VISPĀRĪGĀ DATU AIZSARDZĪBAS REGULA

"MĒS JŪS VĒROJAM"

Svarīgākais, kas jāzina par datu regulas jeb GDPR stāšanos spēkā. Speciālisti atbild uz 12 aktuāliem jautājumiem. JANA SAULĪTE

Tas ir noticis. 25. maijs ir aiz muguras, un visā Eiropas Savienībā (ES) ir stājusies spēkā Vispārīgā datu aizsardzības regula (turpmāk – Regula; *General Data Protection Regulation* – GDPR). Dzīve rit savu ierasto gaitu. Iespējams, daži uzņēmumi un iestādes ir saņēmuši pirmos pieprasījumus no cilvēkiem sniegt informāciju par uzkrātajiem datiem, un tiek gatavotas pirmās atbildes, mēģinot saprast, ko un kā tad atbildēt. Dažas skolas paziņojušas, ka Regulas dēļ netiks uzņemtas nekādas bērnu fotogrāfijas, pašvaldību izdevumos vairs nevar uzzināt, kuram kaimiņam šomēnes 80 gadu jubileja. Vai Regulas prasību dēļ ir iestājies pasaules gals, kā vēl nesen tika sludināts?

Šī dokumenta galvenais mērķis ir ieviest vienotus fizisko personas datu apstrādes principus visā ES, jo līdz šim katra valsts rīkojās pēc saviem ieskatiem, kas ļoti apgrūtināja gan oficiālo iestāžu, gan uzņēmēju pārrobežu sadarbību. Regula attiecas uz jebkuru ES iedzīvotāju, uzņēmumu, iestādi un organizāciju. Ja esat darba devējs kaut vienam cilvēkam – jūsu rīcībā ir personas dati; ja jums ir līgumi ar klientiem – tas pats, jo dati nepieciešami līgumu noslēgšanai, un tā tālāk. Neskatoties uz to, tikai apmēram

10% Latvijas uzņēmumu īsi pirms 25. maija varēja paziņot, ka ir pilnībā sagatavojušies Regulas spēkā stāšanās mirklim, vēl 15% sacīja, ka tam gatavojas, bet 41% joprojām uzskatīja, ka tas uz viņiem neattiecas, – šādus datus maija vidū prezentēja zvērinātu advokātu birojs *Sorainen*.

VĀKT TIKAI NEPIECIEŠAMOS DATUS

Speciālisti uzsver – pirmais svarīgais solis ir audits, proti – saprast, kādi personas dati ir uzņēmuma rīcībā un kādiem mērķiem tie uzkrāti. Vai visi šie dati nepieciešami, lai uzņēmums spētu darboties? Vienkāršākais piemērs – vai darba līguma noslēgšanai ir nepieciešama cilvēka pases kopija? Vai jāglabā dati par klientiem, kam pirms pieciem gadiem izsniedzāt svētkos dāvanas, bet pēc tam kontaktus neesat uzturējuši? Nē? Tātad šādai informācijai plauktos un datoros nav jāatrodas, un tā ir jāiznīcina.

Otra lieta – vai dati ir pietiekami aizsargāti? Kas ar tiem drīkst darboties un cik lielā apmērā. Vai datu krātuves vietām ir drošas paroles un nodrošināta cita aizsardzība? Ja auditu nevar veikt pašu spēkiem, jāpiesaista eksperts no malas. Speciālisti uzsver – viens no Regulas mērķiem ir likt uzņēmumiem uzkrāt tikai tādus datus, kuru izmantošanas nepieciešamību var pierādīt. Nevis kraut kaudzē visu, kas kādreiz var noderēt.

Teiksiet – esmu mazais uzņēmējs, un viss par klientiem man glabājas planšetē. To lietoju tikai es, paroli neviens nezina, klientus visus pazīstu personīgi. Labi, bet vai planšetdators ir pietiekami aizsargāts no svešinieku piekļuves, ja izmantojat publisku bezvadu internetu? Ir vērts ieguldīt laiku un resursus, lai šos jautājumus sakārtotu un mierīgi dzīvotu tālāk.

"MĒS JŪS VĒROJAM"

Galvenā atšķirība no līdzšinējā regulējuma nav tikai uzņēmumu rīcībā esošo datu auditēšana. Viena no aspriestākajām tēmām ir plānotais soda apmērs par prettiesisku vai neatļautu datu apstrādi. Līdz šim vieglāk bija samaksāt nelielo sodu, nekā ieguldīt laiku un resursus procesu sakārtošanai. No 25. maija tas ir mainījies – maksimālais administratīvais naudas sods par datu apstrādes pārkāpumiem vai nelikumīgu to apstrādi var būt līdz 20 miljoniem eiro vai uzņēmuma gadījumā – līdz 4% kopējā apgrozījuma.

Būtiskākā nianse, pēc juristu domām, ir tas, ka datu pārzinim ir jāspēj pierādīt, ka datu apstrāde notiek tiesiski – tas jādara ar attiecīgiem dokumentiem, procedūru aprakstiem u.tml. Ir jābūt datu apstrādes reģistram, privātuma politikai utt.

Vēl viens būtisks jaunums – ir jāsniedz daudz vairāk informācijas: klientam, apmeklētājam, jebkuram cilvēkam ir tiesības zināt, kā notiek datu apstrāde un kādiem nolūkiem tā tiek veikta. Ja ēkā ir video novērošana, nepietiek vairs ar to, ka uz durvīm ir uzlīme ar brīdinājumu „Mēs jūs vērojam". Tā ir jāpapildina ar informāciju par datu pārzini un par to, kā un kur var uzzināt datu apstrādes principus konkrētajā vietā.

JĀATBILD 30 DIENU LAIKĀ

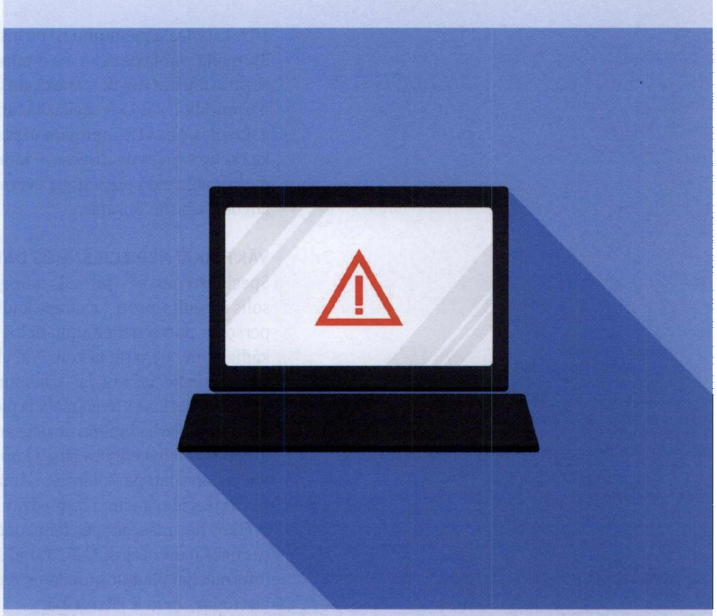
Kā jau minēts, datu pārzinim ir pienākums sniegt informāciju par personas datu apstrādi, ja šī persona to ir pieprasījusi. Kā norāda speciālisti – ja tiek saņemts fiziskas personas pieprasījums sniegt informāciju par datiem, kādi par viņu ir uzņēmuma rīcībā, atbilde ir jāsniedz 30 dienu laikā. Ja to neizdara, var sekot atbildīgās iestādes jeb Datu valsts inspekcijas pārbaude un pavisam slikta scenārija gadījumā – nonākt līdz civilprasībai tiesā.

Inspekciju interesēs arī, vai datu pārzinis ir izveidojis un uztur attiecīgu reģistru, kurā precīzi norādīts, kādi dati ir uzņēmuma rīcībā, kas ar tiem tiek darīts, kādas personas ir tiesīgas veikt apstrādi un kādā apmērā. Šāda reģistra prasības uzskaitītas Regulas 30. pantā.

Tiesa, IT speciālisti norāda – nevajag pārspīlēt un biedēt ar stāstiem par CV un dokumentiem datoros, kuri tagad visi ir jāuzmana un jāizgūst

(jāspēj atdot) personai. Patiesībā Regula runā par datubāzēm un lielapjoma datu glabāšanas vietām. Tajā ir uzskaitīti izņēmumi mazajam biznesam. Uzņēmuma datoros, e-pastos un dokumentos visur būs personas dati, un uzņēmumam būtu jāparūpējas par drošību pamatā (secure by design) šiem datoriem un dokumentu glabātavām, tās šifrējot un ierobežojot pieejas tiesības, bet datu izgūšana jāspēj nodrošināt no datubāzēm un strukturēti iegūtajiem datiem.

Ne Regula, ne arī topošais Personas datu apstrādes likums, protams, nespēj un nespēs paredzēt visas situācijas, kas ikdienā var rasties, daudz vietas paliek interpretācijai, normu tulkošanai un izpratnes veidošanai. Tāpēc *Kapitāls* vērsās pie dažādiem speciālistiem, aicinot skaidrot, kā uzņēmējam vai personai rīkoties dažādās situācijās, kas tiek piesauktas saistībā ar Regulu.



IEVA ANDERSONE, zvērināta advokāte, zvērinātu advokātu birojs *Sorainen*

1 Foto un video fiksācija publiskos pasākumos – kā rīkoties to organizētājiem un apmeklētājiem?

Pirmkārt, ne visas fotogrāfijas būs personas dati, nepārspīlēsim ar to, piemēram, ja tas ir kopskats no kāda notikuma ar daudziem cilvēkiem. Savukārt, ja tas ir portrets, pēc kura mani var pazīt kaimiņš, tie jau būs personas dati. Fotografēšanas labākais pamatojums ir leģitīmās intereses. Tās var būt, piemēram, vārda un preses brīvība. Jā, arī juridiskai personai – pasākuma rīkotājam – ir vārda brīvība: brīvība izplatīt informāciju par pasākumu, informēt par tā norisi, veidot materiālus vēsturei, arhīvam utt. Rīkotājam ir jāsaprot – vai tas ir publisks pasākums, kur var ierasties daudz cilvēku, lietišķa vide, vai ir plaša mediju iesaiste utt.

Vislabāk ir laikus, piemēram, jau ielūgumā, informēt, ka pasākuma laikā notiks fotografēšana un ka iegūtie materiāli tiks izmantoti publicitātei. Mana kā apmeklētāja tiesības ir to zināt un attiecīgi pieņemt lēmumu – iet vai neiet uz turieni. Tāpat jāatceras, ka apmeklētājam būs tiesības vērsties pie rīkotāja un lūgt dzēst kādu foto, taču visam jābūt saprāta robežās – diez vai būtu pareizi dzēst grupas bildi, jo tas nebūtu godīgi pret pārējiem fotogrāfijā esošajiem cilvēkiem.

2 Kā jaunā Regula ietekmēs medijus, īpaši tos, kurus saucam par dzelteno presi un kura lielākoties pārtiek no fotogrāfijām?

Lai kā mums nepatiktu dzeltenā prese, tā tomēr ir prese, un pie mums pastāv preses brīvība. Žurnālistiem un masu medijiem ir jāievēro datu apstrādes pamatprincipi – godīgi, paredzami, caurskatāmi arī jāsniedz informācija, bet nav spēkā visas detalizētās Regulā iekļautās prasības. Izņēmums ir spēkā tik tālu, kamēr žurnālistam šī datu apstrāde ir nepieciešama sabiedrības interesēs. Te būs tests – vai konkrētā informācija ir sabiedrības interesēs? Preses pārstāvjiem tas būs rūpīgi jāvērtē. Piemēram, ja kāds ar slēpto kameru nofilmē, kā kāds politiķis, kas ikdienā publiski iestājas par ģimenes vērtībām un tikumību, atpūšas kopā ar mīļāko. Tas varētu būt sabiedrības interesēs, tomēr katru reizi tas būs vērtēšanas jautājums, redaktora atbildība.

3 Vai turpmāk būs iespējams e-pasta mārketings? Kā Regula mainīs komerciālo paziņojumu izsūtīšanu?

Te jānošķir e-pasta mārketings fiziskajām un juridiskajām personām. Latvijā spēkā esošais Informācijas sabiedrības pakalpojumu likums nosaka, kā drīkst un kā nedrīkst sūtīt

komercinformāciju. Pamatnoteikums ir, ka juridiskajām personām var to sūtīt, ja e-pasta adrese iegūta legālā veidā, piemēram, uzņēmuma mājaslapā. Bet ikvienā savā komerciālajā e-pastā ir jānorāda atteikšanās iespēja.

Ja tiek sūtīts juridiskajai personai, piekrišana tās saņemšanai iepriekš nav jāprasa. Savukārt fiziskajai personai drīkst sūtīt tad, ja tā jau ir bijusi jūsu klients un piekritusi saņemt turpmāko informāciju. Un neaizmirstiet par atteikšanās iespējām. Jā, ikvienam ir tiesības pārdomāt jebkurā brīdī. Kamēr cilvēks nav atteicies, droši var sūtīt.

KRISTAPS SEDOLS, *Squalio* produktivitātes risinājumu speciālists

4 Kā Regula ietekmēs uzņēmumus, kas darbam ar dokumentiem izmanto mākoņpakalpojumus?

Atbildību par datu drošību uzņemas datu apstrādātājs, tātad šādā gadījumā – uzņēmums, kas nodrošina mākoņpakalpojumu. Turklāt svarīgi, lai jūsu sadarbības partneris atbilstu tādiem pašiem datu drošības kritērijiem, kādi ir jūsu uzņēmumā. Tāpat ir svarīgi, lai būtu līgumiskās saistības ar pakalpojumu sniedzēju. Ja jūs darba vajadzībām izmantojat privāto e-pastu – pats būsiet vainīgs, ja šī e-pasta sistēmas nodrošinātājam kaut kas notiks. Tāpēc, lai iegūtu līgumiskās saistības un būtu pārliecība, ka dati ir drošībā, labāk pirkt oficiālus mākoņpakalpojumu risinājumus biznesam. Ja problēma būs otrā pusē, viņiem par to būs jāuzņemas atbildība. Respektīvi – ārpakalpojumiem jābūt legāliem, un jābūt līgumattiecībām. Jo pēc pieprasījuma jums datu subjektam ir jāspēj norādīt, kur dati glabājas un uz kāda pamata. Vēl svarīgi, lai datu glabāšanas vieta atrodas ES, jo tad jau pēc noklusējuma tai ir jāatbilst visām Regulas prasībām.

EDIJS TANONS, SIA *Datakom* risinājumu direktors

5 Vai uzņēmējs arī turpmāk drīkst apstrādāt datus, lai piedāvātu klientiem piemērotus piedāvājumus, proti – veikt profilēšanu?

Datu profilēšanu varētu skaidrot ar šādu piemēru – agrāk mēs iepirkāmies pie vietējā veikalnieka, kas jau pēc mūsu sveiciena zināja, ka vēlamies svaigu pienu un garšīgo aitas desu, savukārt citam ikdienas pircējam zināja, ka viņa bērniem garšo burkānu čipsi. Tā ir profilēšana, bet bez datora. Šis veikalnieks pazina savus klientus, savā galvā bija tos sakārtojis un atcerējās. Pieaugot apjomam un veikalu izmēram, mēs zaudējām šo personīgo pieeju. Automatizētā pircēju segmentēšana un profilēšana cenšas šo personīgo pieskārienu atjaunot.

Regula savukārt saka – lūdzu, esiet godīgi un atklāti pret savu klientu un viņa profilu (datus) glabājiet droši un konfidenciāli! Regula nebūt neaizliedz to darīt, bet saka, ka vajag samērīgumu un nodrošināt cilvēka privātuma aizsardzību. Ja viņš vēlas nopirkt desu, tad to var izdarīt, arī neatdodot visas savas personas iezīmes.

Savukārt uzņēmējiem Regula pieprasa norādīt konkrēto mērķi katram datu gabaliņam, kas cilvēkam tiek prasīts. Tātad, ja uzņēmējam šos profilēšanas – lojalitātes – datus vajag, lai viņš strādātu labāk un iekārtotu veikalu ērtāk, viņam ir tādas tiesības, bet jābūt atklātam pret cilvēku, piedāvājot kontroli, aizsardzību viņa datiem.

6 Regula nosaka – datus drīkst glabāt tik ilgi, cik nepieciešams tam datu apstrādes nolūkam, kādam saņemta piekrišana. Kā noteikt šo termiņu, un vai par to jābrīdina datu subjekts? Vai termiņu var noteikt pats datu pārzinis, vai ir kādi ārēji noteikumi?

Ja uzņēmējam dati ir nepieciešami kādam konkrētam likumīgam nolūkam vai klients ir piekritis savu informāciju iedot, tad to drīkst glabāt. Piemēram, likums nosaka, ka grāmatvedībai nepieciešamā informācija – arī personas dati – jāglabā piecus gadus, tad uzņēmējs izpilda likumu, bet pēc tam ziņas iznīcina. Otrs piemērs – mums ir lojalitātes sistēma, kurai cilvēki sniedz savu brīvu piekrišanu. Tādā gadījumā datus glabā tik ilgi, kamēr vien šī piekrišana nav atsaukta.

7 Kā jāorganizē informācijas nodošana no viena datu turētāja/apstrādātāja citam? Vai jāmaina spēkā esošie līgumi, vai tiem jāveido kādi pielikumi?

Īsā atbilde – jā, jāmaina līgums, jāparedz atruna par datu aizsardzību, drošības standartiem/prasībām un obligātu dzēšanu uzreiz pēc tam, kā beidzies datu apstrādes mērķis. Savukārt par datu apmaiņu cilvēkam jāpastāsta atklāti, vienkāršā un saprotamā valodā, kādā veidā uzņēmums nodrošinās šīs pārsūtītās informācijas konfidencialitāti.

JA JŪS DARBA VAJADZĪBĀM IZMANTOJAT PRIVĀTO E-PASTU – PATS BŪSIET VAINĪGS, JA ŠĪ E-PASTA SISTĒMAS NODROŠINĀTĀJAM KAUT KAS NOTIKS. LAI BŪTU PĀRLIECĪBA, KA DATI IR DROŠĪBĀ, LABĀK PIRKT OFICIĀLUS MĀKOŅPAKALPOJUMU RISINĀJUMUS

LĀSMA DILBA, Datu valsts inspekcijas direktores vietniece

8 Veikaliem un pakalpojumu sniedzējiem ir klienta kartes. Tagad prasa vēlreiz aizpildīt anketas un apstiprināt savus datus. Ja es nepiekrītu kādu ziņu sniegšanai (dzimšanas gads, dzīvesvieta u.c.), tad reizēm šādu karti atsaka izsniegt. Vai tas ir leģitīmi?

Jā, tas ir leģitīmi. Šādā gadījumā kā tiesiskais pamats personas datu apstrādei (ievākšanai, glabāšanai un izmantošanai) var būt tikai paša cilvēka piekrišana. Ja tās nav – karti neizsniedz. Var, protams, diskutēt par pieprasīto datu apjomu – vai tiešām tie visi vajadzīgi pakalpojuma sniegšanai? Bet tas jau ir katra konkrēta pakalpojuma sniedzēja izvērtēšanas jautājums.

9 Ko darīt, ja tiek atklāta datu noplūde? Elementārs piemērs – uzņēmumam ir klientu datubāze, kuru negodprātīgs darbinieks ir pārkopējis un paņēmis līdzi, aizejot strādāt uz citurieni.

Primāri ir jāveic visi iespējamie pasākumi, lai novērstu vai maksimāli samazinātu nelabvēlīgo ietekmi uz personas tiesībām. Protams, jāinformē tiesībaizsardzības iestādes, jāpārskata iekšējie noteikumi par datu apstrādes drošību un tehniskie risinājumi informācijas sargāšanai.

Regula nosaka, ka pārkāpuma gadījumā datu pārzinis „bez nepamatotas kavēšanās un, ja iespējams, ne vēlāk kā 72 stundu laikā no brīža, kad pārkāpums tam kļuvis zināms", informē par to uzraudzības iestādi. Ja paziņošana nav notikusi 72 stundu laikā, jāpaskaidro kavēšanās iemesli. Atsevišķos gadījumos, kas aprakstīti Regulas 34. pantā, pārzinim jādara zināmi arī apdraudētie datu subjekti.

IVONNA BIBIKA, *Exigen Services Latvia* biznesa attīstības direktore

10 Vai regulas noteikumi attiecas uz uzņēmēju, kas darbā izmanto *Google Adwords* vai līdzīgus *online* reklāmas rīkus? Kā saprast – kurā brīdī es esmu vienkārši *Google* klients, kas izmanto viņu produktu, bet kurā – jau datu pārzinis? Vai varbūt uz šo gadījumu Regulas prasības vispār neattiecas?

Prasības attiecas arī uz tiešsaistes reklāmas rīkiem. Ir jānodrošina, ka var atteikties no šādas iespējas. Savukārt, piemēram, uzņēmuma mājaslapa piedāvā lielāku brīvību, jo mēs ļaujam izvēlēties – apmeklēt vai neapmeklēt attiecīgo vietni.

11 Kādas šobrīd ir lielākās problēmas Latvijas uzņēmumos un iestādēs attiecībā uz datu drošību?

Viena no lielākajām problēmām varētu būt tā, ka uzņēmumi ir iešūpojušies nedaudz par vēlu, jo veiksmīgai Regulas ieviešanai un ievērošanai vajadzīgs pietiekami ilgs apzinātības periods. Lielākie izaicinājumi varētu būt saistīti ar to, ka ne visi saprot, kas pēc definīcijas ir personas dati, jo tie ir pietiekami plaši interpretējami. Piemēram, sīkfailu identifikācijas numurs ir šīs personas datu atribūts. Līdz ar to šīs nianses pagaidām ir tikai daļēji skaidras.

Tāpat jāņem vērā vēl vairāki apstākļi: pirmkārt, statiskas situācijas apzināšana – kādi dati ir pieejami, un kas tiem var piekļūt; otrkārt, Regulas process, kas nosaka, ko drīkstam darīt ar šiem datiem. Ar pirmo daļu esam tikuši galā, bet pie otrās – procesu raksturojošās – daudziem vēl ir jāpiestrādā. Ja salīdzina Fizisko personu datu aizsardzības likumu, kas bija saistošs iepriekš, un Regulu, tad otrajai prasības ir nesalīdzināmi augstākas.

12 Vai ir kāda joma, kurā paredzamas būtiskas problēmas pēc Regulas stāšanās spēkā?

Manā skatījumā lielākie izaicinājumi varētu būt medicīnā, jo tur ir liels sensitīvo datu apjoms. Piemēram, ārsta vizīte – terapeits uzklausa mūs un norīko pie traumatologa, kurš savukārt neredz slimības vēsturi. Tajā pašā laikā, lai konkrētais speciālists varētu izdarīt slēdzienu, viņam nepieciešams pietiekami daudz datu: vecums, ārstēšanas vēsture u.c. Protams, izmantojot biznesa inteliģences risinājumu iespējas, var definēt atsevišķi, kura persona konkrētiem datiem tiek vai netiek klāt, bet, tīri teorētiski raugoties no Regulas viedokļa, tas ir pārkāpums.

Šie ir tie bremzējošie faktori, kur nepieciešams aktīvāks *Lean* princips – nedarām vairāk, kā nepieciešams. Tāpat būtiski ir nodrošināt informācijas vidi, kurā ārsti varētu veiksmīgi sadarboties un apmainīties ar vajadzīgajiem datiem, kas ne vienmēr ir triviāli. Īpaši ņemot vērā, ka šīs ziņas var atrasties atšķirīgās sistēmās. Svarīgi, lai Regulas prasību izpilde nekavētu ārstēšanās procesu un neliegtu speciālistiem pieņemt kvalitatīvu lēmumu. K

TERAPEITS NORĪKO PIE TRAUMATOLOGA, KURŠ SAVUKĀRT NEREDZ SLIMĪBAS VĒSTURI. LAI KONKRĒTAIS SPECIĀLISTS VARĒTU IZDARĪT SLĒDZIENU, VIŅAM NEPIECIEŠAMS PIETIEKAMI DAUDZ DATU: VECUMS, ĀRSTĒŠANAS VĒSTURE U.C.