



Datu valsts inspekcija

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

Lietā Nr. [..]

Sabiedrībai ar ierobežotu atbildību “Datoru drošības tehnoloģijas”

Matrožu iela 15
Rīga, LV-1048

Lēmums

Rīgā,
2022.gada 27.janvārī

Nr. [..]

Par pārbaudē konstatēto un rājienu izteikšanu

[1] Datu valsts inspekcijā (turpmāk – DVI) 2021.gada 22.martā tika saņemts privātpersonas iesniegums¹ (turpmāk – Iesniegums), kurā sniegtā informācija liecināja par sabiedrības ar ierobežotu atbildību “Datoru drošības tehnoloģijas”, reģistrācijas numurs 40003516277 (turpmāk – SIA) iespējamu personas datu apstrādes pārkāpumu. Proti, publiskā resursā – hipersaitē ar adresi: [..] turpmāk – hipersaite) bija pieejami žurnālieraksti (*logfile* jeb datnes) par maksājumu transakcijām saistībā ar SIA sniegtajiem pakalpojumiem. Iespējamais pārkāpums raksturojās ar personas datu vākšanu un glabāšanu ilgstošā periodā (no 2014.gada 11.septembra) un šo datu pieejamību publiskā resursā, kur tos varēja *rasmot* un *indeksēt* interneta meklētāju lietotnes, tādējādi padarot datus brīvi pieejamus meklēšanai interneta tīklā (turpmāk – Pārkāpums). Tāpat Iesniegumā sniegtā informācija liecināja, ka datnēs iespējams atlasīt šādu informāciju: veiktie pasūtījumi (58 811), personu vārdi, uzvārdi (25 592), elektroniskā pasta adreses (23 370), tālruņa numuri (18 812), bankas konta numuri (11 304), IP adreses (40 401), fiziskās adreses dati (41 808), reģistrācijas numurs (1352), valstis ar vismaz vienu personu (123), kā arī licences seriālie numuri (58 690).

Veicot Iesniegumā norādītās hipersaites apskati², konstatēts, ka tajā ir pieejama tabula/saraksts, kas satur vairākas datnes par periodu no 2014.gada 11.septembra līdz DVI Akta sagatavošanas dienai. Izlases veidā, atverot jebkuru no datnēm, konstatēts, ka tajā pieejama lapa, kurā redzami cipari, burti, atsevišķi vārdi, simboli, pieturzīmes un hieroglifi, starp kuriem atrodamas, piemēram, atsevišķas elektroniskā pasta adreses, bankas konta numuri, fizisku personu vārdi, uzvārdi, telefona numuri, ar maksājumu veikšanu saistīta informācija. Izvēloties datni ar nosaukumu [..], konstatēts, ka tajā cita starpā ir redzams arī fiziskas personas vārds, uzvārds, elektroniskā pasta adrese, telefona numurs.

Vienlaikus konstatēts, ka tīmekļa vietne www.antivirus.lv³ (turpmāk – Vietne) pieder SIA un atbilstoši tajā sniegtajai informācijai, Vietne ir SIA *blogs*, kurā uzņēmuma komanda informē savus lasītājus un sekotājus par svarīgām norisēm IT drošībā, publicē brīdinājumus par

¹ DVI reģistrēts ar Nr. [..]

² DVI 2021.gada 29.marta akts Nr. [..]

³ Par AntiVirus.LV | AntiVirus.LV

apdraudējumiem Latvijā un sniedz padomus IT drošībā. Vietne nesatur informāciju par tās drošības (privātuma) politikas nosacījumiem.

[2] Tiesisko regulējumu fizisko personu datu apstrādei nosaka Vispārīgā datu aizsardzības regula⁴ (turpmāk – VDAR), Fizisko personu datu apstrādes likums (turpmāk – FPDAL) un citi normatīvie akti, savukārt DVI kompetenci, uzdevumus un pilnvaras nosaka VDAR 55., 57. un 58.pants un FPDAL 4. un 5.pants.

VDAR 4.panta 1. un 2.apakšpunkts nosaka, ka “personas dati” ir jebkura informācija, kas attiecas uz identificētu vai identificējamu⁵ fizisku personu (“datu subjekts”), savukārt “apstrāde” ir jebkura ar personas datiem vai personas datu kopumiem veikta darbība vai darbību kopums, ko veic ar vai bez automatizētiem līdzekļiem [...]. Pamatojoties uz minēto, fiziskas personas vārds, uzvārds, informācija par elektroniskā pasta adresi, bankas konta numuru, tālruņa numuru un cita informācija pēc kuras persona ir identificējama, ir atzīstama par personas datiem, bet jebkura ar tiem veikta darbība vai darbību kopums ir personas datu apstrāde VDAR 4.panta 2.apakšpunkta izpratnē.

Saskaņā ar VDAR 4.panta 7.apakšpunktu par personas datu apstrādes atbilstību VDAR ir atbildīgs pārzinis – fiziska vai juridiska persona, publiska iestāde, aģentūra vai cita struktūra, kas viena pati vai kopīgi ar citām nosaka personas datu apstrādes nolūkus un līdzekļus [...]. Konkrētajā gadījumā par pārzini ir atzīstama SIA.

Lai pārzina veikto datu apstrādi atzītu par likumīgu, pārzinim apstrādājot personas datus, ir jāpiemēro vismaz viens no VDAR 6.panta pirmajā punktā minētajiem pamatojumiem – datu subjekta piekrišana, līguma izpilde, juridisks pienākums, sabiedrības intereses, vitālo interešu aizsardzība un leģitīmo interešu ievērošana. Papildus tiesiskā pamata nodrošināšanai pārzinim jāievēro arī VDAR 5.panta 1.punktā noteiktie personas datu apstrādes principi, tostarp “a” apakšpunktā noteiktais, ka personas dati tiek apstrādāti likumīgi, godprātīgi un datu subjektam pārredzamā veidā (“likumīgums, godprātība un pārredzamība”) un “f” apakšpunktā noteiktais, ka dati tiek apstrādāti tādā veidā, lai tiktu nodrošināta atbilstoša personas datu drošība, tostarp aizsardzība pret neatļautu vai nelikumīgu apstrādi un pret nejaušu nozaušanās, iznīcināšanu vai sabojāšanu, izmantojot atbilstošus tehniskos vai organizatoriskos pasākumus (“integritāte un konfidencialitāte”). Turklāt ievērojot VDAR 5.panta 2.punktā noteikto pārskatatbildības principu, tieši pārzinim ir pienākums nodrošināt tādu personas datu apstrādes procesu, kas ļauj pierādīt, ka pārzina veiktā personas datu apstrāde ir atbilstoša datu aizsardzības normatīvā regulējuma prasībām.

Saskaņā ar VDAR 24.panta 1. un 2.punktu, ņemot vērā apstrādes raksturu, apmēru, kontekstu un nolūkus, kā arī dažādas iespējamības un nopietnības pakāpes riskus attiecībā uz fizisku personu tiesībām un brīvībām, pārzinis īsteno atbilstošus tehniskos un organizatoriskos pasākumus, lai nodrošinātu un spētu uzskatāmi pierādīt, ka apstrāde notiek saskaņā ar VDAR. Ja nepieciešams, minētos pasākumus pārskata un atjaunina. Ja tas ir samērīgi attiecībā uz apstrādes darbībām, 1.punktā minētajos pasākumos ietver to, ka pārzinis īsteno atbilstīgu politiku attiecībā uz datu aizsardzību.

VDAR 24. panta 1. un 2. punktu konkretizē VDAR 32.pants, kas nosaka, ka, ņemot vērā tehnikas līmeni, īstenošanas izmaksas un apstrādes raksturu, apmēru, kontekstu un nolūkus, kā arī dažādas iespējamības un smaguma pakāpes risku attiecībā uz fizisku personu tiesībām un brīvībām, pārzinis un apstrādātājs īsteno atbilstīgus tehniskus un organizatoriskus pasākumus, lai nodrošinātu tādu drošības līmeni, kas atbilst riskam, tostarp b) apakšpunktā minēto spēju nodrošināt apstrādes sistēmu un pakalpojumu nepārtrauktu konfidencialitāti, integritāti, pieejamību un noturību un d) apakšpunktā minēto procesu regulārai tehnisko un organizatorisko pasākumu efektivitātes testēšanai, izvērtēšanai un novērtēšanai, lai nodrošinātu apstrādes drošību.

⁴ Eiropas Parlamenta un Padomes regulas (ES) 2016/679 par fizisko personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK

⁵ identificējama fiziska persona ir tāda, kuru var tieši vai netieši identificēt, jo īpaši atsaucoties uz identifikatoru, piemēram, minētās personas vārdu, uzvārdu, identifikācijas numuru, atrašanās vietas datiem, tiešsaistes identifikatoru vai vienu vai vairākiem minētajai fiziskajai personai raksturīgiem fiziskās, fizioloģiskās, ģenētiskās, garīgās, ekonomiskās, kultūras vai sociālās identitātes faktoriem.

Tādējādi pārzinim ir pienākums nodrošināt tādus tehniskos un organizatoriskos pasākumus, lai datu apstrāde būtu droša un atbilstoša VDAR prasībām. No šiem nosacījumiem izriet, ka likumdevējs ir noteicis mērķi, kas būtu sasniedzams, bet līdzekļus, kā to sasniegt, jāizvēlas pašam pārzinim, proti, pārziņa kompetencē ietilpst tas, kā tieši tiks nodrošināta personas datu apstrādes atbilstība VDAR prasībām.

VDAR 4.panta 12.punkts nosaka, ka “personas datu aizsardzības pārkāpums” ir drošības pārkāpums, kura rezultātā notiek nejauša vai nelikumīga nosūtīto, uzglabāto vai citādi apstrādāto personas datu iznīcināšana, nozaudēšana, pārveidošana, neatļauta izpaušana vai piekļuve tiem. Savukārt VDAR 33.pantā noteikta pārkāpuma paziņošanas uzraudzības iestādei kārtība.

[3] Pamatojoties uz DVI rīcībā esošo informāciju, VDAR 57.panta 1.punkta “a” un “f” apakšpunktu un FPDAL 4.panta pirmās daļas 1.punktu, DVI uzsāka personas datu apstrādes pārbaudi par SIA ieviesto un īstenoto tehnisko un organizatorisko pasākumu atbilstību VDAR 32.pantam.

Pārbaudes ietvaros DVI pieprasīja⁶ un saņēma⁷ no SIA paskaidrojumus Lietā. Tāpat DVI saņēma SIA vēstuli⁸, kurā SIA informēja, ka ir veikusi tehniskos pasākumus un novērsusi iespēju piekļūt personas datiem, izmantojot minēto hipersaiti. Vienlaikus SIA lūdza sniegt DVI viedokli par nepieciešamību informēt datu subjektus par Pārkāpumu, uz ko DVI paskaidroja, ka DVI rīcībā nav pilnīgas informācijas par Pārkāpumu un ievērojot, ka visa informācija par konkrēto notikumu ir pārziņa (SIA) rīcībā, tikai pārzinis var izvērtēt Pārkāpuma apstākļus un atkarībā no incidenta smaguma, lemt par nepieciešamajām darbībām, tostarp, datu subjektu informēšanu.

Izvērtējot DVI rīcībā esošo informāciju kopsakarā ar SIA sniegtajiem paskaidrojumiem, konstatēts un secināts turpmāk minētais.

Līdz DVI vēstules saņemšanas dienai, SIA nebija informācijas par minētās hipersaites esamību, proti, par Pārkāpumu SIA uzzināja tikai no DVI vēstulē sniegtās informācijas. SIA veica Pārkāpuma apstākļu izpēti un konstatēja, ka minētās datnes nebija iespējams atrast ar parastajiem interneta meklētāja rīkiem, piemēram, Google.com. Tas nozīmē, ka, tikai zinot konkrētās hipersaites adresi: [...], varēja piekļūt servera tehniskās darbības dienas žurnālēšanas datnēm (*log failiem*). Veicot hipersaitē pieejamo datņu analīzi, secināts, ka datnes tajā sāktas veidot no 2014.gada 11.septembra. Veicot iekšējo izmeklēšanu, SIA konstatējusi, ka neilgi pirms šo datņu parādīšanās tika konstatēta kļūdaina servera darbība, apstrādājot klientu pasūtījumus interneta veikalā, kā rezultātā klienti uz elektronisko pastu saņēma dublētus (atkārtoti nosūtītus) vienus un tos pašus pasūtījumus. Par minēto problēmu tika informēts ārpakalpojuma sniedzējs SIA “BORN digital”, reģistrācijas numurs 50103480851, kas saskaņā ar savstarpēju vienošanos 2014.gadā veica programmēšanas darbus interneta veikalā (SIA ir pieejama elektroniskā pasta sarakste un bankas maksājumu atskaites visa 2014.gada garumā).

SIA noteiktā darba prakse paredzēja sekojošus drošības pasākumus – ārpakalpojuma darbu veikšana varēja notikt tikai no noteiktas IP adreses caur šifrētu savienojumu un darbiem bija pieejama tikai ar paroli aizsargāta vide. Kā parādīja veiktā izmeklēšana, ārpakalpojumu sniedzējs, neinformējot SIA, bija veicis darbus, pārkāpjot elementārus drošības noteikumus. Tā vietā, lai izmantotu aizsargātu vidi, ārpakalpojuma sniedzēja darbinieks interneta veikala programmatūras kodā bija veicis izmaiņas, kuru rezultātā darba veikšanai nepieciešamās servera darbības žurnālēšanas datnes (*log faili*) tika veidotas brīvi pieejamā hipersaitē. Pabeidzot darbus pie augstāk minētās kļūdas novēršanas, ārpakalpojuma sniedzēja darbinieks nepārtrauca žurnālēšanas datņu veidošanu brīvi pieejamā hipersaitē un nenodvēsa izveidotās žurnālēšanas datnes. Šo rupju pārkāpumu rezultātā, SIA nezinot, minētajā hipersaites adresē uzkrājās ikdienas servera darbības žurnālēšanas datnes, kas saturēja informāciju arī par sekmīgiem darījumiem interneta veikalā. Lai gan notikušo SIA vērtē kā ārpakalpojuma sniedzēja rupju kļūdu, SIA neizslēdz arī ļaunprātīgu rīcību, jo žurnālēšanas datnes saturēja darījumu datus, klientu ievadīto informāciju pirkumu veikšanai un programmatūras aktivizācijas kodus, kuriem ir komerciāla vērtība noteiktā laika periodā. SIA ir sazinājusies ar interneta veikalā pārdoto produktu ražotāju un noskaidrojusi, ka

⁶ DVI 2021.gada 15.jūnija vēstule Nr. [...]

⁷ SIA 2021.gada 12.jūlija vēstule (DVI reģistrēta ar Nr. [...])

⁸ SIA 2021.gada 21.jūnija vēstule (DVI reģistrēta ar Nr. [...])

interneta veikalā pārdotās programmatūras aktivizācijas kodu izmantošanā nav novērotas anomālijas, kas nozīmē to, ka interneta veikalā pārdotie aktivizācijas kodi līdz šim nav tikuši nesankcionēti izmantoti. SIA informēja, ka tuvākā gada laikā ir plānots regulāri veikt šādas pārbaudes, lai konstatētu iespējamo datu noplūdi. Papildus tam, ir ieplānots veikt regulāras pārbaudes tumšajā tīmeklī (DarkNet) ar atsevišķi izvēlētiem datu paraugiem. Datu noplūdes konstatēšanas gadījumā ir plānots informēt potenciālajam riskam pakļautos pircējus, izmantojot viņu ievadītos datus interneta veikalā (dati tiek glabāti 5 gadus atbilstoši grāmatvedības prasībām) un datus no minētajām žurnālēšanas datnēm, kā arī nepieciešamības gadījumā mainīt iegādātās programmatūras aktivizācijas kodus bez maksas.

SIA ir veikusi tehniskos pasākumus, lai turpmāk piekļuve datiem, izmantojot hipersaiti ar adresi: [...], nebūtu iespējama un uzkrātās servera darbības žurnālēšanas datnes būtu izdzēstas no servera. Interneta veikala programmatūrā ir veikti attiecīgi labojumi, lai šādas žurnālēšanas datnes turpmāk netiktu veidotas. Atbilstoši SIA secinātajam, informācija publiskā vietnē bija nonākusi ārpus pakalpojuma sniedzēja SIA "BORN digital" darbību rezultātā. Proti, žurnālēšanas datnes bija izveidojis ārpus pakalpojuma sniedzējs, neizmantojot tam piešķirto aizsargāto vidi, kā rezultātā darbi daļēji tika veikti publiskā vidē, pārkāpjot vispārpieņemtās drošības normas nozarē. Hipersaitē uzkrātās servera darbības žurnālēšanas datnes saturēja informāciju arī par sekmīgiem pirkumiem interneta veikalā, kuros parādās pircēja ievadītā informācija sekojošos laukos – vārds vai/un uzvārds, adrese, e-pasta adrese, telefona numurs (neobligāts datu ievades lauks) un pircēja IP adrese. Ja sekmīgais maksājums bija veikts ar AS "Swedbank" vai AS "SEB banka" *banklink* maksājuma starpniecību, tad pie attiecīgā pirkuma bija atrodamas pircēja bankas konta numurs. SIA nevar apgalvot, ka visi pirkumos norādītie dati ir reālu personu dati, jo personai veicot pirkumu netiek veikta tā identificēšana (pirkuma piegāde notiek uz pircēja norādīto e-pasta adresi). Kā piemēru SIA minēja sekmīgu pirkuma gadījumu, kurš bija atrodamas norādītajās servera tehniskās darbības žurnālēšanas datnēs - sekmīgs pirkums 236188, kurš veikts 2017.gada 7.decembrī, plkst.15:46 un satur personas datus ar sekojošiem ierakstiem: Vārds – test; Adrese – test; E-pasta adrese – test@test.lv.

Veicot pirkumus, klienti iegādājās kiberdrošības programmatūras 1 vai 2 gadu izmantošanas licences (kiberdrošības programmatūras aktivizācijas kodus). Iespējamais laika periods ir sākot no 2014.gada 11.septembra līdz 2021.gada 15.jūnijam un iespējamais datu subjektu skaits – 17 646. Tā kā pirkumu veikšanas procesā persona netiek identificēta no SIA puses, tad datu subjektu skaits varētu būt mazāks par iepriekš norādīto. SIA informēja, ka saistībā ar konstatēto Pārkāpumu SIA nav saņēmusi nevienu datu subjekta sūdzību.

Attiecībā uz auditācijas pierakstiem SIA norādīja, ka auditācijas pieraksti par pieprasījumiem serverim tiek glabāti 14 (četrpadsmit) dienas. Uz DVI vēstules saņemšanas dienu SIA pieejami auditācijas pieraksti sākot no 2021.gada 1.jūnija, un pēc auditācijas pierakstu analīzes hipersaitei ar adresi: [...] piekļūts no IP adreses [...], kas pēc publiski pieejamās informācijas pieder VAS "Tiesu Namu Aģentūra".

Pārbaudes ietvaros, DVI veica atkārtotu hipersaites apskati⁹ un konstatēja, ka tā nav aktīva un piekļuve datnēm vairs nav iespējama. Tādējādi DVI secina, ka atbilstoši SIA sniegtajai informācijai, Pārkāpums ir novērts un piekļuve datnēm nav iespējama.

Papildus DVI vērsās pie Informācijas tehnoloģiju drošības incidentu novēršanas institūcijas¹⁰ (turpmāk – CERT.LV) ar lūgumu izvērtēt SIA atbildē norādītos apsvērumus, kā arī sniegt informāciju, vai SIA bija iespējams pamanīt Pārkāpumu savlaicīgi u.c. Uz ko CERT.LV informēja, ka ņemot vērā to, ka SIA izmanto ārpus pakalpojumu (SIA "BORN digital" sniegtos pakalpojumus), tad SIA tiešām varēja nezināt par šādas hipersaites pieejamību. Tāpat CERT.LV norādīja, ka arī žurnālfaili par šādu laika periodu varētu būt jau pārrakstīti un vēsturiskos datus, kurš skatījās šo resursu, iegūt vairs nevarēs.

Papildus DVI vērsās pie privātpersonas, kura ziņoja par Pārkāpumu¹¹, taču līdz šī lēmuma sagatavošanas dienai, atbilde uz minēto DVI pieprasījumu nav saņemta.

⁹ DVI 2021.gada 7.oktobra akts Nr. [...]

¹⁰ DVI 2021.gada 25.oktobra elektroniskā pasta vēstule Nr. [...]

¹¹ DVI 2021.gada 2.decembra vēstule Nr. [...]

[4] Ievērojot šajā lēmumā norādīto, DVI secina, ka konkrētajā gadījumā SIA ir atzīstama par pārzini, bet ārpalpojumu sniedzējs (SIA "BORN digital") par apstrādātāju¹². Lai gan Pārkāpums tika pieļauts apstrādātāja veikto darbību dēļ, DVI vērš uzmanību uz VDAR noteikto pārziņa atbildību. Proti, saskaņā ar VDAR 28.panta 1.punktu gadījumos, kad apstrāde ir jāveic pārziņa vārdā, pārzinis izmanto tikai tādus apstrādātājus, kas sniedz pietiekamas garantijas, ka tiks īstenoti atbilstoši tehniskie un organizatoriskie pasākumi tādā veidā, ka apstrādē tiks ievērotas VDAR prasības un tiks nodrošināta datu subjektu tiesību aizsardzība. Tātad primāri gan par atbilstoša apstrādātāja izvēli, gan par personas datu apstrādes drošību un atbilstību VDAR prasībām ir atbildīgs pārzinis (konkrētajā gadījumā – SIA). Līdz ar to, tieši SIA ir pienākums kontrolēt apstrādātāja veiktās personas datu apstrādes darbības, tostarp vai tiek pildīti SIA norādījumi, uzdevumi u.c.

Ņemot vērā minēto, DVI secina, ka pārbaudes ietvaros iegūtās informācijas kopums ir pietiekošs un ļauj secināt, ka SIA nav nodrošinājusi pietiekamu apstrādātāja kontroli, proti nav veikusi VDAR 24.panta 1.punktā un 32.panta 1.punktā paredzētos atbilstošos tehniskos un organizatoriskos pasākumus, tādējādi pieļaujot SIA klientu personas datu pieejamību publiskā resursā – hipersaitē ar adresi: [..]. Tāpat SIA nav izpildījusi VDAR 32.pantā 2.punktā noteikto pārziņa pienākumu un nav novērtējusi atbilstīgu personas datu drošības līmeni, ņemot vērā apstrādes radītos riskus neatļautai piekļuvei tiem.

Ievērojot minēto, DVI secina, ka ar minētajām darbībām SIA ir pārkāpusi VDAR 5.panta 1.punkta f) apakšpunktā noteikto personas datu apstrādes principu un 24.panta 1.punktā un 32.panta 1.punkta "b" un "d" apakšpunktā noteiktās prasības.

Pamatojoties uz šajā vēstulē izklāstīto, DVI informē, ka uzsāktā pārbaude ir pabeigta, konstatējot SIA rīcībā iepriekš minētos VDAR pārkāpumus.

[5] DVI savā darbībā īsteno principu "Konsultē vispirms"¹³, kas paredz, ka DVI darbībai primāri ir preventīva, nevis sodīšanas funkcija, līdz ar to, tās primārie uzdevumi ir efektīva fizisko personu datu aizsardzība (norādījumu par pārziņa veiktajā personas datu apstrādē konstatētajām nepilnībām un ierosinājumu sniegšana to novēršanai) un nelikumīgas personas datu apstrādes gadījumā nepieciešamo darbību veikšana ar mērķi pēc iespējas ātrāk pārtraukt to, tādā veidā mazinot datu subjektam radīto kaitējumu.

Administratīvā procesa likuma (turpmāk – APL) 66.panta 1.daļa paredz, ka, apsverot administratīvā akta izdošanas vai tā satura lietderību (65.pants), iestāde lemj: 1) par administratīvā akta nepieciešamību, lai sasniegtu tiesisku (leģitīmu) mērķi; 2) par administratīvā akta piemērotību attiecīgā mērķa sasniegšanai; 3) par administratīvā akta vajadzību, tas ir, par to, vai šo mērķi nav iespējams sasniegt ar līdzekļiem, kuri mazāk ierobežo administratīvā procesa dalībnieku tiesības vai tiesiskās intereses; 4) par administratīvā akta atbilstību, salīdzinot privātpersonas tiesību aizskārumu un sabiedrības interešu ieguvumu un ņemot vērā, ka privātpersonas tiesību būtisku ierobežošanu var attaisnot tikai ievērojams sabiedrības ieguvums.

Veicot APL 66.pantā paredzēto izvērtējumu, DVI vērš uzmanību uz sekojošajiem apsvērumiem.

DVI norāda, ka šis administratīvais akts tiek izdots ar mērķi aizsargāt datu subjektu tiesības uz savu personas datu aizsardzību, kas konkretizētas VDAR, FPDAL un citos normatīvajos aktos, respektīvi, lai atturētu SIA un citas personas salīdzināmās situācijās no pārkāpumu izdarīšanas nākotnē.

Vērtējot SIA pieļautā Pārkāpuma smagumu, DVI ņem vērā, ka personas datus saturošā informācija publiski bija pieejama ilgstošu laika periodu, t.i. no 2014.gada 11.septembra līdz 2021.gada jūnijam, t.i. gandrīz 7 gadus. Šī iemesla dēļ, Pārkāpums skāra lielu datu subjektu skaitu (SIA klientus), fiziskas personas, ko SIA apkalpoja minētajā laika periodā. Tāpat DVI ņem vērā skartās personas datu kategorijas un no tā izrietošās iespējamās negatīvās sekas datu subjektiem, ja būtu piepildījies risks, ka kāda persona iegūtu hipersaitē pieejamos personas datus vai programmatūras aktivizācijas kodus un izmantotu tos kaitnieciskos nolūkos. Turklāt atbilstoši SIA

¹² Saskaņā ar VDAR 4.panta 8.punktu apstrādātājs ir fiziska vai juridiska persona, publiska iestāde, aģentūra vai cita struktūra, kura pārziņa vārdā apstrādā personas datus.

¹³ DVI 2017.gada 15.jūnijā parakstīja sadarbības memorandu par "Konsultē vispirms" principa iedzīvināšanu, veicinot valsts pārvaldes iestāžu uz klientu orientētu darbību

interneta vietnē [www.kaspersky.antivirus.lv](https://kaspersky.antivirus.lv)¹⁴ publicētajai SIA misijai - SIA kopš uzņēmuma dibināšanas nodarbojas ar inovatīvu IT projektu realizāciju un kibernetikas produktu/pakalpojumu izplatīšanu, lai piedāvātu lietotājiem vislabāko aizsardzību, kas konkrētajā gadījumā nesaskan ar pašas SIA rīcību un ieviestajiem personas datu drošības pasākumiem.

Papildus DVI ņem vērā SIA sadarbību ar DVI, operatīvo Pārskatīšanas novērtēšanu tiklīdz SIA par to kļūva zināms, kā arī to, ka neskatoties uz Pārskatīšanas smagumu, ilgstoši publiskotos datus trešās personas nav izguvušas un izmantojušas skartajiem datu subjektiem kaitnieciskos nolūkos. Tāpat DVI Pārskatīšanu vērtē kontekstā ar SIA veiktajiem un plānotajiem pasākumiem, lai turpmāk nepieļautu līdzīgu gadījumu atkārtanos, proti, regulāru pārbažu veikšanu, tehnisko un organizatorisko pasākumu pārskatīšanu, datu noplūdes konstatēšanas gadījumā, potenciālajam riskam pakļauto datu subjektu informēšanu, kā arī klientu iegādāto programmatūras aktivizācijas kodu bez maksas samainīšanu. Vienlaikus DVI konstatē, ka Vietnē esošā informācija ir papildināta ar SIA drošības (privātuma) politikas nosacījumiem¹⁵.

VDAR 58.panta 2.punkta "b" apakšpunkts paredz DVI pilnvaras izteikt rājienu pārzinim vai apstrādātājam, ja ar apstrādes darbībām ir tikuši pārkāpti VDAR noteikumi, savukārt, "d" apakšpunkts paredz DVI pilnvaras izdot rīkojumu pārzinim vai apstrādātājam saskaņot apstrādes darbības ar VDAR noteikumiem, vajadzības gadījumā – konkrētā veidā un konkrētā laikposmā.

Ievērojot minēto, kā arī ņemot vērā šajā lēmumā konstatēto pārziņa (SIA) atbildību attiecībā uz apstrādātāja veiktajām darbībām, Pārskatīšanas būtību, ilgumu, smagumu, datu subjektu skaitu, kurus Pārskatīšanas varēja skart, SIA sadarbības pakāpi un rīcību Pārskatīšanas novērtēšanā, DVI, pamatojoties uz VDAR 58.panta 2.punkta "b" un "d" apakšpunktu, FPDAL 23.pantu, APL 63.panta pirmās daļas 2.punktu, **nolemj izteikt rājienu SIA.**

Vienlaikus DVI aicina turpmākā SIA darbībā, veicot personas datu apstrādi, nodrošināt šajā lēmumā minētās un citas personas datu aizsardzības prasības, izvērtēt dažādas iespējamības un nopietnības pakāpes riskus attiecībā uz fizisku personu tiesībām un brīvībām, ņemot vērā datu apstrādes raksturu, apmēru, kontekstu, nolūkus un veiktos tehniskos un organizatoriskos pasākumus, lai aizsargātu personas datus un novērstu to iespējamu nelikumīgu apstrādi, kā arī novērst neatbilstības, nodrošinot tiesisku personas datu apstrādi un aizsardzību.

Saskaņā ar FPDAL 24.panta otro daļu, APL 76.panta pirmo un otro daļu, 79.panta pirmo daļu, 188.panta otro daļu un 189.panta pirmo daļu un Tieslietu padomes 2021.gada 26.marta lēmumu Nr.25 "Par tiesām, to darbības teritorijām un atrašanās vietām" šo lēmumu var pārsūdzēt viena mēneša laikā no tā spēkā stāšanās dienas Administratīvās rajona tiesas attiecīgajā tiesu namā pēc SIA juridiskās adreses atrašanās vietas.

Direktore

J.Macuka

[..]

¹⁴ <https://kaspersky.antivirus.lv/>

¹⁵ <https://antivirus.lv/privatuma-politika/>