

# MĀCĪSIMIES DAROT

JAUNĀ ES DATU REGULA LIEK UZŅĒMUMIEM NOPIETNI PĀRVĒRTĒT — KĀPĒC UN KĀDA INFORMĀCIJA TIEK IEVĀKTA PAR KLIENTIEM VAI CITĀM PERSONĀM

**V**isā Eiropas Savienībā 25. maijā stāsies spēkā Vispārīgā datu aizsardzības regula (*General Data Protection Regulation*), kurai nav gatava vairāk nekā puse reģiona uzņēmumu un iestāžu — vismaz tā liecina pētījumu kompānijas *Gartner* vērtējums, un Latvija nav izņēmums.

Kaut gan jau tagad darbojas Fizisko personu datu aizsardzības likums, jaunais regulējums paredz vairākas būtiskas atšķirības. Regula nosaka daudz plašāku pienākumu un atbildības apjomu jebkādu personas datu apstrādātājiem. Šīs izmaiņas jo īpaši skars visdažādākos ārpalpojumu sniedzējus, kuru darbība ir saistīta ar personas datu apstrādi.

Pirmkārt, regula ir tieši piemērojama visās ES dalībvalstīs, tātad tām vairs nebūs iespēju noteikumus brīvi interpretēt. Vienlaikus regula neizslēdz dalībvalstu tiesības pieņemt nacionāla līmeņa tiesību aktus par dažiem aspektiem. Piemēram, tas attiecas uz sodu apmēru — regulā norādītais sods ir vienāds visās dalībvalstīs, līdz 4% no kompānijas starptautiskā apgrozījuma vai 20 miljoniem eiro (atkarībā no tā, kurš ir lielāks). Tomēr advokātu biroja *Cobalt* juriste un sertificēta personas datu aizsardzības speciāliste Anna Vladimirova-Krjukova stāsta, ka, cik zināms no Latvijas jaunā likumprojekta, sodi būs krievu mazāki. Regulas tiešā piemērojāmība arī nozīmē, ka visi, kam ir pienākums nodrošināt atbilstošu

personas datu apstrādi, tagad būs pienākums pārzināt ne tikai Latvijas normatīvos aktus, bet arī pašu regulu. Tas nav viegls uzdevums, ņemot vērā ES aktu īpašo valodu.

Otrkārt, regula tiks piemērota ne tikai attiecībā uz ES, bet arī uz jebkurām pasaulē esošajām personām, kuras piedāvā preces vai pakalpojumus fiziskām personām ES vai veic viņu uzvedības novērošanu, ja tas notiek ES. Tas automātiski ietver tiešsaistes veikalus, starptautisko lojalitātes programmu piedāvājumu sniedzējus, Eiropas uzņēmumu sadarbības partnerus. Tomēr Vladimirova-Krjukova spriež, ka joprojām aktuāls ir jautājums, cik reāli būs iespējams piemērot regulas prasības šādām ārzemju personām.

Runājot par konkrētām jaunām prasībām, atbildīgajām personām būs pienākums sniegt daudz plašāku informāciju par darbībām ar personu datiem, kā arī informēt par datu aiz-

**«Visi saprot, ka pārdot svešu mašīnu bez īpašnieka atļaujas nav likumīgi, bet par datiem tādā virzienā nedomā, lai gan datu subjektam ir vairākas tiesības, kas ierobežo tādu biznesu»**

sardzības incidentu 72 stundu laikā. Latvijā par to būs jāziņo Datu valsts inspekcijai un *CERT.LV*.

## IEMESLI DOMSTARPĪBĀM

Galvenais izaicinājums — uzņēmumi bieži vien pat neapzinās, kādi dati tiem vispār ir un kā uzņēmumu biznesa modeļiem sadzīvot ar normatīvo aktu prasībām, saka Vladimirova-Krjukova.

Pirmā problēma raksturīga lieliem uzņēmumiem un to grupām, kuri parasti darbojas kopš tiem laikiem, kad informācijas aprīte notika galvenokārt papīra formā. Šobrīd šādiem uzņēmumiem ir milzīgs papīra informācijas apjoms, kura sakārtošana aizņem ļoti daudz laika. Ar milzīgu datu apjomu saskaras arī tie uzņēmumi, kuri veido rezerves kopijas. Aktuāls ir arī darbinieku plūsmas jautājums — ja uzņēmumā tikai konkrēti darbinieki zina, kas un kā notiek ar personas datiem un šī informācija netiek nekā citādi fiksēta, tad darbinieku nomainīšanas gadījumā paredzamas nopietnas grūtības.

Otrā problēma saistīta ar uzņēmumiem, kuru galvenais pakalpojums ir datu pārdošana. Tie var būt dati par personu parādēm, kontaktinformāciju (dažreiz arī dzīvesvietas adresēm), pirkšanas ieradumiem.

«Visi saprot, ka pārdot svešu mašīnu bez īpašnieka atļaujas nav likumīgi, bet par datiem tādā virzienā nedomā, lai gan datu subjektam ir vairākas tiesības, kas ierobežo tādu biznesu,» secina Vladimirova-Krjukova.

Līdz ar to konfliktu iespējamība starp uzņēmumiem un fiziskām personām, kā arī uzņēmumiem un uzraudzības iestādēm ir liela — prakses ir maz, normatīvos aktus var interpretēt diezgan plaši. Viss atkarīgs no tā, cik aktīvi datu subjekti izmantos savas tiesības un kāda būs DVI pieeja. Tas pats attiecas arī uz sodiem, jo neviens pagaidām nezina, vai Latvijā tā būs realitāte.

IT uzņēmuma *Squalio* speciālista Pētera Tāra ieskatā visvairāk neskaidriību varētu būt attiecībā uz risku novērtēšanu uzņēmumos, kopējās datu uzskaites vešanas veidu — kad, vai un cik daudz uzņēmumiem jāatbild uz datu subjektu pieprasījumiem. Piemēram, kā rīkoties, ja uzņēmumam ienāk 100 pieprasījumu no datu subjektiem, kuros lūgts sniegt informāciju par šo





## KO SAKA INSPEKCIJA?

Vispārīgajā datu aizsardzības regulā nav noteikts precīzs pasākumu kopums, kas jāveic, lai nodrošinātu personas datu aizsardzību. Kopumā vispārīgie datu aizsardzības principi paliks nemainīgi, vienlaikus regula paredz datu subjektiem (fiziskām personām, kuru dati tiek apstrādāti) plašākas kontroles tiesības pār saviem datiem, piemēram, tiesības uz datu dzēšanu vai pārnēsamību. Papildus tam regulā ir iestrādāts pārskatatbildības princips. Tas paredz, ka pārzinim ir pienākums nodrošināt tādu personas datu apstrādes procesu organizāciju, kas ļauj pierādīt, ka personas datu apstrāde atbilst datu aizsardzības prasībām. Datu valsts inspekcijas galvenais uzdevums ir veicināt personas datu aizsardzības prasību ievērošanu, izmantojot «konsultē vispirms» principu. Galvenais nav sodīt, bet gan būt uzņēmēja palīgam un sadarbības partnerim.

AVOTS: DATU VALSTS INSPEKCIJA

## KĀDI IR UZŅĒMUMU PIENĀKUMI, UN AR KO SĀKT?

- 1 Uzņēmumam ir pienākums **dokumentēt**, kādi personu dati atrodas tā rīcībā, no kurienes tie rodas un kam tālāk tiek nodoti.
- 2 Pārlicinieties, vai jūsu procedūras **atbilst jaunajām prasībām**, tajā skaitā individuāliem tiesībām pieprasīt savu datu dzēšanu vai izsniegšanu.
- 3 Izvērtējiet, kā **apkalposit** personu pieprasījumus, lai varētu laikus sniegt atbildes.
- 4 Lai atbilstu regulas prasībām, jums jāidentificē **likumīgs pamats** datu apstrādes veikšanai un šis process jādokumentē.
- 5 Personām ir jāsniedz **piekrišana** savu datu apstrādei — pārbaudiet, vai pašreizējās procedūras atbilst regulas standartiem.
- 6 Pārlicinieties, vai jums ir atbilstoša sistēma, lai atklātu un **izmeklētu** datu apstrādes pārkāpumus.
- 7 Uzņēmumā kādam darbiniekam ir jāuztic **atbildība** par datu aizsardzības ievērošanu.

VAIRĀK: PREPARING FOR THE GENERAL DATA PROTECTION REGULATION (GDPR): 12 STEPS TO TAKE NOW

personu datu apstrādi? Šo nosacījumu var izmantot arī ļaunprātīgi. Atbilde ir jāsniedz mēneša laikā.

### KAUT KO VAR PASPĒT

Visvieglāk un ātrāk lietas varēs sakārtot uzņēmumi, kam ir maz darbinieku un maz klientu. Sakārtošanai nepieciešams ieviest kontroli attiecībā uz to, kādi personas dati uzņēmumam ir, fiksēt šo informāciju centralizēti. Pēc tam jāpārlicinās, ka datu apstrādei ir likumīgs pamats un nolūks, jānosaka personas datu glabāšanas termiņi, jāseko datu atrašanās vietai un jāizstrādā nepieciešamie dokumenti. Galvenais, iesaka Vladimirova-Krjukova, ir definēt personas datu apstrādes pamatprincipus, lai izvairītos no haotiskas apstrādes.

Piemēram, *Maxima* veikaliem, kas ir viens no lielākajiem uzņēmumiem un darba devējiem Latvijā, apjomīgākais jautājums bija tieši klientu datu apstrāde, jo pircēji var piedalīties lojalitātes programmā, un tas ir ļoti ievērojams datu apjoms.

Savukārt *Squalio* speciālisti, analizējot savu saimniecību, secināja — vismazāk piepūles datu apzināšanā un procesu sakārtošanā prasa tās programmatūras, kuras jau pēc savas būtības paredz datu apstrādi, konkrētas darbības ar tiem un pat likumā noteiktu datu aizsardzības prasību izpildi (grāmatvedības programmas, personālvadības sistēmas, CRM — klientu datu bāzes utt.). Uzņēmums arī pārskatīja iekšējās procedūras, lai

saprastu, vai no juridiskā aspekta viss ir kārtībā.

Tārs norāda, ka uzņēmumiem jāsniedz ar to, ka darbinieki jāapmāca par datu aizsardzības prasībām, lai visi saprot, par ko vispār ir uzņēmuma bažas un kādus procesus tas ievieš. Piemēram, tādā sensitīvā nozarē un uzņēmumā kā Vidzemes slimnīca darbinieki ir apmeklējuši seminārus par datu aizsardzību, un šobrīd joprojām notiek organizatoriskais darbs, lai precizāk noteiktu riska jomas un nepieciešamos papildu pasākumus. Ir paredzēts arī informācijas sistēmas audits. Skaidrs, ka līdz maijam var sakārtot datu apstrādes kārtību uzņēmumā, «kāda tā ir šodien», bet datu apstrādes un aizsardzības process būs jāturpina arī pēc tam. ●