BILANCE
34
Nr. 5 (449) 2019. gada maijs

Ko mācīties no citu pieļautajām kļūdām datu aizsardzības jomā

Drīz būs aizritējis pirmais gads, kopš tiek piemērota Vispārīgā datu aizsardzības regula (GPR). Aizvadītajā gadā daudzi uzņēmumi ir aktīvi strādājuši, lai sakārtotu dokumentāciju un datu apstrādes procesus atbilstoši GDPR prasībām.

Gatavojoties GDPR ieviešanai, daudz tika apspriests jautājums par augsto naudas sodu piemērošanu, bieži minot maksimālo naudas sodu līdz 20 miljoniem EUR vai uzņēmumu gadījumā līdz 4 procentiem no uzņēmuma apgrozījuma. Vai bažas par milzīgajiem sodiem ir bijušas pamatotas? Vairākas ES dalībvalstis jau ir ziņojušas par pirmajiem piemērotajiem sodiem.

Šo sodu un pieļauto pārkāpumu izvērtēšana var palīdzēt novērst atlikušos trūkumus datu apstrādes procesos, tādēļ apkopojām galvenos secinājumus no šiem lēmumiem.

Lai gan Latvijā vēl nav ziņu par piemērotajiem naudas sodiem, ES Datu aizsardzības kolēģijas (iepriekš: 29. panta darba grupa) vadlīnijas par naudas sodu piemērošanu nosaka, ka, lai gan nacionālās uzraudzības iestādes saglabā neatkarību, vajadzētu izvairīties no situācijām, kad līdzīgās lietās uzraudzības iestādes izvēlas atšķirīgus korektīvos pasākumus. Tādēļ ir ticams, ka attiecībā uz līdzīgiem pārkāpumiem Latvijā ir sagaidāma pastiprināta Datu valsts inspekcijas uzmanība un, iespējams, līdzīga apmēra naudas sodu piemērošana.

Pārmērīga videonovērošana

Valsts: **Austrija**
Sods: **4800 EUR**
Sods piemērots sporta kafejnīcai, kas veica publiskas telpas videonovērošanu (ietves, stāvvietas, ieeju kafejnīcā). Novērošanas kamerās redzamā lielā publiskās telpas daļa nebija samērīga ar datu apstrādes mērķi. Teritorijā, kurā tika veikta videonovērošana, nebija izvietoti paziņojumi par videonovērošanu. Netika ievērots videoierakstu glabāšanas termiņš, kas ir noteikts Austrijas nacionālajos normatīvajos aktos (GDPR ļauj šo termiņu noteikt katrai dalībvalstij individuāli).

Ko varam mācīties no šīs situācijas?

- **Videokameras.** Pārzinim, kurš veic videonovērošanu, ir jābūt skaidri definētiem datu apstrādes mērķiem (piemēram, ražošanas procesa uzraudzībai, drošībai, noziegumu prevencijai, piekļuves kontrolei u.c.). Kamerās redzamajam ir jābūt samērīgam ar izvirzīto mērķi.
- **Videonovērošanas zīmes.** Pārzinim ir pienākums informēt datu subjektus par datu apstrādi, sniedzot visu GDPR 13. pantā norādīto informācijas klāstu par datu apstrādi, apstrādes termiņiem, datu subjektu tiesībām u.c. Videonovērošanas gadījumā informācija ir jāsniedz, pirms cilvēks nonāk teritorijā, kurā notiek videonovērošana. Informēšanai labi kalpo informatīvas zīmes. Latvijā likumdevējs ir atstājis pārziņiem izvēli, vai paziņošanai izmantot videonovērošanas zīmi vai kādu citu līdzekli, piemēram, plakātu ar visu nepieciešamo informāciju. Videonovērošanas zīmē atbilstoši Fizisko personu datu apstrādes likuma prasībām ir jānorāda vismaz pārziņa nosaukums, kontaktinformācija, datu apstrādes mērķi un norāde par iespēju iegūt citu GDPR 13. pantā norādīto informāciju (piemēram, mājaslapā vai zvanot pa tālruni).
- **Videoierakstu glabāšanas termiņš.** Latvijas normatīvie akti neparedz konkrētu videoierakstu glabāšanas termiņu. Pārzinim ir jāizvēlas samērīgs glabāšanas laiks, vadoties no izvēlētā datu apstrādes mērķa. Datu valsts inspekcijas vadlīnijas «Datu apstrāde videonovērošanas jomā» kalpo kā konsultatīvs avots pārziņiem, lai izvērtētu riskus un izvēlētos piemērotu videonovērošanas materiālu uzglabāšanas termiņu.

«Mirušās dvēseles» datu apstrādes sistēmā

Valsts: **Portugāle**
Sods: **200 000 EUR**
Sods piemērots slimnīcai par datu apstrādes pamatprincipu neievērošanu, pienācīgu tehnisko un organizatorisko pasākumu nepiemērošanu un nespēju nodrošināt informācijas drošības principu ievērošanu. Slimnīcai nebija dokumentācijas par lietotāja tiesību piešķiršanu tās datu apstrādes sistēmas lietotājiem. Sistēmā bija reģistrēti 985 aktīvi ārstu profili, lai gan faktiskais nodarbināto ārstu skaits bija tikai 296. Deviņiem tehniskajiem darbiniekiem bija piešķirtas tikpat plašas piekļuves tiesības pacientu datiem kā medicīnas personālam. Šajā gadījumā augsta soda piemērošanu ietekmēja arī tas, ka pārzinis apstrādā medicīnas datus, kas ir uzskatāmi par paaugstināta riska datu kategoriju.

Ko varam mācīties no šīs situācijas?

- **Dokumentēšana.** Pārskatatbildības princips ir viens no GDPR pamatprincipiem. Šis princips nozīmē, ka pārzinim ir jānodrošina iespēja pārliecināties par to, kā notiek informācijas sistēmu darbība, piekļuves tiesību piešķiršana un liegšana un kā notiek GDPR principu nodrošināšana.
- **Lietotāju profilu deaktivizācija.** Pārziņi nereti grēko, aizmirstot deaktivizēt no darba aizgājušo darbinieku profilus. Tādēļ, izbeidzot darba attiecības, vienmēr jāatceras, ka nepieciešams deaktivizēt bijušo darbinieku lietotāju kontus uzreiz pēc darba attiecību izbeigšanas.
- **Minimizācija.** Cits būtisks GDPR princips ir datu minimizācijas princips jeb «apstrādāt tikai tik daudz, cik nepieciešams». Tādēļ, konfigurējot piekļuves tiesības datubāzē esošajai informācijai, ir svarīgi, lai iespēja piekļūt informācijai plašā apjomā, ievadīt, labot un dzēst informāciju būtu tikai tiem darbinie-

Ieva Andersone,
Sorainen partnere,
zvērināta advokāte

Jūlija Terjuhana,
Sorainen juriste

kiem, kuru darba pienākumos tas ietilpst.

Vāji datu aizsardzības risinājumi

Valsts: **Vācija**
Sods: **20 000 EUR**
Sociālais tīkls *Knuddels.de* glabāja savu lietotāju datus (t.sk. profilu lietotājvārdus un paroles) nešifrētā veidā, kas bija iemesls, kādēļ ļaundari, uzlaužot sistēmu, varēja brīvi piekļūt 808 000 lietotāju personas datiem. Uzraugošā iestāde konstatēja būtiskus tehniskās un organizatoriskās aizsardzības trūkumus un uzlika pienākumu pārzinim uzlabot datu aizsardzības risinājumus. Uzņēmums rīkojās atbilstoši uzraugošās iestādes uzliktajam pienākumam. Neraugoties uz lielu iesaistīto datu subjektu skaitu, uzraugošā iestāde nepiemēroja uzņēmumam pārāk augstu sodu.

Ko varam mācīties no šīs situācijas?

■ **IT sistēmās izmantotajiem drošības risinājumiem ir būtiska nozīme datu aizsardzībā.** Ja uzņēmums jau no sākuma būtu izvēlējies situācijai atbilstošus datu aizsardzības risinājumus, arī tādā gadījumā, ja faili ar personas datiem nonāktu ļaundaru rokās, tie nevarētu piekļūt šiem datiem.

■ **Sadarbība ar uzraudzības iestādi.** Ne katrs pārkāpums datu aizsardzībā noved pie maksimālā naudas soda piemērošanas. Trūkumu novēršana noteiktajā termiņā un aktīva sadarbība ar uzraugošo iestādi ir viens no kritērijiem, ko iestāde ņem vērā pirms naudas soda piemērošanas, un aktīva sadarbība var ievērojami mazināt risku saņemt maksimālo sodu.

Datu subjekta tiesību neievērošana

Valsts: **Ungārija**
Sods: **3135 EUR**
Datu subjekts vērsās pie uzņēmuma, lai savas tiesvedības vajadzībām saņemtu videonovērošanas ierakstu, kurā viņš bija redzams. Uzņēmums atteica šāda ieraksta izsniegšanu, norādot, ka šis ieraksts nepalīdzēs subjekta pozīcijas stiprināšanai, bet tikai pierādīs, ka šis cilvēks ir bijis konkrētajā laikā konkrētajā vietā. Šāda uzņēmuma rīcība pārkāpj subjekta tiesības piekļūt saviem datiem.

Ko varam mācīties no šīs situācijas?

■ **Pārziņa pienākums sniegt informāciju.** GDPR nosaka datu subjektu tiesības saņemt savu datu kopiju. Tādos gadījumos pārzinim nav tiesību prasīt paskaidrojumu par to, kādēļ datu subjektam nepieciešami izprasītie dati, kā arī nav nedz pienākuma, ne tiesību vērtēt, vai šie dati varētu būt noderīgi tiesvedības mērķim.

Informācija datu subjektam ir jāsniedz bez maksas, bet, ja pārzinis sastopas ar acīmredzami nepamatotiem vai pārmērīgiem datu subjekta pieprasījumiem, viņam ir tiesības vai nu atteikties izpildīt pieprasījumu, vai pieprasīt saprātīgu maksu, ņemot vērā administratīvās izmaksas, kas saistītas ar informācijas vai saziņas nodrošināšanu vai pieprasītās darbības veikšanu. Šajā gadījumā pārzinim ir jāsniedz motivēta atbilde, kādēļ pieprasījums ir acīmredzami nepamatots vai pārmērīgs.

Pārredzamības trūkums un komerciālo paziņojumu nosūtīšana bez tiesiska pamata

Valsts: **Francija**
Sods: **50 000 000 EUR**
Pirms datu apstrādes katram lietotājam ir tiesības saņemt informāciju par to, kā tiks apstrādāti viņa dati. Lai iegūtu informāciju par datu apstrādes mērķi, datu glabāšanas termiņu, komerciālu paziņojumu personalizēšanu, *Google* produktu lietotājiem bija jāveic 5–6 darbības, kas padarīja informāciju grūti sasniedzamu. Pieejamā informācija bija pārāk vispārīga un neskaidra. Atzīmējot «piekrītu» Google lietotnē, lietotāji deva savu piekrišanu visām apstrādes darbībām, ko veic *Google*. Taču GDPR paredz, ka piekrišana ir jāsaņem katram personas datu apstrādes nolūkam atsevišķi. Šāda piekrišana visām apstrādes darbībām ir pārāk plaša un nekonkrēta, tādēļ ir uzskatāma par nederīgu.

Ko varam mācīties no šīs situācijas?

■ **Vienkāršāk ir labāk.** Lietotājam adresētā informācija ir jāsniedz kodolīgā, viegli pieejamā un saprotamā veidā, izmantojot skaidru un vienkāršu valodu. Informācijai ir jābūt izvietotai tā, lai lietotājs varētu viegli tai piekļūt, neslēpjot to aiz daudziem klikšķiem.

■ **Konkrēta piekrišana.** Ne katra piekrišana, kas satur vārdus «piekrītu», ir derīga. Piekrišanai ir jābūt apzinātai, brīvi sniegtai, konkrētai un viennozīmīgai, t.i., lietotājam pirms piekrišanas sniegšanas ir jāsaprot, kāda informācija un kādiem tieši mērķiem tiks izmantota.

Ar detalizētu Francijas datu aizsardzības uzraugošās iestādes CNIL lēmuma izklāstu varat iepazīties DVI mājaslapā.

Datu aizsardzības sistēmas izveide ir ilgtermiņa process, kas jāpielāgo mainīgajiem riska apstākļiem. Ceram, ka šie padomi palīdzēs jums novērst atlikušos trūkumus datu aizsardzībā. ■

Foto no *Sorainen* arhīva