DATU AIZSARDZĪBA: VISS TIKAI SĀKAS

Pēc šā gada 25. maija, kad stājās spēkā jaunā Eiropas Vispārīgā datu aizsardzības regula (GDPR), daudzi uzņēmumi, īpaši mazie, apmulsa un uzdeva sev daudzus jautājumus. Vai kompānija ir gatava aizsargāt savu klientu personiskos datus? vai uzņēmums ir pilnībā gatavs jaunajai regulai un kā par to pārliecināties? vai arī turpmāk ir jāpievērš uzmanība GDPR vai arī tas ir vienreizējs process? ar ko draud normu neievērošana? Izprast šo tēmu žurnālam L'Officiel Hommes *palīdzēja eksperti – uzņēmuma* Squalio *datu aizsardzības speciāliste Marina Briškena un advokātu biroja* Sorainen *partneris Agris Repšs.*

Teksts OLGA KŅAZEVA

DROŠĪBA – NE TIKAI UZ CEĻA

Īsumā: GDPR (*General Data Protection Regulation*) ir vispārīgs datu aizsardzības reglaments, kas apraksta personiskas informācijas savākšanas, apstrādes un glabāšanas noteikumus. Pēc tā stāšanās spēkā visus šos iepriekšminētos pasākumus veikt un – vēl jo vairāk – nodot (vai pārdot) personisku informāciju drīkst tikai ar lietotāja piekrišanu. Turklāt lietotājam jāsaņem paskaidrojums, kādiem mērķiem viņa dati tiks izmantoti.

Uzņēmumam – gan lielam, gan mazam – regula nozīmēja ne tikai jaunu iekšējo noteikumu izveidi, bet arī darbinieku apmācību darbam ar datiem, kā arī IT sistēmu drošības pārbaudi.
Varētu šķist – nekā jauna. Jo arī iepriekš likumdošanā bija noteiktas pietiekami stingras prasības datu aizsardzībai, un ar tiem «mētāties» nebija atļauts. Arī tagad gan Latvijā, gan citur ES ir spēkā likums par datu aizsardzību, kura darbību pie mums kontrolē Datu valsts inspekcija. Taču normatīvajos aktos nebija ņemti vērā visi riski, kuri varētu rasties personas datu ievākšanas, glabāšanas, apstrādes, lietošanas un nodošanas procesā. Tas tad arī ir cēlonis daudziem skandāliem, kurus izraisīja plašas datu noplūdes.

ARĪ MILŽIEM GADĀS NOPLŪDES

Šādu skandālu nebija maz. Te ir vietā atgādināt, ka 2016. gadā hakeri uzlauza *Uber* datubāzi un piekļuva 57 miljonu klientu vārdiem, uzvārdiem, elektroniskā pasta adresēm un mobilo tālruņu numuriem, kā arī 600 tūkstošu

2017. gada pavasarī kibernoziedznieki no Lietuvas plastiskās ķirurģijas klīnikas Grožio Chirurgija *nozaga pacientu datus, viņu fotogrāfijas, to skaitā kailfotogrāfijas, fotogrāfijas «pirms» un «pēc» un izlika tās pārdošanā «tumšajā» internetā.*

taksometru šoferu personiskajiem datiem, ieskaitot informāciju par licencēm. Par šo incidentu publiski kļuva zināms tikai 2017. gadā – izrādās, kompānija *Uber* samaksājusi hakeriem 80 000 eiro, lai nozagtie dati tiktu iznīcināti un nekad netiktu izmantoti.

2017. gada pavasarī kļuva zināms, ka kibernoziedznieki no Lietuvas plastiskās ķirurģijas klīnikas *Grožio Chirurgija* nozaguši pacientu datus, viņu fotogrāfijas, to skaitā kailfotogrāfijas, fotogrāfijas «pirms» un «pēc» un izlikuši tās pārdošanā «tumšajā» internetā jeb *dark web*. Cena – no 50 līdz 2000 eiro par pacienta kartīti, jāpiebilst, ka pacienti bija gan vietējās, gan starptautiskās slavenības. Par kiberuzbrukuma upuriem kļuva pat tādi globālie giganti kā auditorfirma *Deloitte*, kad tika uzlauzta korporatīvā e-pastu sistēma. Tiek uzskatīts, ka hakeri, visticamāk, ieguvuši informāciju par kompānijas turīgākajiem klientiem jeb

FOTO: © PANTHERMEDIA.NET / ANDRIY POPOV / REUTERS/SCANPIX/LETA

blue chips – uzvārdus, paroles, personas datus, konfidenciālu saraksti. Pērnā gada augustā Zviedrijā konfidenciālu datu noplūdes dēļ amatu zaudēja iekšlietu ministrs Anderss Igemans, infrastruktūras ministre Anna Johansone un Nacionālās transporta aģentūras vadītāja Marija Agrēna.

Nepatīkams incidents notika šā gada septembrī, kad GDPR jau bija ieviesta visā ES. Par hakeru upuriem kļuva lidsabiedrības *British Airways* klienti, kuru personas datus un kredītkaršu informāciju ļaundari nozaga. Datu noplūde varēja skart vismaz 380 tūkstošus *British Airways* klientu.
Ja jau problēmas ar datu aizsardzību ir lielām kompānijām, tad ko gan lai saka par mazo biznesu, kur reti kurš vispār pievērš uzmanību tam, kā glabājas iekšējā informācija. Pēc šā gada 25. maija situācija būtiski mainījās.

PROCESS DZĪVES GARUMĀ

Izrādījās, ka bizness šīm izmaiņām nebija gatavs. Šā gada aprīlī aptaujā, ko vairāk nekā tūkstotim kompāniju, ko veica *McDermott Will & Emery* juristi un datu aizsardzības pētniecības institūts *Ponemon Institute*, atklājās, ka vairāk nekā 60 procenti tehnoloģiju kompāniju neatbildīs regulas prasībām datumā, kad tā stājas spēkā. Latvijā veikta aptauja īsi pirms regulas stāšanās spēkā atklāja vēl skumjāku ainu: tikai 10% uzņēmumu bija gatavi GDPR. Taču atlikušajiem 90% nevajadzētu krist izmisumā: ir jāsāk darboties.
Eksperti uzskata, ka uzņēmumu gatavība GDPR un atbilstība šīs regulas prasībām ir mērķis, kuru uzreiz ir grūti sasniegt. Tehnoloģijas attīstās, līdz ar tām mainās arī kibernoziedznieku iespējas piekļūt datiem, tādēļ gan juridiskos, gan IT procesus – un to atbilstību GDPR – būs jāpārskata pietiekami regulāri. Iespējams, pat reizi vai divas gadā, uzņēmumā veicot iekšējo auditu.
Visinteresantākais: daudzi uzņēmumi – līdz 25. maijam tādu bija 41% – uzskata, ka vispār neapstrādā personas datus. Tā ir kļūda. Jo, kā liecina statistika, GDPR ir attiecināma uz 99% uzņēmumu.
Nav būtiski, kādā jomā uzņēmums darbojas, cik tam ir darbinieku un klientu. Būtiskākais ir, lūk, kas: ja kompānijai ir kaut jel kāda informācija ar personas datiem, jaunās regulas prasības uz to attiecas automātiski. Pat ja jūs sastādāt viesu sarakstu pasākumam, jūs jau apstrādājat personas datus. Ja ierakstījāt savus darbiniekus burtnīciņā – arī tie ir personas dati. Citiem vārdiem sakot, no GDPR izvairīties neizdosies.
Piemēram, uzņēmumam ir klientu, atsauksmju vai piedāvājumu anketu datu bāze, klientu lojalitātes programmas dati, elektroniskā pasta vēstules, fotogrāfijas, videoieraksti no novērošanas kamerām vai vienkārši darbinieku saraksti ar personas datiem, piemēram, personas kodiem.
Ja personas datus sakārto «pa plauktiņiem», tad tie ir izvietojami šādā kārtībā: vārds, uzvārds, telefona numurs, elektroniskais pasts, dzīves vietas adrese, automašīnas reģistrācijas numurs, bankas konta numurs, norēķinu kartes numurs/derīguma termiņš, ziņas par slimību vēsturi, asinsgrupu, informācija par ģimenes locekļiem, ārējais izskats, foto un video materiāli, biometriskie dati, visi pases dati un visa informācija par ģimenes locekļiem. Ar vienu vārdu sakot, faktiski jebkura informācija par cilvēku.

KAD IZMĒRAM IR NOZĪME

Jautājums, kas uztrauc daudzus uzņēmumus, ir šāds: kurš būs tas brīnumdaris, kas tiks skaidrībā ar visām visnotaļ komplicētās regulas gudrībām un niansēm? Visvieglākais ceļš – noalgot īpaši apmācītu cilvēku, *Data Protection Officer* (DPO), jo viņam labāk par citiem vajadzētu zināt, kā GDPR prasības piemērojamas konkrētam uzņēmumam. Viņš sekos jaunu normu ievērošanai un, iespējams, firma ietaupīs prāvus līdzekļus, nepieļaujot būtiskas kļūdas ar personas datiem.
Taču eksperti saka, ka patlaban Latvijā šādu speciālistu ir ļoti maz. Latvijas augstskolās DPO speciālistus nesagatavo, un šī tātad ir visai deficīta profesija. Turklāt izvēle – algot vai nealgot šādu speciālistu – ir atkarīga nevis no paša uzņēmuma lieluma, bet gan no apstrādājamās informācijas apjomiem. Var gadīties, ka kompānijā strādā desmit darbinieku, toties klientu ir daudz un tiek apstrādāts simtiem reižu vairāk datu nekā uzņēmumā ar simts strādājošajiem.
Var lūgt palīdzību juridiskajai kompānijai, kas specializējusies datu aizsardzības jautājumos; tas būs viens no ārpakalpojumu variantiem. Taču šādā gadījumā jābūt pilnīgi atklātam pret speciālistu no malas, maksimāli tam jāzucticas, lai viņš varētu sakārtot datu aizsardzības jomu. Tas, kā secinājuši eksperti, vienmēr neizdodas, jo uzņēmumi bieži vien paši nesaprot, kas tiem ir vajadzīgs.

Arī uzņēmumu darbinieku dzimšanas dienas drīkst svinēt tikai ar viņu atļauju, jo arī šis datums ir konfidenciāla informācija.

PALĪDZI SEV PATS

Ja datu apjoms uzņēmumā nav pārāk liels, var mēģināt tikt galā pašu spēkiem. Vispirms ar neliela audita palīdzību jāizvērtē iekšējie riski. Piemēram, jāveic darbinieku aptauja, lai noskaidrotu, kādus personas datus viņi vāc un apstrādā, un – kādiem mērķiem. Ja mērķi nav skaidri, iespējams, šie dati nav obligāti vajadzīgi. Tad labāk tos neglabāt, nevis atstāt «katram gadījumam».
Tālāk pie uzņēmuma partneriem, kuri apstrādā datus uzņēmuma uzdevumā (piemēram, mārketinga uzņēmumi, kuriem tiek nodoti klientu dati pārdošanas aktivitātes paaugstināšanai) jānoskaidro un jāvienojas par to, kā sagatavojami līgumu papildinājumi, lai tajos būtu iekļautas jaunās regulas prasības.