, 25. panta 1. punktā, 32. panta 1. un 2. punktā, 33. pantā un 35. pantā pārzinim noteiktos pienākumus, par ko ir paredzēta administratīvā atbildība Datu regulas 83. panta 4. punkta a) apakšpunktā un 83. panta 5. punkta a) apakšpunktā.

[2.2] Pamatojoties uz Ziņojumu, ar 2026. gada 11. maija lēmumu Nr. 01630000100826-1 *Par administratīvā pārkāpuma procesa uzsākšanu un lietas izskatīšanas termiņa pagarināšanu* (turpmāk – Lēmums):

[2.2.1] uzsākta administratīvā pārkāpuma procesa Lieta pret Sabiedrību par pārkāpumu, par kuru paredzēta administratīvā atbildība Datu regulas 83. panta 4. punkta a) apakšpunktā un 83. panta 5. punkta a) apakšpunktā;

[2.2.2] pagarināts Lietas izskatīšanas termiņš līdz 2026. gada 14. septembrim.

[2.3] Lietas materiālos atrodas Sabiedrības 2026. gada 20. februāra[4] paskaidrojumi, no kuriem izriet, ka Lietotnē autentifikācija tiek veikta, izmantojot uz konkrēto mobilā tālruņa numuru nosūtītu vienreizēju verifikācijas kodu (OTP).

[2.4] Lietas materiālos atrodas Inspekcijas 2026. gada 19. marta vēstule Nr. 2-4.2/613-N *"Par papildu informācijas un dokumentu pieprasījumu"*, kurā Inspekcija norāda, ka Sabiedrības iepriekš sniegtā atbilde ir formāla, vispārīga un daļēji izvairīga, kā arī nesatur pilnīgu un ar objektīviem pierādījumiem pamatotu informāciju. Inspekcija norādīja arī uz to, ka Sabiedrības atbildei nav pievienoti dokumenti, kas saturētu informāciju par faktiem, uz kuriem Sabiedrība bija pamatojusi savu atbildi. Sabiedrība tiek lūgta novērst konstatētās nepilnības un iesniegt papildu informāciju un dokumentus.

[2.5] Lietas materiālos atrodas Sabiedrības 2026. gada 9. aprīļa papildus paskaidrojumi ar 3 pielikumiem.[5]

[2.6] Lietas materiālos atrodas Sabiedrības 2026. gada 19. jūnija paskaidrojumi[6], kuros Sabiedrība norāda, ka tai nav skaidrs faktiskais pamats, uz kura uzsākts administratīvā pārkāpuma

[3] Vietne: https://ridemobility.eu/
[4] Reģ. Inspekcijā 20.02.2026. ar Nr. 2.4.2/370-S
[5] Reģ. Inspekcijā 09.04.2026. ar Nr. 2.4.2/712-S
[6] Reģ. Inspekcijā 19.06.2026. ar Nr. 2-4.2/1309-S

process. Vienlaikus Sabiedrība apstiprināja jau iepriekš sniegtos paskaidrojumus, tostarp, ka Lietotnē autentifikācija tiek veikta, izmantojot uz konkrētu mobilā tālruņa numuru nosūtītu vienreizējo verifikācijas kodu (SMS OTP).

[2.7] Lietas materiālos atrodas Sabiedrības 2026. gada 26. augusta paskaidrojumi[7], kuros Sabiedrība, iepazīstoties ar Inspekcijas nosūtītajiem videomateriāliem, norādīja, ka tajos neesot konstatējami objektīvi pierādījumi tam, ka konkrētais mobilā tālruņa numurs būtu ticis atkārtoti piešķirts citai personai.

[2.8] Lietas materiālos atrodas Amatpersonas 2026. gada 27. augusta Nr. 2-4.2/1682-N un 2026. gada 16. septembra Nr. 2-4.2/1844-N noslodzes datu pieprasījumi elektronisko sakaru komersantam un elektronisko sakaru komersanta atbildes[8] uz minētajiem pieprasījumiem.

[2.9] Lietas materiālos atrodas Amatpersonas 2026. gada 15. septembra apskates protokols Nr. 2-2.3/1, kurā fiksēts PTAC 2025. gada 2. decembra vēstules pielikumā esošo videomateriālu saturs.

[2.10] Lietas materiālos atrodas Lēmums, kurā Amatpersona secina, ka Sabiedrības ieviesto tehnisko un organizatorisko pasākumu kopums nenodrošināja tādu drošības līmeni, kas novērstu neatļautu piekļuvi iepriekšējā lietotāja personas datiem pēc mobilā tālruņa numura atkārtotas piešķiršanas citai personai. Līdz ar to Sabiedrība nav izpildījusi Datu regulas 5. panta 1. punkta a) un f) apakšpunktā noteiktos personas datu apstrādes pamatprincipus, kā arī 5. panta 2. punktu un Datu regulas 24. panta 1. punktā, 25. panta 1. punktā, 32. panta 1. un 2. punktā, 33. pantā un 35. pantā pārzinim noteiktos pienākumus.

Lēmumā Sabiedrība atzīta par vainīgu Datu regulas 83. panta 4. punkta a) apakšpunktā un 83. panta 5. punkta a) apakšpunktā paredzētā administratīvā pārkāpuma izdarīšanā. Sabiedrības vaina Datu regulas 83. panta 4. punkta a) apakšpunkta un 5. punkta a) apakšpunkta administratīvā pārkāpuma izdarīšanā ir pierādīta ar: PTAC vēstuli, Sabiedrības paskaidrojumiem, apskates protokolu, elektronisko sakaru komersanta atbildi.

2026. gada 12. oktobrī Lēmums nosūtīts Sabiedrībai uz oficiālo elektronisko adresi. Atbilstoši Paziņošanas likuma 9. panta $1.^1$ daļai dokuments, kas nosūtīts uz oficiālo elektronisko adresi, uzskatāms par paziņotu otrajā darba dienā pēc tā nosūtīšanas. Līdz ar to Lēmums uzskatāms par paziņotu 2026. gada 14. oktobrī.

[2.11] 2026. gada 16. oktobrī saņemta Sabiedrības sūdzība (reģ. Inspekcijā 16.10.2026. ar Nr. 7-4.2/499-S; turpmāk – Sūdzība), ar kuru Sabiedrība pārsūdz Lēmumu pilnā apjomā un lūdz to atcelt, izbeidzot administratīvā pārkāpuma procesu. Sabiedrība lūdz arī pārskatīt piemēroto sodu, kā arī izdarīto pārkāpumu kvalifikāciju, atkārtoti izvērtējot Lēmuma secinājumus.

[3] Saskaņā ar Administratīvās atbildības likuma (turpmāk – AAL) 168. panta pirmo daļu lēmumu var pārsūdzēt augstākai amatpersonai 10 darba dienu laikā no lēmuma paziņošanas dienas. Ņemot vērā, ka Lēmums paziņots 2026. gada 14. oktobrī, Lēmumu var pārsūdzēt līdz 2026. gada 28. oktobrim. Inspekcijas direktore konstatē, ka Sūdzība iesniegta likumā noteiktajā termiņā un tās izskatīšana ir pieļaujama.

[4] Atbilstoši AAL 172. panta pirmajai daļai augstāka amatpersona sūdzību izskata rakstveida

[7] Reģ. Inspekcijā 26.08.2026. ar Nr.2-4.2/1845-S
[8] Reģ. Inspekcijā 16.09.2026. ar Nr. 1-6.1.1/120-IP-S un 18.09.2026. ar Nr. 1-6.1.1/122-IP-S

procesā viena mēneša laikā no sūdzības saņemšanas dienas. Administratīvā pārkāpuma lietas apstākļus augstāka amatpersona noskaidro, pamatojoties uz attiecīgajā lietā esošajiem pierādījumiem. Vienlaikus AAL 47. pantā noteikts, ka augstāka amatpersona šā likuma izpratnē ir persona, kura atbilstoši normatīvajos aktos noteiktajai kompetencei ir pilnvarota veikt administratīvā pārkāpuma lietā pieņemtā lēmuma tiesiskuma un pamatotības kontroli. Ņemot vērā minēto, Inspekcijas direktore kā augstāka amatpersona izskata Lietu vēlreiz pēc būtības saistībā ar Sūdzībā norādītajiem apstākļiem.

[5] Sabiedrība uzskata, ka viena konkrēta neatļauta piekļuves gadījuma konstatēšana nepierāda, ka Sabiedrība nenodrošināja atbilstošus tehniskos un organizatoriskos pasākumus. Sabiedrība uzskata, ka Lietotnē nebija paredzēta tikai SMS OTP autentifikācija, jo Lietotnē esot bijusi arī Device ID funkcionalitāte, kura konkrētajā gadījumā nenostrādāja. Sabiedrība uzskata ka, viena konkrēta gadījuma konstatēšana, nepierāda, ka visa sistēma kopumā neatbilst riskam atbilstošam līmenim.

[5.1] Inspekcijas direktore norāda, ka Datu regulas 5. panta 1. punkta f) apakšpunkts paredz, ka personas dati jāapstrādā tā, 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 (“integritāte un konfidencialitāte”). Detalizētāk šis princips ir skaidrots Datu regulas 25. panta 1. punktā, kas paredz pārziņa pienākumu īstenot atbilstošus tehniskos un organizatoriskos pasākumus, lai efektīvi īstenotu datu aizsardzības principus, un Datu regulas 32. panta 1. punktā, kas nosaka, ka pārzinim, ņemot vērā tehnikas līmeni, īstenošanas izmaksas un apstrādes raksturu, kā arī dažādas iespējamības un smaguma pakāpes riskus attiecībā uz fiziskas personas tiesībām un brīvībām, ir jāīsteno atbilstīgus tehniskus un organizatoriskus pasākumus, lai nodrošinātu riskam atbilstošu personas datu drošības līmeni. Attiecīgi šīs tiesību normas nosaka, ka pārzinim ir būtiska svarīga loma personas datu drošības nodrošināšana atbilstoši pastāvošajiem riskiem. Tas nozīmē, kā pārziņa pienākumus nav tikai formāla drošības mehānisma ieviešana, jo Datu regula paredz, ka pārziņa atbildība ir dinamisks, patstāvīgs process, pārzinim vērtējot iespējamos personas datu apstrādes drošības riskus un izvēloties tiem piemērotākos aizsardzības pasākumus, uzraugot to darbības efektivitāti, un izvēloties to piemērotību, lai tādējādi nodrošinātu apstrādāto personas datu drošību un aizsardzību.

Lietā ir konstatēs konkrēts gadījums, kad, izmantojot vienu un to pašu mobilā tālruņa numuru, personai bija iespējams piekļūt cita lietotāja kontam, līdz ar to Lietā ir pieejami pierādījumi, ka Sabiedrības īstenotie autentifikācijas un piekļuves kontroles pasākumi, lai gan atbilstoši Sabiedrības norādītajam ir tikuši ieviesti, tomēr nav bijuši efektīvi un pietiekami, lai aizsargātu jau reģistrēta lietotāja kontu no trešo personu piekļuves. Līdz ar to ir secināms, ka Sabiedrības kā pārziņa ieviestie tehniskie un organizatoriskiem pasākumi bija nepietiekami, lai aizsargātu lietotāju kontos esošos personas datus un novērstu prognozējumu personas datu apstrādes risku iestāšanos. Savukārt, to, ka šāds risks bija prognozējams, apliecina arī pati Sabiedrība savos paskaidrojumos.

Inspekcijas direktore secina – tas, ka pārzinis ir ieviesis noteiktas drošības funkcionalitātes personas datu aizsardzībai, nenozīmē, ka ar to pārziņa atbildība ir izsmelta, jo pārzinim ir jānodrošina, ka izstrādātā funkcionalitāte praksē arī darbojas un pilda tai paredzēto funkciju. Tas nozīmē, ka Sabiedrības ieviestie tehniskie un organizatoriskie pasākumi nebija pietiekami, lai novērstu personas datu aizsardzības riskus, kuri bija prognozējami un paredzami, un tādējādi no pārziņa puses netika izpildītas Datu regulā paredzētās personas datu aizsardzības prasības.

Sabiedrības apgalvojums par to, ka Device ID funkcionalitāte bija ieviesta, bet nenostrādāja, pats par sevi apliecina to, ka drošības risku vērtēšana nebija ieviesta kā dinamisks process vai Sabiedrības prakse. Lietas izskatīšanas gaitā Sabiedrība atzina, ka par šādas funkcijas esamību vispār uzzināja tikai procesa gaitā no ārpakalpojuma sniedzēja un pati nepārzina šādas funkcijas darbības mehānismu. Ja pārzinis nezina, kā funkcija darbojas un nav veicis tās efektivitātes kontroli un

testēšanu, tas nav uzskatāms par riskam atbilstošu drošības līmeni.

[5.2] Attiecībā uz apstrādes riskiem Sabiedrība pamatoti atsaucas uz Eiropas Savienības Tiesas (turpmāk – EST) 2023. gada 14. decembra spriedumu lietā C-340/21, *Natsionalna agentsia za prihodite*, kurā atzīts, ka neatļauta trešās personas piekļuve personas datiem pati par sevi nav pietiekama, lai secinātu, ka pārziņa ieviestie tehniskie un organizatoriskie pasākumi nav atbilstoši Datu regulas 24. un 32. panta prasībām. Tomēr, kā uzsvērts pašā spriedumā, ir nepieciešams vērtēt konkrēto datu apstrādes gadījumu, pastāvošos riskus un pārziņa īstenotos pasākumus šo risku novēršanai. Tādējādi tiesa norāda, ka nepastāv automātiska atbildības konstatēšana tikai pēc notikušā incidenta fakta, bet pārzinim ir jāspēj pamatot risku iespējamībai un apmēriem atbilstošu pasākumu izvēle un ieviešana.[9]

Konkrētajā lietā būtiska nozīme ir tam, ka Lietotnes autentifikācijas procesā tika izmantots personas telefona numurs. Svarīgi uzsvērt, ka telefona numurs nav nemainīgs personas identifikācijas veids, jo ikviena persona var mainīt telefona numuru. Tas nozīmē, ka atbilstoši mobilo sakaru operatoru praksei viens un tas pats numurs var tikt piešķirts citai personai. Atbilstoši Sabiedrības sniegtajiem paskaidrojumiem, Sabiedrība bija informēta par šo mobilo sakaru operatoru praksi. Līdz ar to Sabiedrībai, paredzot šādu autentifikācijas risinājumu, bija jāņem vērā šis apstāklis un attiecīgi jāievieš pasākumi šī konkrētā riska mazināšanai. Proti, ja piekļuve iepriekš izveidotam lietotāja kontam tiek atļauta, balstoties uz iespēju saņemt autentifikācijas kodu uz attiecīgo tālruņa numuru, pārzinim ir jāņem vērā risks, ka numura pašreizējais lietotājs var nebūt persona, kura kontu sākotnēji bija izveidojusi. SMS autentifikācijas kods apliecina piekļuvi konkrētajam tālruņa numuram autentifikācijas brīdī, bet pats par sevi neapliecina, ka persona ir sākotnējais konta īpašnieks. Tāpēc Sabiedrībai, izvēloties šādu autentifikācijas risinājumu, bija jāparedz efektīvi papildu pasākumi, kas novērstu šādu risku, proti, citas personas piekļuvi iepriekš reģistrēta lietotāja kontam, gadījumā, ja šai personai tiek atkārtoti piešķirts tas pats telefona numurs. Šādu prasību paredz Datu regulas 5. panta 1. punkta f) apakšpunkts, 25. panta 1. punkts un 32. pant 1. punkts.

[5.3] Sabiedrības norāde uz jau Lietotnes tehnoloģijā iestrādāto Device ID funkcionalitāti nemaina konkrētajā gadījumā konstatēto citas personas piekļuvi jau reģistrētam lietotāja kontam. Kā norādīts jau Lēmumā, tad Device ID funkcionalitātes ieviešana ir vērtējama pozitīvi, tomēr tas, ka konkrētā funkcionalitāte Lietotnē ir paredzēta, nenozīmē, ka tā praksē arī efektīvi darbojas, kā arī nepierāda to, vai ir novērsti visi iespējamie šķēršļi, kāpēc pārbaudes laikā tika konstatēta konkrēta situācija, kad šī funkcionalitāte pietiekami efektīvi neaizsargā jau reģistrētus lietotāju profilus. Papildus tam Lēmuma 5.5.3. apakšpunktā ir norādīts, ka Sabiedrība nespēja paskaidrot, kādēļ minētais mehānisms nenostrādāja, un līdz Lietas izskatīšanas brīdim nebija iesniegusi dokumentus par tehniskās kļūmes cēloni, tās izvērtēšanu un novēršanu.

Vērtējot pārziņa spēju pamatot risku iespējamībai un apmēriem atbilstošu pasākumu izvēli un ieviešanu, būtisks ir apstāklis, ka Sabiedrība nav iesniegusi nevienu pirms incidenta veiktu tehnisko testēšanas aktu, audita ziņojumu vai riska izvērtējumu, kas apliecinātu, ka tās drošības pasākumi attiecībā uz numuru rotāciju un ierīču maiņu vispār ir izvērtēti un atzīti par atbilstošiem un efektīviem.

Ņemot vērā iepriekš minēto, secināms, ka Sabiedrība nebija ieviesusi atbilstoši Datu regulas 5. panta 1. punkta f) apakšpunktam, 25. panta 1. punktam un 32. panta 1. punktam tādu tehnisko un organizatorisko pasākumu kopumu, kas efektīvi aizsargātu reģistrētu lietotāju personas datus, jo Sabiedrības ieviestais drošības pasākumu kopums autentifikācijas procesā pietiekami neaizsargātu jau izveidotu kontu lietotāju personas datus pret iespējamu trešo personu piekļuvi.

[6] Sabiedrība norāda, ka administratīvā naudas soda piemērošanai nepieciešams pierādīt pārkāpuma tīšu vai neuzmanīgu raksturu. Sabiedrības ieskatā, tās ieviestie drošības pasākumi, tostarp

[9] Eiropas Savienības Tiesas 2023. gada 14. decembra spriedumu lietā Nr. C-340/21, *Natsionalna agentsia za prihodite* 46. punkts

Device ID mehānisms, apliecina pienācīgu rūpību, savukārt viena drošības mehānisma nenostrādāšana nav pietiekams pamats neuzmanības konstatēšanai.

Inspekcijas direktore norāda, ka saskaņā ar EST 2023. gada 5. decembra sprieduma lietā C-807/21 *Deutsche Wohnen SE* 76. punktu administratīvo naudas sodu var piemērot, ja pārzinis nevarēja neapzināties savas rīcības pārkāpjošo raksturu, neatkarīgi no tā, vai tas apzinājās konkrētas Datu regulas normas pārkāpumu. Savukārt Eiropas Datu aizsardzības kolēģija (turpmāk – EDAK) Pamatnostādņu 04/2022 55.–56. punktā skaidro, ka neuzmanība ir konstatējama, ja pārzinis nav ievērojis tam noteikto rūpības pienākumu, un tā vērtējama, ņemot vērā no lietas faktiskajiem apstākļiem izrietošos objektīvos rīcības elementus.[10]

Inspekcijas direktore uzsver, ka Sabiedrības paskaidrojumos norādīto drošības pasākumu ieviešana pati par sevi neapliecina pienācīgu rūpību, jo Sabiedrība nenodrošināja Lietotnes lietotāju datu aizsardzību pret objektīvi paredzamiem personas datu apstrādes riskiem. Atbilstoši Datu regulas 25. panta 1. punktam un 32. panta 1. punktam pārzinim ir pienākums ne tikai ieviest drošības pasākumus, bet arī nodrošināt to efektivitāti, kā arī darbības uzraudzību.

Konkrētajā gadījumā Sabiedrība izvēlējās autentifikācijas risinājumu, kas balstīts uz mobilā tālruņa numuru. Sabiedrībai kā nomas pakalpojuma sniedzējam, kura lietotāji reģistrējas mobilā tālruņa Lietotnē, bija jāapzinās un jāparedz, ka mobilā tālruņa numurs var tikt piešķirts citai personai un tā jaunais lietotājs nav automātiski uzskatāms par iepriekš reģistrētā profila lietotāju. Tādējādi risks, ka jaunais numura lietotājs varētu iegūt neatļautu piekļuvi iepriekšējā lietotāja personas datiem, bija objektīvi paredzams, un Sabiedrībai bija pienākums ieviest šā riska novēršanai atbilstošus drošības pasākumus.

Lietas materiāli apliecina, ka Sabiedrības izmantotais Device ID mehānisms nenovērsa neatļautu piekļuvi citas personas profilam, savukārt citi pietiekami kontroles pasākumi šāda riska mazināšanai nebija ieviesti. Līdz ar to Sabiedrības neuzmanība izpaužas nevis pašā tehniskās kļūmes faktā, bet gan tajā, ka Sabiedrība, izvēloties un izmantojot konkrēto autentifikācijas risinājumu, nebija nodrošinājusi pienācīgu aizsardzību pret tai paredzamu personas datu neatļautas piekļuves risku, kā arī nepārliecinājās par to, vai paredzētie drošības mehānismi praksē pilda savu funkciju un ir pietiekams un efektīvs paredzamo risku novēršanai.

Tādējādi Inspekcijas direktore secina, ka Sabiedrība nav ievērojusi no tās kā pārziņa objektīvi sagaidāmo rūpību, jo nav nodrošinājusi izvēlētā autentifikācijas risinājuma atbilstību paredzamajiem personas datu apstrādes riskiem. Šāda rūpības pienākuma neievērošana ir kvalificējama kā neuzmanība Datu regulas 83. panta izpratnē. Apstāklis, ka Sabiedrība bija ieviesusi Device ID mehānismu, šo secinājumu nemaina, jo izšķiroša nozīme ir ieviesto drošības pasākumu faktiskajai atbilstībai konkrētajiem riskiem, kas konkrētajā gadījumā nedarbojās, ko apliecina arī Sabiedrība savos paskaidrojumos.

[7] Sabiedrība norāda, ka Inspekcija no viena PTAC pārbaudes gadījuma nepamatoti izdarījusi secinājumu par sistēmisku pārkāpuma raksturu, pārkāpuma ilgumu, kā arī ietekmi.

[7.1] Inspekcijas direktore norāda, ka ir nepieciešams nošķirt faktiski konstatēto neatļautas piekļuves gadījumu skaitu no riska, ko var radīt konkrēts autentifikācijas risinājums. Lietā konstatētais viens neatļautas piekļuves gadījums pats par sevi nepierāda, ka identiski incidenti būtu notikuši arī attiecībā uz citiem Lietotnes lietotājiem. Tomēr tas ļauj secināt, ka pārbaudē konstatētais piekļuves kontroles trūkums ir saistīts ar Sabiedrības ieviesto lietotāju autentifikācijas procesu kopumā, nevis tikai ar individuālu autentifikācijas gadījumu. Līdz ar to secināms, ka attiecīgais autentifikācijas

[10] EDAK Pamatnostādnes 04/2022 administratīvo naudas sodu aprēķināšanai saskaņā ar Vispārīgo datu aizsardzības regulu. Pieņemts 2023. gada 24. maijā. 20. lp. Pieejamas: https://www.edpb.europa.eu/system/files/documents/2024-01/edpb_guidelines_042022_calculationofadministrativefines_lv_0.pdf

risinājums neatbilst Datu regulā noteiktajām personas datu drošības un aizsardzības tehniskajām un organizatoriskajām prasībām.

Norādāms, ka Datu regulas 32. panta 1. punkts paredz personas datu apstrādes raksturam, apmēram, kontekstam un nolūkam atbilstošu tehnisko un organizatorisko pasākumu ieviešanu, līdz ar to pārzinim nav jāgaida vairāki personas datu aizsardzības pārkāpumi, lai tam rastos pienākums novērst zināmu vai paredzamu personas datu apstrādes drošības risku. Tādējādi, lai konstatētu drošības pasākumu nepietiekamību, nav nepieciešams pierādīt, ka neatļauta piekļuve notikusi atkārtoti vai skārusi lielu datu subjektu skaitu, ir pietiekami konstatēt, ka sistēmas drošības risinājumi ir neatbilstoši konstatējamu un paredzamu risku novēršanai.

[7.2] Attiecībā uz pārkāpuma ilgumu norādāms, ka Datu regulas 83. panta 2. punkta a) apakšpunkts paredz vērtēt pārkāpuma raksturu, smagumu un ilgumu. Ja neatbilstošs personas datu apstrādes drošības risinājums ir izmantots ilgstoši, šā risinājuma izmantošanas periods var būt nozīmīgs, izvērtējot pārziņa pienākumu izpildi. Līdz ar to apstāklis, ka Lietotne darbojas kopš 2020. gada 15. jūlija, un visu šo periodu tajā ir izmantots autentifikācijas risinājums, kas nav bijis efektīvs, lai novērstu reģistrētu lietotāju kontu aizsardzību pret trešo personu piekļuvi, ir vērtējams kā papildus faktors saistībā ar pārziņa atbildību par personas datu aizsardzības prasībām atbilstošu risinājumu ieviešanu, nevis kā pierādījums tam, ka neatļauta piekļuve personas datiem nepārtraukti notikusi kopš 2020. gada.

[7.3] Sabiedrība norāda arī uz konkrētā incidenta ierobežoto faktisko ietekmi, jo nav konstatēta ļaunprātīga personas datu izmantošana, mantisks kaitējums vai īpašu kategoriju personas datu izpaušana.

Inspekcijas direktore norāda, ka minētie apsvērumi ir ņemami vērā soda apmēra individuālajam izvērtējumam, vienlaikus tie neizslēdz personas datu aizsardzības un Datu regulas prasību pārkāpumu. Datu regulas 4. panta 12. punkts personas datu aizsardzības pārkāpumu definē kā drošības pārkāpumu, kura rezultātā notikusi nejauša vai nelikumīga personas datu neatļauta izpaušana vai piekļuve tiem. Līdz ar to, lai konstatētu pārkāpumu, nav nepieciešams noteikt, ka neatļautās piekļuves rezultātā būtu radies mantisks kaitējums vai dati būtu izmantoti ļaunprātīgi. Datu aizsardzības pārkāpuma konstatēšanai pietiekami ir konstatēt, ka ir notikusi neatļauta piekļuve personas datiem, kas arī tika izdarīts PTAC veiktās pārbaudes rezultātā.

Ir būtiski ņemt vērā, ka profilā ir pieejama detalizēta braucienu vēsture, kas ļauj nepārprotami izdarīt secinājumus par personas privāto dzīvi, pārvietošanās paradumiem, personas dzīvesvietu un darba vietu, kā arī var saturēt īpašu kategoriju datus, piemēram, informāciju par regulāri apmeklētām veselības aprūpes iestādēm, reliģiskajām celtnēm, izklaides vietām. Turklāt šāda informācija var būt pieejama vairāku gadu griezumā, tādējādi ļaujot izdarīt precīzus secinājumus par personu. Eiropas Savienības Tiesu judikatūrā atrašanās vietas dati tiek uzskatīti par ļoti personiska rakstura datiem, kuru aizsardzībai piemērojami paaugstināti drošības standarti, lai gan tie formāli nav kvalificēti kā īpašas kategorijas personas dati. Sabiedrība visā lietas izskatīšanas gaitā ir centusies mazināt šo personas datu nozīmību, tādējādi paužot savu subjektīvo attieksmi pret tās apstrādātajiem personas datiem un to aizsardzības nepieciešamību.

Tāpat Sabiedrība ignorē faktu, ka lietotājas profilā atradās reāls e-maka atlikums. Kā atzinusi pati Sabiedrība, jebkura persona, kas autentificējās ar šo numuru, varēja izmantot šos naudas līdzekļus pakalpojuma apmaksai. Tas, ka mantiskais zaudējums netika nodarīts tikai tāpēc, ka pārbaudi veica PTAC amatpersonas, nevis trešā persona ar negodprātīgu nolūku, nemaina apstākli, ka piemēroto neefektīvo drošības pasākumu rezultātā personām tiek radīts tiešs mantiska rakstura apdraudējums.

[8] Sabiedrība norāda, ka Lēmumā viena un tā pati neatļautā situācija ir izmantota, lai konstatētu Datu regulas 5. panta 1. punkta a) apakšpunkta, 5. panta 1. punkta f) apakšpunkta, 5. panta 2. punkta, 25. panta un 32. panta pārkāpumu. Sabiedrība apstrīd Datu regulas 5. panta 1. punkta

a) apakšpunkta piemērošanu, norādot, ka lietā nav konstatēts, ka sākotnējai datu apstrādei nebūtu bijis tiesiskais pamats, ka datu subjektam būtu sniegta maldinoša informācija vai pastāvētu atsevišķs pārredzamības pārkāpums.

Lēmuma, vērtējot Sabiedrības pārkāpuma raksturu, tika detalizēti skaidrots, kādus Datu regulas 5. panta 1. punkta principus Sabiedrība ir pārkāpusi, proti, Datu regulas 5. panta 1. punkta a) apakšpunktā nostiprināto likumības, godprātības un pārredzamības principu, jo lietotājiem bija tiesisks pamats paļauties, ka Sabiedrība nodrošinās to personas datu un lietotāja kontu aizsardzību, pasargājot tos no trešo personu piekļuves, kā arī Datu regulas 5. panta 1. punkta f) apakšpunktā nostiprināto integritātes un konfidencialitātes principu, jo lietotāja konta dati kļuva pieejami trešajai personai. Šāds detalizēts pārkāpto principu skaidrojums sniegts, lai izskaidrotu Sabiedrībai tās veiktā pārkāpuma raksturu, jo gan Datu regulas 5. panta 1. punkta a), gan f) apakšpunktā paredzot prasību ievērošanu paredz Datu regulas 5. panta 2. punktā nostiprinātais pārziņa pienākums.

Datu regulas 5. panta 2. punkts paredz, ka pārzinim ir jāievēro pārskatatbildības princips. Pārskatatbildība paredz, ka pārzinis ir atbildīgs par personas datu apstrādes atbilstību Datu regulas 5. panta 1. punktā noteiktajiem personas datu apstrādes principiem un tam ir pienākums spēt šo atbilstību pierādīt. Rezumējot, Datu regulas 5. panta 2. punkts jeb pārskatatbildības princips nosaka, ka pārzinis ir atbildīgs par personas datu apstrādes tiesiskumu un atbilstību Datu regulai, kā arī spēj uzskatāmi pierādīt, ka apstrādes darbības atbilst Datu regulas prasībām, t.sk. visiem Datu regulas 5. panta 1. punktā minētajiem principiem.[11]

Nosakot sodu, Amatpersona ir ņēmusi vērā to, ka Sabiedrības konstatētais Datu regulas 5. panta 1 .punkta a) un f) apakšpunkta, kā arī 5. panta 2. punkta pārkāpums ir savstarpēji cieši saistīts, tāpēc sods par šo pārkāpumu ir piemērots vienoti, atbilstoši Datu regulas 83. panta 5. punkta a) apakšpunktā paredzētajam (skat. Lēmuma 6.11. apakšpunktu).

Inspekcijas direktore uzsver, ka Datu regulas 83. panta 5. punkta a) apakšpunkta piemērošana nav atkarīga tieši no Datu regulas 5. panta 1. punkta a) apakšpunkta pārkāpuma konstatēšanas. Minētā soda kategorija attiecas uz Datu regulas 5. pantā nostiprināto personas datu apstrādes principu pārkāpumiem kopumā, tostarp Datu regulas 5. panta 1. punkta f) apakšpunktā noteiktā integritātes un konfidencialitātes principa pārkāpumu, kas konkrētajā lietā ir konstatēts, kā arī Datu regulas 5. panta 2. punkta pārkāpuma, kas paredz pārziņa pienākumu, nodrošināt personas datu apstrādes atbilstību Datu regulas prasībām.

Līdz ar to Inspekcijas direktore secina, ka Datu regulas 5. panta 1. punkta a) apakšpunkta patstāvīga pārkāpuma pamatojuma precizēšana pati par sevi nemaina piemērojamā naudas soda apmēru. Lēmumā par savstarpēji saistītajiem pārkāpumiem ir piemērots viens naudas sods, nevis atsevišķs sods par katru pārkāpto normu.

Vienlaikus ir jāņem vērā, ka godprātības principa un datu subjekta pamatoto gaidu aizskārums ir nodalāms no pārziņa faktiski ieviestajiem tehniskajiem pasākumiem, kas nav izrādījušies efektīvi. Godprātības princips pats par sevi liedz pārzinim apstrādāt datus veidā, kas datu subjektam rada nepamatotas, negaidītas vai netaisnīgas sekas. Persona, kas reģistrējas platformā, nevar pamatoti sagaidīt, ka pārzinis, nepārbaudot lietotāja identitāti, nodrošinās brīvu piekļuvi tās uzkrātajiem privātās dzīves datiem nākamajam tālruņa numura īpašniekam. Šai personai nav jāpārzina specifiski tehniskie risinājumi, lai izdarītu šādus secinājumus. Jo īpaši, ja tiek paredzēta konta bloķēšana, persona nevar sagaidīt, ka neaktīvie konti netiek savlaicīgi dzēsti, bet gan paliek piesaistīti tikai tālruņa numuram, radot pastāvīgu piekļuves risku nākotnē.

[9] Sabiedrība uzskata, ka vieni un tie paši apstākļi soda aprēķinā izmantoti atkārtoti.

[11] EDAK 2020. gada jūlija pamatnostādnes 07/2020 par pārziņa un apstrādātāja jēdzieniem VDAR 8.lp. Pieejamas: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_en

Sabiedrības ieskatā konkrētajā lietā Datu regulas 5. panta 1. punkta f) apakšpunkta un Datu regulas 32. panta pārkāpuma pamatojums pēc būtības balstīts uz vienu un to pašu faktu, ka Sabiedrība nebija nodrošinājusi lietotāju kontu aizsardzību pret neatļautu piekļuvi. Attiecīgi vienas un tās pašas personas datu apstrādes darbības ietvaros konstatētajiem pārkāpumiem noteikti naudas sodi EUR 14 000 un EUR 7 000 apmērā, tos summējot. Sabiedrības ieskatā, nav pienācīgi izvērtēta Datu regulas normu konkurence un vieni un tie paši apstākļi atkārtoti izmantoti naudas soda aprēķinā.

Inspekcijas direktore norāda, ka atbilstoši EDAK Pamatnostādņu 04/2022 30.–37. punktam, ja viena rīcība veido vairāku Datu regulas normu pārkāpumus, vispirms jāizvērtē, vai viena tiesību norma izslēdz otras normas piemērošanu. Ja viena norma specialitātes, subsidiaritātes vai iekļaušanas principa dēļ pilnībā aptver to pašu prettiesisko darbību, nav pieļaujama atkārtota sodīšana. Savukārt, ja normām ir patstāvīgi mērķi un tās paredz atšķirīgus pienākumus, pārkāpumus var vērtēt atsevišķi.[12]

Konkrētajā gadījumā Datu regulas 5. panta 1. punkta f) apakšpunkts nostiprina integritātes un konfidencialitātes principu, savukārt 32. pants konkretizē pārziņa pienākumus nodrošināt riskam atbilstošu personas datu drošību. Tādējādi šo normu piemērošanas tvērums ir savstarpēji saistīts, tomēr tas pats par sevi nenozīmē, ka to pārkāpumi vienmēr ir savstarpēji aizstājoši. Izšķiroši ir tas, vai konkrētajā lietā katras normas pārkāpums aptver patstāvīgu prettiesisku rīcību vai arī viens pārkāpums pilnībā ietver otra pārkāpuma būtību. Vērtējot konkrētās lietas materiālus secināms, ka būtu piemērojams specialitātes princips, jo pārzinim bija jānodrošina atbilstoši tehniskie un organizatoriskie pasākumi datu drošības garantēšanai, ko paredz gan Datu regulas 5. panta 1. punkta f) apakšpunkts, gan detalizēti nosaka Datu regulas 32. pants.

Savukārt, attiecībā uz naudas soda apmēra noteikšanu, Inspekcijas direktore norāda, ka saskaņā ar Datu regulas 83. panta 3. punktu un EDAK Pamatnostādņu 04/2022 38.–43. punktu vairāku Datu regulas pārkāpumu gadījumā, kas izdarīti vienas vai saistītu apstrādes darbību ietvaros, visi pārkāpumi ir ņemami vērā, nosakot galīgo naudas sodu. Vienlaikus naudas soda kopējā summa nedrīkst pārsniegt par smagāko pārkāpumu likumā noteikto maksimālo apmēru, nevis summu, kas individuāli aprēķināta par smagāko pārkāpumu.[13] Ja vienas apstrādes darbības ietvaros ir konstatēts vairāku Datu regulas pantu pārkāpums, uzraudzības iestāde var piemērot naudu sodu apmērā, kas paredzēts par smagāko pārkāpumu, konkrētajā situācijā par Datu regulas 85. panta 5. punkta pārkāpumu. Vairāku pārkāpumu gadījumā var noteikt vairākus naudas sodus. Tomēr sodu kopējā summa nevar pārsniegt maksimālo robežu, kas noteikta Datu regulā.[14] Lai gan tiesību aktos paredzēto naudas soda maksimālo apmēru nosaka, ņemot vērā smagāko pārkāpumu atbilstoši Datu regulas 83. panta 4. un 5. punktā norādītajam pārkāpumu uzskaitījumam, citiem pārkāpumiem ir nozīme, aprēķinot galīgo naudas sodu.[15] Ja uzskatītu, ka uzraudzības iestādei ir jāignorē citi konstatētie pārkāpumi, tiktu pārkāpts tiesību efektivitātes princips, jo pārzinis, kurš izdarījis piecus pārkāpumus, atrastos tieši tādā pašā situācijā kā pārzinis, kurš pieļāvis tikai vienu pārkāpumu.

Līdz ar to Lēmuma 6.11. un 6.12. apakšpunktā noteikto summu saskaitīšana pati par sevi nav pretrunā Datu regulas 83. panta 3. punktam. Tomēr, nosakot galīgo naudas sodu, jānodrošina, ka viena un tā pati prettiesiska rīcība netiek sodīta atkārtoti un Datu regulas 83. panta 2. punktā minētie apstākļi netiek atkārtoti izmantoti kopējā soda palielināšanai. Šie apsvērumi ir ņemami vērā soda apmēra noteikšanai Sabiedrībai.

Tādējādi Inspekcijas direktore secina, ka vairāku pārkāpumu konstatēšana vienas apstrādes

---

[12] EDAK Pamatnostādnes 04/2022 administratīvo naudas sodu aprēķināšanai saskaņā ar Vispārīgo datu aizsardzības regulu. Pieņemts 2023. gada 24. maijā. 13.-15. lp. Pieejamas: https://www.edpb.europa.eu/system/files/documents/2024-01/edpb_guidelines_042022_calculationofadministrativefines_lv_0.pdf

[13] Turpat, 15. – 16. lp.

[14] Vispārīgā datu aizsardzības regula. Skaidrojumi un komentāri. Autoru kolektīvs J.Plepa un M.Ruķera zinātniskajā redakcijā, Tiesu namu aģentūra, 2026, 740 – 741. lp

[15] Turpat.

darbības ietvaros pati par sevi neliecina par dubultu sodīšanu. Vienlaikus 21 000 EUR naudas soda samērīgums ir pamatojams ar katra patstāvīgā pārkāpuma izvērtējumu un kopējā soda aprēķinu, nepieļaujot identisku apstākļu atkārtotu ieskaitīšanu, soda apmēra palielināšanai.

[10] Sabiedrība uzskata, ka apstāklis, ka pārkāpumu atklāja nevis Sabiedrība iekšējās kontroles rezultātā, bet gan PTAC savas tirgus uzraudzības darbības ietvaros ir vērtējams kā sodu palielinošs apstāklis.

Attiecībā uz faktu, ka pārkāpums kļuva zināms PTAC pārbaudes rezultātā, norādāms, ka Datu regulas 83. panta 2. punkta h) apakšpunkts paredz ņemt vērā veidu, kādā uzraudzības iestāde uzzinājusi par pārkāpumu. Tomēr apstāklis, ka pārkāpumu atklājusi cita valsts iestāde, nevis pats pārzinis, automātiski nav uzskatāms par atbildību pastiprinošu apstākli. Šis apstāklis ir vērtējams kopsakarā ar pārziņa pienākumiem, tā faktisko informētību un iespējām atklāt pārkāpumu, nevis izmantojams kā patstāvīgs pamats soda palielināšanai.

[11] Sabiedrība uzskata, ka Inspekcija nelabvēlīgi vērtēja to, ka Sabiedrība ilgstoši balstījusi savu juridisko pozīciju uz argumentāciju, ka risks, ka viens un tas pats numurs var tikt izmantots autentifikācijai ir teorētisks vai ārējs, un Sabiedrība to nevar ietekmēt. Sabiedrība vērš uzmanību, ka elektronisko sakaru komersanta pierādījumi tika iegūti tikai pēc Sabiedrības 2026. gada 26. augusta paskaidrojumiem, un tā bija aizstāvības tiesību izmantošana.

Inspekcijas direktore norāda, ka, vērtējot Sabiedrības iesniegtos paskaidrojumus, redzams, ka tie sniegti formāli, neiedziļinoties lietas un problēmas būtībā. Papildus tam iesniegtie dokumenti un pierādījumi nesniedz Inspekcijai priekšstatu par Sabiedrības kā pārziņa īstenotajiem tehniskajiem un organizatoriskajiem pasākumiem, lai aizsargātu reģistrēto lietotāju datus, jo dokumentācija ir sagatavota vispārīgi, neiedziļinoties jautājuma būtībā un Sabiedrības individuālā situācijā un darbības specifikā.

Papildus tam Sabiedrības paskaidrojumos sniegtā informācija ir pretrunīga, piemēram, sniegtā informācija par kontu bloķēšanu, datu glabāšanu, drošības mehānismu izmantošanu utml. Arī attiecībā uz Device ID funkcionalitātes izmantošanu, pirmkārt, Sabiedrībai kā pārzinim bija jāpārliecinās kādi personas datu drošības mehānismi tika iestrādāti tās Lietotnē, ja Sabiedrībā norāda, ka netika informēta par to, ka Lietotnē ir Device ID funkcionalitāte, tad tas liecina, ka Sabiedrība nepārzināja visas Lietotnē esošās funkcijas un attiecīgi nebija informēta par ieviestajiem datu drošības un aizsardzības pasākumiem. Otrkārt, ja šāda funkcionalitāte Lietotnē ir bijusi paredzēta, tad Sabiedrība visā Lietas izskatīšanas procesā nav sniegusi informāciju par to, kāpēc konkrētajā gadījumā šī funkcionalitāte nenostrādāja, kādi tam bija iemesli un kādi pasākumi tika veikti, lai šos riska iemeslus nākotnē novērstu.

Ņemot vērā minēto, Inspekcijas direktore norāda, ka paskaidrojumu papildināšana ar jaunu tehnisko informāciju netika interpretēta kā soda apmēru pastiprinoša rīcība. Vienlaikus Sabiedrības pretrunīgā, dažādos paskaidrojumos atšķirīgā informācija, neļāva Inspekcijai pārliecināties par to, ka Sabiedrība būtu ieviesusi Datu regulas prasības attiecībā uz personas datu aizsardzību un kopumā rūpīgi, atbildīgi un apzinīgi piegājusi personas datu aizsardzības jautājumiem kā to paredz Datu regula.

[12] Sabiedrība nepiekrīt Inspekcijas konstatētajam Datu regulas 33. panta 5. punkta pārkāpumam, jo Sabiedrība neesot iesniegusi atsevišķu pietiekami dokumentētu incidenta izvērtējumu. Sabiedrība uzskata, ka Datu regulas 33. panta 5. punkta izpilde jāvērtē pēc dokumenta satura, nevis dokumenta nosaukuma. Ņemot vērā, ka pēc incidenta Sabiedrība uzsāka saziņu ar Lietotnes tehnisko uzturētāju ATOM Mobility, tad tās ieskatā elektroniskā sarakste, tehniskie skaidrojumi, pieprasījumi un atbildes ir vērtējami pēc to satura un uzskatāmi par Datu regulas

33. panta 5. punktā minēto dokumentāciju.

Datu regulas 33. panta 5. punkts nosaka, ka pārzinim jādokumentē visus personas datu aizsardzības pārkāpumus, norādot faktus, kas saistīti ar personas datu pārkāpumu, tā sekas un veiktās koriģējošās darbības, lai šie dokumenti ļauti Inspekcijai pārliecināties par Datu regulas 33. panta prasību ievērošanu. Tas nozīmē, ka pārzinis var dokumentēt incidentu dažādos veidos, tostarp izmantojot elektronisko reģistru, iekšējos ziņojumus, pārbaudes materiālus un citu dokumentāciju, jo būtisks ir šīs dokumentācijas saturs, nevis forma.

Saziņa ar Lietotnes tehnoloģiju izstrādātāju nav uzskatāma par tādu, kas atbilstu Datu regulas 33. panta 5. punkta prasību izpildei, jo lai atzītu šo pārziņa pienākumu par izpildītu dokumentu kopumam, jābūt tādam, ka tas ļautu Inspekcijai pārliecināties, ka pārzinis ir identificējis faktisko apstākļus, tā iespējamos cēloņus, sekas, kā arī veicis koriģējošās darbības un pasākumus, lai šo incident novērstu. Ņemot vērā, ka Sabiedrība norāda, ka joprojām nav sapratusi, kāpēc ir noticis konkrētais incidents, kā arī šī informācija netika iesniegta Inspekcijai līdz Lietas izskatīšanas pabeigšanai, tad tas neļauj Inspekcijai viennozīmīgi pārliecināties, ka Sabiedrība ir veikusi notikušā incidenta pilnīgu izvērtējumu un ieviesusi pasākumus, lai novērstu šādu incidentu atkārtošanos nākotnē.

Inspekcijas direktore secina, ka lietas materiālos nav dokumentācijas, kas ļautu Inspekcijai pilnvērtīgi pārbaudīt incidenta apstākļus, tā sekas un Sabiedrības veiktos koriģējošos pasākumus, tāpēc Lēmumā ir pamatoti konstatēts, ka Sabiedrība ir pārkāpusi Datu regulas 33. panta 5. punkta prasības.

[13] Sabiedrība uzskata, ka Inspekcija nepamatoti norādījusi uz Datu regulas 35. panta 1. punkta pārkāpumu, jo Sabiedrība bija veikusi Novērtējuma par ietekmi uz datu aizsardzību (NIDA) nepieciešamības sliekšņa izvērtējumu un secinājusi, ka pilna NIDA veikšana nav nepieciešama.

Datu regulas 35. panta 1. punkts nosaka, ka, ja apstrādes veids, jo īpaši, izmantojot jaunās tehnoloģijas un ņemot vērā apstrādes raksturu, apjomu, kontekstu un nolūkus, varētu radīt augstu risku fizisku personu tiesībām un brīvībām, pārzinis pirms apstrādes veic NIDA par to, kā plānotās apstrādes darbības ietekmēs personas datu aizsardzību. Minētais pārziņa pienākums nav atkarīgs no tā, vai personas datu aizsardzības pārkāpums vēlāk ir tiešām noticis, jo ietekmes uz datu aizsardzību novērtējums ir preventīvs pasākums, kura mērķis ir identificēt iespējamos riskus personas datu apstrādei pirms personas datu apstrādes uzsākšanas, attiecīgi ieviešot arī pasākumus šo risku mazināšanai.

Lai gan Sabiedrība bija veikusi NIDA sliekšņa testu, tomēr tas nepierāda Datu regulas 35. panta 1. punkta izpildi, jo svarīga ir šī izvērtējuma kvalitāte, tvērums un pamatotība. Papildus tam Lēmuma 5.5.10. apakšpunktā secināts, ka veiktais sliekšņa tests ir veikts nekvalitatīvi un nepilnīgi, kā arī tajā nav pilnvērtīgi izvērtēti visi ar personas datu apstrādi saistītie aspekti. Papildus tam Lēmumā Amatpersona secināja, ka, lai gan Sabiedrības veiktā personas datu apstrāde ietvēra vairākas augsta riska pazīmes fizisku personu tiesībām un brīvībām, Sabiedrība nav izpildījusi Datu regulas 35. panta 1. punkta pienākumu, bet iesniegusi tikai formāli sagatavotu NIDA sliekšņa testu.

Tas, ka Sabiedrība formāli veica NIDA sliekšņa testu, secinot, ka padziļināta NIDA nav nepieciešama, ievērojot Sabiedrības veikto personas datu apstrādes raksturu, neatbrīvo Sabiedrību no pienākuma veikt NIDA. Ņemot vērā, ka Lietotne paredz plašu personas datu apstrādi, kura notiek, izmantojot jaunās tehnoloģijas, tad pārzinim pirms šādas apstrādes uzsākšanas bija nepieciešams pienācīgi izvērtēt iespējamos apstrādes riskus, tostarp riskus, kas saistīti ar lietotāju autentifikāciju un iespēju piekļūt jau reģistrētu lietotāju kontiem. Ja šie riski pirms datu apstrādes uzsākšanas nav pienācīgi izvērtēti, tad tas ir pamats Inspekcijas direktorei secināt, ka Sabiedrība pēc būtības nav izpildījusi Datu regulas 35. panta 1. punkta prasības, kura mērķis ir identificēt pirms pārbaudes uzsākšanas iespējamos apstrādes riskus un veikt pasākumus preventīvai šo riskus novēršanai.

[14] Sabiedrība norāda, ka Lēmumā kļūdaini interpretēta ATOM Mobility tehniskā dokumentācija, konta bloķēšanu pēc sešu mēnešu neaktivitātes pielīdzinot konta dzēšanai.

Inspekcijas direktore piekrīt, ka konta bloķēšana un konta dzēšana ir atšķirīgas datu apstrādes darbības. Konta bloķēšana parasti ierobežo piekļuvi kontam, savukārt dzēšana nozīmē attiecīgo datu izņemšanu no apstrādes. Sabiedrības iesniegtajā ATOM Mobility dokumentā "Pielikums Nr. 4 – ATOM platformas tehniskās funkcionalitātes apraksts un izmantotie drošības mehānismi.pdf" ir norādīts, ka, ja lietotājs nav lietojis profilu sešus mēnešu vai ilgāk, konts tiek automātiski bloķēts.

Vienlaikus minētā terminoloģiskā atšķirība pati par sevi neatspēko galveno lietā konstatēto apstākli – citas personas piekļuvi iepriekš izveidotam Lietotnes kontam. Ja pēc ilgstošas perioda, kopš konts nav ticis izmantots, tam bija jābūt bloķētam, bet pārbaudes laikā tam varēja piekļūt, ir jāvērtē, kādēļ bloķēšanas mehānisms nenovērsa attiecīgo piekļuvi. Tas pats attiecas uz Device ID mehānismu, ja tā galvenā funkcija bija ierobežot piekļuvi kontam no citas ierīces.

Neskatoties uz to, ka tehniskajā dokumentācijā ir lietots termins "bloķēšana", tas neizslēdz nepieciešamību nodrošināt šīs funkcijas izpildi kontiem, kas netiek lietoti ilgāk kā 6 mēnešus atbilstoši Sabiedrības iesniegtajai dokumentācijai. Ņemot vērā no mobilo sakaru operatora iegūto informāciju, tad laikposmā no 2022. gada 12. novembra līdz 2024. gada 8. decembrim nebija spēkā neviens LMT pakalpojumu līgums par mobilā tālruņa numura 20293120 lietošanu, proti, minētais tālruņa numurs nebija nodots lietošanā nevienam klientam, tad, ievērojot Sabiedrības norādīto informāciju, šim kontam vajadzēja būt bloķētam, taču no Lietā pieejamajiem pierādījumiem redzams, ka šis konts bija aktīvs un tam varēja piekļūt ar iepriekš minēto telefona numuru pat pēc 3 gadiem, līdz ar to konkrētais piekļuves ierobežošanas mehānisms nenodrošināja atbilstošu personas datu aizsardzību. Līdz ar to secināms, ka neskatoties uz terminoloģijas atšķirībām – dzēšana vai bloķēšana, ir konstatēts, ka netika nodrošināta reģistrēta konta lietotāja datu aizsardzība, neskatoties uz to, ka šis konts ilgstoši netika lietots.

[15] Sabiedrība uzskata, ka EUR 21 000 naudas sods ir nesamērīgs, jo lietā konstatēts viens faktisks neatļautas piekļuves gadījums, nav pierādīta ļaunprātīga datu izmantošana, mantisks kaitējums vai īpašu kategoriju personas datu izpaušana.

[15.1] Inspekcijas direktore norāda, ka saskaņā ar Datu regulas 83. panta 1. punktu uzraudzības iestādei ir jānodrošina, ka par šīs regulas pārkāpumiem piemērotie naudas sodi katrā konkrētā gadījumā ir iedarbīgi, samērīgi un atturoši. Atbilstoši Datu regulas 83. panta 2. punktam, nosakot soda apmēru, uzraudzības iestādēm pienācīgi jāņem vērā vairāki elementi, kas liecina par pārkāpuma raksturu un nopietnību vai par pārkāpēja attieksmi pret izdarīto pārkāpumu. Tāpat nepieciešams ņemt vērā arī citus elementus, kam ir nozīme lietā, pat ja tie nav tieši uzskaitīti Datu regulas 83. panta 2. punktā.

[15.2] Inspekcijas direktore atkārtoti izvērtē administratīvajam pārkāpumam, kas paredzēts Datu regulas 83. panta 5. punkta a) apakšpunktā, piemēroto naudas sodu, jo Sabiedrība nenodrošināja Datu regulas 5. panta 1. punkta a) un f) apakšpunktu, 5. panta 2. punkta noteikto. Ievērojot šā lēmuma [9] punktā konstatēto, kopsakarā tiks ņemts vērā arī Datu regulas 32. panta 1. punkta pārkāpums, jo tas vērtējams kopā ar Datu regulas 5. panta 1. punkta f) apakšpunktu un 5. panta 2. punktu.

Inspekcijas direktore, vērtējot Datu regulas 82. panta 2. punktā noteiktos kritērijus secina:

1) *pārkāpuma būtību, smagumu un ilgumu, ņemot vērā attiecīgo datu apstrādes veidu, apmēru vai nolūku, kā arī ietekmēto datu subjektu skaitu* – pārkāpums ir attiecināms uz Datu regulas 5. pantā noteikto principu aizskārumu. Lietā konstatēts, ka personai, kurai bija atkārtoti piešķirts mobilā tālruņa numurs, bija iespējams piekļūt citas personas lietotāja profilam un tajā esošajiem personas datiem, tostarp lietotāja vārdam, e-pasta adresei, tālruņa numuram, braucienu vēsturei, maršrutu un pārvietošanās informācijai, kā arī e-maka datiem. Lai arī Lietā nav konstatēta īpašu kategoriju

personas datu apstrāde vai mantiska kaitējuma nodarīšana datu subjektam, pieejamo datu kopums ļauj izdarīt secinājumus par personas pārvietošanās paradumiem un pakalpojumu izmantošanas ieradumiem. Pārkāpums ir attiecināms uz Sabiedrības pamatdarbību, līdz ar to tas potenciāli varēja aizskart visus Sabiedrības pakalpojuma lietotājus.

Tāpat jāņem vērā, ka izmantotais autentifikācijas risinājums Lietotnē tika izmantots kopš 2020. gada 15. jūlija un Inspekcijas direktore neguva papildus pierādījumus vai informāciju, ka kopš šī termiņa būtu bijuši ieviesti kādi drošības risinājumi, kas šo autentifikācijas risku mazinātu. Papildus tam, neskatoties uz Sabiedrības norādīto, konkrētais lietotāja konts nebija bloķēts, lai gan nebija aktīvs kopš 2022. gada. Turklāt Sabiedrībai mobilā tālruņa numuru atkārtotas piešķiršanas risks bija zināms un paredzams, taču netika veikta pietiekama šī riska izvērtēšana un pārvaldība. Tas norāda, ka pārkāpuma pamatā nebija vienreizēja tehniska kļūda, bet gan ilgstoša un nepietiekama riska pārvaldība. Minēto apstiprina arī tas, ka Sabiedrība pati norādīja, ka mobilā tālruņa numuru atkārtotas piešķiršanas risku pēc būtības sāka vērtēt tikai pēc informācijas saņemšanas no Inspekcijas.

Ņemot vērā minēto, Inspekcijas direktore secina, ka pārkāpums pēc sava rakstura, smaguma, ilguma un potenciālās ietekmes uz datu subjektu tiesībām un brīvībām ir vērtējams kā vidēji smags pārkāpums, jo tas skāra Sabiedrības pamatdarbības procesus un faktiski materializējās kā neatļauta piekļuve personas datiem.

2) *to, vai pārkāpums izdarīts tīši vai neuzmanības dēļ* – Inspekcijas direktore secina, ka ir pamats atzīt Sabiedrības rīcību kā neuzmanību un nepietiekamu rūpību kā pārzinim, neieviešot nepieciešamos tehniskos un organizatoriskos pasākumus. Kaut arī Sabiedrībai nebija apzināts nodoms izraisīt pārkāpumu, tomēr tā nebija veikusi nepieciešamos pasākumus, lai mazinātu risku neautorizētai piekļuvei;

3) *par veiktajiem pasākumiem kaitējuma mazināšanai* – Inspekcijas direktore ņem vērā, ka līdz Lietas izskatīšanas dienai Sabiedrība nebija iesniegusi dokumentētus pierādījumus par pilnībā veiktu incidenta izmeklēšanu, konkrētu tehniskā cēloņa identificēšanu vai efektīvu korektīvo pasākumu ieviešanu;

4) *par pārziņa atbildības pakāpi* – Inspekcijas direktore secina, ka, ņemot vērā Sabiedrības darbības jomu, Sabiedrība pati izvēlējās un ieviesa lietotāju autentifikācijas metodi, un Lietā esošais pārkāpums ir saistīts ar Sabiedrības veikto personas datu apstrādi. Līdz ar to Sabiedrības atbildības pakāpe vērtējama kā augsta, ņemot vērā, ka Sabiedrībai vajadzēja ieviest tehniskos un organizatoriskos pasākumus, lai aizsargātu Lietotnes lietotāju personas datus;

5) *pārziņa iepriekšējus pārkāpumus* – Sabiedrība iepriekš nav administratīvi sodīta par Datu regulas pārkāpumiem;

6) *sadarbības pakāpi ar uzraudzības iestādi* – konstatējams, ka Sabiedrība sadarbojās lietas izmeklēšanas gaitā, sniedza paskaidrojumus un Inspekcijas pieprasītos dokumentus, kā arī piedalījās Lietas izskatīšanā. Vienlaikus ievērojama daļa paskaidrojumu bija formāli, pretrunīgi vai nepilnīgi, īpaši attiecībā uz Device ID funkcionalitāti un konkrētā incidenta izvērtēšanu;

7) *par attiecīgo personas datu kategorijām* – pārkāpums neskāra īpašu kategoriju personas datus. Tomēr tika skarti identificējoši dati, kontaktinformācija un personas pārvietošanās paradumus raksturojoši dati, kuru aizsardzībai ir būtiska nozīme;

8) *par veidu, kā pārkāpums tika atklāts* – pārkāpums netika identificēts pašas Sabiedrības iniciatīvas rezultātā. Inspekcija par pārkāpumu uzzināja no PTAC, kas to atklāja tirgus uzraudzības funkcijas ietvaros;

9) *par citiem atbildību ietekmējošiem apstākļiem* – atbildību mīkstinošus apstākļus Inspekcijas direktore nav konstatējusi. Vienlaikus Sabiedrība ilgstoši balstīja savu juridisko pozīciju uz argumentu, ka risks, ka vienu numurs var tikt piešķirts vairākām personām, ir teorētisks vai ārējs, lai gan Lietā tika pierādīts pretējais.

Ņemot vērā Datu regulas 83. panta 2. punktā noteikto kritēriju izvērtējumu kopumā, secināms, ka Datu regulas 5. panta 1. punkta a) un f) apakšpunkta, 5. panta 2. punkta, kā arī 32. panta 1. punkta pārkāpumi ir uzskatāmi par vidējas smaguma pakāpes pārkāpumiem.

Konkrētajā lietā pārkāpums saistīts ar Lietotnes autentifikācijas un piekļuves kontroles procesu, kas ir būtisks personas datu aizsardzības elements. Pārzinim, kurš nodrošina pakalpojumu, izmantojot lietotāju kontus, jāspēj novērst situācijas, kurās vienas personas identifikācijas līdzekļa iegūšana ļauj piekļūt citas personas kontam. Tādējādi pārkāpuma raksturs ir vērtējams nopietni arī tad, ja faktiski pierādīts tikai viens neatļautas piekļuves gadījums.

Sabiedrības norādītie labvēlīgie apstākļi, tostarp iepriekšēju pārkāpumu neesamība, tas, ka netika apstrādāti īpašu kategoriju personas dati, tas, ka netika konstatēts mantisks kaitējums un sadarbība ar Inspekciju un tehnisko nodrošinātāju, ir ņemami vērā.

Tomēr neviens no šiem apstākļiem atsevišķi nedod pamatu atteikties no naudas soda piemērošanas par konstatētajiem Sabiedrības Datu regulas pārkāpumiem.

Tāpat tas, ka pārkāpums nav izdarīts tīši, pats par sevi neizslēdz naudas soda piemērošanu, jo Datu regulas 83. pants paredz atbildību arī par aiz neuzmanības veiktiem pārkāpumiem.

Ņemot vērā pārkāpuma raksturu, faktiski materializējušos personas datu aizsardzības pārkāpumu, personas datu kategorijas, pārkāpuma ilgumu, Sabiedrības augsto atbildības pakāpi, kā arī konstatētos mīkstinošos un pastiprinošos apstākļus, Inspekcijas direktore secina, ka par minēto pārkāpumu taisnīgs un samērīgs administratīvais naudas sods ir nosakāms **EUR 14 000,00** (*četrpadsmit tūkstoši euro*) apmērā.

[15.3] Inspekcijas direktore atkārtoti izvērtē administratīvajam pārkāpumam, kas paredzēts Datu regulas 83. panta 4. punkta a) apakšpunktā, piemēroto naudas sodu, jo Sabiedrība nenodrošināja Datu regulas 25. panta 1. punkta, 33. panta 5. punkta, 35. panta 1. punktā noteikto.

Inspekcijas direktore, vērtējot Datu regulas 82. panta 2. punktā noteiktos kritērijus secina:

1) *pārkāpuma būtību, smagumu un ilgumu, ņemot vērā attiecīgo datu apstrādes veidu, apmēru vai nolūku, kā arī ietekmēto datu subjektu skaitu* – Inspekcijas direktore secina, ka konstatētie pārkāpumi skar datu aizsardzības pārvaldības sistēmas būtiskākos elementus, proti, datu aizsardzību pēc noklusējuma, personas datu aizsardzības pārkāpumu dokumentēšanu un ietekmes uz datu aizsardzību novērtēšanu. Lietā konstatēts, ka Sabiedrība bija izvēlējusies autentifikācijas modeli, kas būtiski balstīts uz mobilā tālruņa numuru un SMS OTP autentifikāciju. Vienlaikus Sabiedrība nebija nodrošinājusi efektīvus mehānismus, kas nepieļautu iepriekšējā lietotāja konta pieejamību gadījumā, ja mobilā tālruņa numurs tiek atkārtoti piešķirts citai personai.

Lietā konstatēts, ka Sabiedrības izmantotie aizsardzības mehānismi konkrētajā situācijā nenodrošināja paredzēto rezultātu. Lai gan Sabiedrība vēlāk atsaucās uz Device ID funkcionalitāti, tā nespēja paskaidrot, kādēļ šis mehānisms konkrētajā gadījumā nenostrādāja, kā arī neiesniedza dokumentus, kas apliecinātu tehniskās kļūmes izmeklēšanu un novēršanu. Lietā iesniegtais DPIA sliekšņa tests nesaturēja pilnvērtīgu izvērtējumu par lietotāju atrašanās vietas datu apstrādi, autentifikācijas modeļa radītajiem riskiem, mobilo tālruņu numuru rotāciju un ilgstošu lietotāju kontu saglabāšanu. Attiecīgi šis tests bija veikts formāli, neiedziļinoties ne personas datu apstrādes būtībā, ne izmantoto jauno tehnoloģiju radītājos riskos.

Lēmuma ir konstatēts, ka pēc informācijas saņemšanas par personas datu aizsardzības pārkāpumu Sabiedrība nebija veikusi pilnvērtīgu incidenta dokumentēšanu Datu regulas 33. panta 5. punkta izpratnē. Vērtējot pārkāpuma ilgumu, ņemams vērā apstāklis, ka esošās sistēmas autentifikācijas risinājums tika izmantots kopš Lietotnes darbības uzsākšanas. Līdz ar to Inspekcijas direktore secina, ka Datu regulas 25., 33. un 35. panta pārkāpumi kopumā vērtējami kā vidēja smaguma pakāpes pārkāpumi;

2) *to, vai pārkāpums izdarīts tīši vai neuzmanības dēļ* – Inspekcijas direktore secina, ka ir pamats atzīt Sabiedrības rīcību kā neuzmanību un nepietiekamu rūpību kā pārzinim, neieviešot

nepieciešamos tehniskos un organizatoriskos pasākumus. Lietā nav iegūti pierādījumi, ka Sabiedrība būtu veikusi šī riska dokumentētu izvērtēšanu, pārbaudījusi izmantotās autentifikācijas metodes noturību attiecībā uz šādu risku vai periodiski testējusi drošības pasākumu efektivitāti. Tieši pretēji, lietas izskatīšanas laikā Sabiedrības valdes priekšsēdētājs norādīja, ka atkārtoti piešķirta mobilā tālruņa numura risku Sabiedrība esot sākusi vērtēt tikai pēc Inspekcijas informācijas saņemšanas. Līdz ar to Sabiedrība nav ievērojusi tādu rūpības pakāpi, kādu no personas datu pārziņa bija iespējams un nepieciešams sagaidīt;

3) *par veiktajiem pasākumiem kaitējuma mazināšanai* – pēc Inspekcijas iesaistes Sabiedrība uzsāka komunikāciju ar ATOM Mobility un apsvēra dažādu drošības pasākumu pilnveidošanu. Sabiedrība norādīja arī uz iespēju ieviest papildu identitātes pārbaudes mehānismus, pārskatīt neaktīvo kontu glabāšanas termiņus un veikt citas izmaiņas. Vienlaikus līdz lietas izskatīšanas brīdim netika iesniegti pietiekami pierādījumi, kas apliecinātu pilnīgu konstatētā riska novēršanu vai efektīvu koriģējošo pasākumu ieviešanu;

4) *par pārziņa atbildības pakāpi* – Inspekcijas direktore secina, ka, ņemot vērā Sabiedrības darbības jomu, Sabiedrība pati izvēlējās un ieviesa lietotāju autentifikācijas metodi, un Lietā esošais pārkāpums ir saistīts ar Sabiedrības veikto personas datu apstrādi. Līdz ar to Sabiedrības atbildības pakāpe vērtējama kā augsta, ņemot vērā, ka Sabiedrībai vajadzēja ieviest tehniskos un organizatoriskos pasākumus, lai aizsargātu Lietotnes lietotāju personas datus**.** Lietā konstatētie pārkāpumi nav radušies ārēju apstākļu rezultātā vien. Tie lielā mērā saistīti ar Sabiedrības pieņemtajiem organizatoriskajiem un tehniskajiem lēmumiem, kā arī nepietiekamu risku pārvaldību;

5) *par iepriekšējiem pārkāpumiem* – Sabiedrība iepriekš nav administratīvi sodīta par Datu regulas pārkāpumiem;

6) *par sadarbību ar uzraudzības iestādi* **–** konstatējams, ka Sabiedrība sadarbojās lietas izmeklēšanas gaitā, sniedza paskaidrojumus un Inspekcijas pieprasītos dokumentus, kā arī piedalījās Lietas izskatīšanā. Vienlaikus sākotnēji Sabiedrības sniegtā informācija bija nepilnīga, vispārīga un daļēji pretrunīga. Vairāki nozīmīgi apstākļi tika paskaidroti tikai pēc atkārtotiem Inspekcijas pieprasījumiem. Līdz ar to sadarbība ir vērtējama kā daļēja;

7) *par attiecīgo personas datu kategorijām* – pārkāpums neskāra īpašu kategoriju personas datus. Tomēr tika skarti identificējoši dati, kontaktinformācija un personas pārvietošanās paradumus raksturojoši dati, kuru aizsardzībai ir būtiska nozīme;

8) par veidu, kā pārkāpums tika atklāts – pārkāpums netika identificēts pašas Sabiedrības iniciatīvas rezultātā. Inspekcija par pārkāpumu uzzināja no PTAC, kas to atklāja tirgus uzraudzības funkcijas ietvaros;

9) *par citiem atbildību ietekmējošiem apstākļiem* – atbildību mīkstinošus apstākļus Inspekcijas direktore nav konstatējusi. Sabiedrība ir veikusi NIDA sliekšņa testu, kā arī tās rīcībā pastāvēja dokumentēti drošības politikas dokumenti. Vienlaikus NIDA sliekšņa tests veikts vispārīgi, neiedziļinoties Sabiedrības veiktajā personas datu apstrādes specifikā, līdz ar ko tajā ir konstatētas būtiskas nepilnības. Papildus tam Lietā konstatētie pierādījumi liecina, ka Sabiedrības ieviestie tehniskie un organizatoriskie pasākumi nav bijuši pietiekami, lai identificētu un efektīvi pārvaldītu faktiskos personas datu apstrādes riskus.

Ņemot vērā Datu regulas 83. panta 2. punktā noteikto kritēriju izvērtējumu kopumā, secināms, ka Datu regulas 25. panta 1. punkta, 33. panta 5. punkta un 35. panta 1. punkta pārkāpumi ir uzskatāmi par vidējas smaguma pakāpes pārkāpumiem.

Pārkāpuma smagumu palielina tas, ka konstatētie trūkumi skāra Sabiedrības pamatdarbības procesus un tieši veicināja personas datu aizsardzības pārkāpuma iestāšanos. Vienlaikus ņemams vērā tas, ka Sabiedrība iepriekš nav sodīta par līdzīgiem pārkāpumiem.

Ņemot vērā pārkāpuma raksturu, faktiski materializējušos personas datu aizsardzības pārkāpumu, personas datu kategorijas, pārkāpuma ilgumu, Sabiedrības augsto atbildības pakāpi, kā

arī konstatētos mīkstinošos un pastiprinošos apstākļus, Inspekcijas direktore secina, ka par minēto pārkāpumu taisnīgs un samērīgs administratīvais naudas sods ir nosakāms **EUR 4 000,00** (*četri tūkstoši euro*) apmērā.

Naudas soda apmērs ir samazināts, ņemot vērā, ka iepriekš tika atsevišķi paredzēta atbildība arī par Datu regulas 32. panta 1. punkta pārkāpumu, kurš, ievērojot konstatētā pārkāpuma raksturu, tiek vērtēts kopsakarā ar Datu regulas 5. panta pārkāpumu, jo tas galvenokārt ir saistīts ar Sabiedrības kā pārziņa pienākumu ieviest atbilstošus tehniskos un organizatoriskos pasākumus, lai aizsargātu Lietotnes lietotāju datus. Tāpēc konkrētā soda apmērs noteikts par Datu regulas 25. panta 1. punkta, 33. panta 5. punkta, 35. panta 1. punkta pārkāpumu.

[15.4] Sabiedrība atsaucas uz EDAK Vadlīnijās 04/2022 paredzēto soda aprēķināšanas metodoloģiju un norāda, ka piemērotās summas atrodas orientējošo sākuma diapazonu augšējā daļā.

Inspekcijas direktors norāda, ka vadlīnijās paredzētās sākuma summas nav uzskatāmas par galīgo sodu apmēru. Soda noteikšana ir individuāls process, kurā tiek ņemti vērā visi konkrētās lietas apstākļi. Vienlaikus arī galīgajai soda summai jābūt pietiekami pamatotai, un vienus un tos pašus apstākļus nedrīkst nepamatoti atkārtoti izmantot soda palielināšanai.

Attiecībā uz soda piemērošanu par vairākiem pārkāpumiem norādāms, ka Datu regulas 83. panta 3. punkta piemērošanai ir jāizvērtē, vai konstatētie pārkāpumi izriet no vienas vai savstarpēji saistītām apstrādes darbībām. Ja vairāki pārkāpumi saistīti ar vienu apstrādes darbību, tas ir ņemams vērā naudas soda apmēra noteikšanā.

[15.5] Sabiedrība norāda, ka Datu regulas mērķi iespējams sasniegt ar rājienu un Lēmumā jau noteiktajiem korektīvajiem pienākumiem.

EST 2024. gada 26. septembra spriedumā lietā C-768/21, *TR pret Land Hessen* ir atzinusi, ka uzraudzības iestādei nav pienākuma par katru konstatētu Datu regulas pārkāpumu obligāti piemērot administratīvo naudas sodu. Vienlaikus minētā atziņa nenozīmē, ka pārzinim būtu subjektīvas tiesības prasīt tikai rājiena piemērošanu, ja uzraudzības iestāde konstatējusi pārkāpumu. Inspekcijai ir jāizvēlas tāds korektīvais līdzeklis, kas konkrētās lietas apstākļos ir piemērots un nepieciešams Datu regulas prasību efektīvai nodrošināšanai.

Tādēļ apstāklis, ka Sabiedrībai noteikti pienākumi uzlabot autentifikācijas un piekļuves kontroles mehānismus, pats par sevi neizslēdz administratīvā naudas soda piemērošanu.

Izvērtējot Lietas apstākļus un pierādījumus, kā arī Lēmumu un Sūdzību, Inspekcijas direktore secina, ka Inspekcijas Amatpersona Lēmumā ir pamatoti atzinusi Sabiedrību par vainīgu Datu regulas 83. panta 4. punkta a) apakšpunktā un 83. panta 5. punkta a) apakšpunktā paredzētā administratīvā pārkāpuma izdarīšanā, vienlaikus pārvērtējot noteiktā soda apmērus, Inspekcijas direktore groza Sabiedrībai piemērota naudas soda apmēra, nosakot Sabiedrībai **administratīvo naudas sodu EUR 18 000.00 (astoņpadsmit tūkstoši eiro 00 centi) apmērā**.

Ņemot vērā minēto un saskaņā ar Administratīvās atbildības likuma 132. pantu, 168. panta pirmo daļu, 172. pantu un 173. panta pirmās daļas 1. punktu, Datu regulas 58. panta 2. punkta i) apakšpunktu, Inspekcijas direktore

nolēma

grozīt ar 2026. gada 12. oktobrī pieņēma lēmumu Nr. 01630000100826-3 "Par soda piemērošanu" piemērotā administratīvā naudas soda apmēru, nosakot sabiedrībai ar ierobežotu atbildību "RIDE", vienotais reģistrācijas numurs 40203212928, juridiskā adrese: Sēļu iela 10, Mārupe, Mārupes novads, LV-2167, par Datu regulas 83. panta 5. punkta a) apakšpunktā un 83. panta 4. punkta a) apakšpunktā paredzētā administratīvā pārkāpuma veikšanu administratīvo naudas sodu **EUR 18 000.00** (astoņpadsmit tūkstoši eiro 00 centi) apmērā.

Naudas sods pilnā apmērā samaksājams ne vēlāk kā viena mēneša laikā no šī lēmuma spēkā stāšanās dienas jebkurā bankas iestādē vai arī pēc naudas soda brīvprātīgas izpildes termiņa beigām šis lēmums saskaņā ar Administratīvās atbildības likuma 262. un 269. pantu nekavējoties tiks nodots piespiedu izpildei zvērinātam tiesu izpildītājam.

Rekvizīti naudas soda samaksai:
Saņēmējs: Valsts Kase
Reģistrācijas Nr.: 90000050138
Konta Nr.: LV69TREL1060191019200
Saņēmēja BIC kods: TRELLV22
Piezīmes: Norādīt šī lēmuma numuru.

Administratīvā pārkāpuma procesā piemēroto naudas sodu, piespiedu naudu, atlīdzināmos procesuālos izdevumus un zaudējumus dabas resursiem var samaksāt portālā www.latvija.lv, izmantojot e-pakalpojumu Administratīvo sodu pārbaude un nomaksa.

Lūdzam ņemt vērā, ka, atbilstoši Civilprocesa likuma 568. pantam, lēmuma brīvprātīga izpilde pēc tam, kad izpildu dokuments iesniegts piespiedu izpildei, neatbrīvos no pienākuma atlīdzināt izpildes izdevumus tiesu izpildītājam.

Vienlaikus informējam, ka SIA "RIDE", ievērojot Administratīvās atbildības likuma 266. panta pirmo, otro un trešo daļu, ir tiesības Inspekcijai lūgt atlikt naudas soda izpildi uz laiku līdz vienam mēnesim vai sadalīt naudas sodu daļās, ja pastāv objektīvi apstākļi, kuru dēļ naudas soda brīvprātīgas izpildes termiņā nav iespējams pilnā apmērā izpildīt nolēmumu par sodu.

Saskaņā ar Administratīvās atbildības likuma 184. panta pirmo daļu un 186. panta pirmo un trešo daļu šo lēmumu SIA "RIDE" var pārsūdzēt 10 darbdienu laikā no dienas, kad paziņots lēmums administratīvā pārkāpuma lietā, rajona (pilsētas) tiesā pēc sūdzības iesniedzēja juridiskās adreses, sūdzību iesniedzot Datu valsts inspekcijā (Elijas ielā 17, Rīgā, LV-1050), kura triju darbdienu laikā pēc sūdzības iesniegšanas termiņa beigām, sūdzību ar lietas materiāliem nosūta rajona (pilsētas) tiesai pēc piekritības.

Direktora p.i. L.Dilba