

Datu krātuvēs haoss un kārtība – puse uz pusi

Tuvojas Vispārīgā personas datu aizsardzības regula

IMANTS VĪKSNE,
analītiskās žurnālistikas darbnīca „6K”

Krūtīs. Pa kreisi – dabīgas, pa labi – skalpeļa uzlabotas. Vēderi, dībeni, deguni, ausis, dzimumorgāni. Pirms un pēc. Arī Latvijas advokātu kantori glabā turīgu cilvēku noslēpumus par hakeru iebrukumiem ārstniecības iestāžu datu sistēmās. Taču mūsu klīnikām ar šantāžas gadījumiem līdz šim izdevies tikt galā konfidenciali, bet lieka trokšņa un publiska kaitējuma klientiem. Ne tā kā Lietuvā.

Informācijas laikmetā nav vērtīgākas preces par informāciju. To varbūt pagaidām neapzinās visi datu īpašnieki, turētāji un apstrādātāji, taču noziedznieki gan. Un gadījums ar nozagtajām pirms un pēc operāciju bildēm Lietuvas klīniku tīklā „Grozio Chirurģija” ir tam apliecinājums. Paviršības vai ļaunprātības dēļ klīniku iekšējā datortīkla izveidotāji bija atstājuši brīvus pieejas kodus. Tiem varēja piekļūt katrs hakeris ar elementārām zināšanām, un konkrētajā gadījumā tas izrādījās Krievijas izselsmes grupējums „Isar Team”. Vai vismaz uzdevās par to.

Personu datus zog arī Latvijā

Par 25 000 fotogrāfiju noziedznieki pieprasīja samaksu kriptovalūtā. 300 bitkoīnus, kas tobrīd bija aptuveni 616 tūkstošus eiro vērti. Klīnika maksāt atteicās, un noziedznieki sāka apstrādāt klientus pa vienam, bilžu cenu nosakot līdz 2000 eiro atkarībā no upura personības. Cietušo vidū esot arī daudz slavenību, tostarp no Liebrītnījas, un par slavu, protams, jāmaksā vairāk. Apliecinot savu noziedzīgo nolūku noziedznieku, daļu bilžu hakeri publicēja martā. Klīnika datu noplūdi sākotnēji noliedza, un maijā sekoja nākamā porcija. Šā digitālā uzbrukuma sekas joprojām nav novērstas. Visi iesaistītie hakeri nav apcietināti. Šantāža turpinās, arī klientu tiesvedības pret klīniku. Kontekstā ar jauno Vispārīgo datu aizsardzības regulu*, kas stāsies spēkā 25. maijā, šo notikumu ir pētījis advokātu biroja „Sorainen” partneris, zvērināts advokāts **Agris Repšs**. Viņš ir pārliecināts, ka datus zog arī Latvijā, kur datu aizsardzības līmenis ir zems. Taču uzņēmumiem vienkāršāk ir samaksāt noziedzniekiem, nekā pazaudēt klientu datus un reputāciju, tāpēc par šādiem notikumiem tiek klusēti. „Pērn paši esam konsultējuši divus lielus starptautiskus uzņēmumus šādu incidentu gadījumos,” stāsta advokāts. Cilvēki, kuru informācija tiek nozagta, iespējams, pat neuzzina, ka bijuši par šantāžas objektu un ka jutīga privāta informācija bijusi briemās. Turpmāk situācijai jāmainās. Par datu incidentu 72 stundu laikā jāziņo gan uzraudzības iestādei, kas Latvijas gadījumā ir Datu valsts inspekcija, gan datu subjektam – cilvēkam, kura fotogrāfijas „pirms un pēc” nozagtas. Vai jebkādi citi būtiski dati. Viņam par to pienāksies arī kompensācija, bet uzņēmumam par datu apstrādi pielautajām paviršībām – pamatīgs sods, kas atkarībā no pazaudēto datu apjoma un nozīmības var sasniegt līdz pat 4% no uzņēmumu grupas gada apgrozījuma jeb

20 miljonus eiro. Eiropas Savienība ir skaidri pateikusi: turpmāk dalībvalstīm pret datu vākšanu, apstrādi un aizsardzību jāizturas ar vislielāko nopietnību, un tas attiecas ne tikai uz valstu valdībām, bet ikvienu juridisku personu. Regulu nepiemēro tikai atsevišķās izņēmuma situācijās, piemēram, personas datu apstrādei, ko veic fiziska persona „tikai personiska vai mājsaimnieciska pasākuma gaitā”.

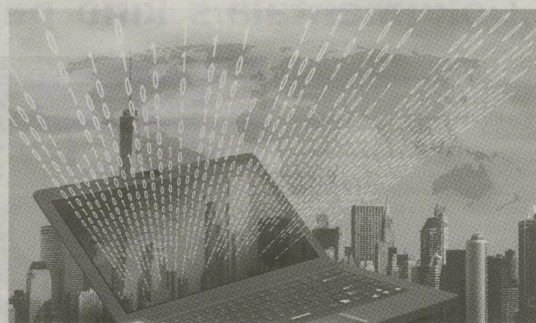
Iespēja sakārtot saimniecību

Mūsdienās katrs uzņēmums apstrādā personu datus. Gan savu darbinieku, savu klientu, arī konkurentu klientu datus. Tātad jaunā regula attiecas uz katru uzņēmumu, tikai atkarībā no apstrādāto datu daudzuma atšķirsies ar tiem saistīto pienākumu apjoms. Kas ir dati? Faktiski jebkura faktu kombinācija, ar kuras palīdzību iespējams identificēt personu. Vārds, personas kods, adrese, mašīnas numurs, ārsta recepte, seksuālā orientācija, bilde sociālajā tīklā, nemaz nerunājot par fotogrāfijām skaitu ma klīnikas datu bāzē. Šī informācija nedrīkst

Paviršības vai ļaunprātības dēļ klīniku iekšējā datortīkla izveidotāji bija atstājuši brīvus pieejas kodus.

mētāties, kur pagadās, to nedrīkst redzēt katrs, kam ienāk prātā. Tas nozīmē, ka datu lietošana jāsakārto, un nodarboties ar to jāsaik nekavējoties. Maijs ir tuvu. Un, kā atzīst advokāts **Agris Repšs**: „Ši ir iespēja sakārtot datu saimniecību, un ir jāatmet ilūzija, ka to var izdarīt pašu spēkiem.” Bez IT speciālistu piesaistes tas neesot izdarāms. Un arī jurists acimredzot būs nepieciešams. Ugunsūmiri, kriptēšana, anonimizēšana, instrukcijas darbiniekiem, rīcības algoritmi uzbrukuma vai zādzības gadījumā – lai datus pasargātu, darāmā ir daudz.

Datu valsts inspekcija gan neoficiāli jau devusi vēsti, ka ar kontroliem un uzņēmumu sodīšanu šogad neaizrausies. Ja nu vienīgi reaģēs uz sūdzībām. Jaunie pienākumi iestādei pašai uzkrītuši kā sniegs uz galvas, jo vēl nesen tā bija potenciāli likvidējamo mazo valsts iestāžu sarakstā, bet tagad saņēms juridisku neatkarību, lielāku budžetu, kā pamatošanai valdība pašlaik sacer Personas datu apstrādes likumu, un lērumu uzraudzības pienākumu, tostarp ser-



titificēt personas datu aizsardzības speciālistus. Šis būs ļoti pieprasīts un labi atalgotā amats.

Kā novērtēt daudzumu

To, kas ir liels datu daudzums, regula nepaskaidro, taču, kā vēsta Datu valsts inspekcija, ir izstrādātas vadlīnijas, kā to vērtēt. Jāņem vērā datu subjektu skaits, arī proporcionāli pret iedzīvotāju skaitu, datu apjoms, datu apstrādes ilgums, apstrādes darbības ģeogrāfiskais apmērs.

Lielā mēroga datu apstrādes piemēri ir šādi:

- pacienta datu apstrāde slimnīcā, ko ikdienā veic slimnīcā;
- pārvietošanās datu apstrāde personām, kas izmanto pilsētas sabiedriskā transporta sistēmu (piemēram, izsekošana ar braukšanas kartēm);
- starptautiskās ātrās ēdināšanas ķēdes klientu reālā laika ģeogrāfiskās atrašanās vietas datu apstrāde statistikas vajadzībām;
- klientu datu apstrāde, ko ikdienā veic apdrošināšanas sabiedrība vai banka;
- meklētājprogrammas paradumorientētās reklāmas personas datu apstrāde;
- datu apstrāde (saturs, transports, atrašanās vieta), ko veic pa telefonu vai caur interneta pakalpojumu sniedzējiem.

Piemēri, kas nav liela mēroga datu apstrāde, ir mazāki:

- ārstējošā ārsta pacienta datu apstrāde;
 - individuāli praktizējoša advokāta personas datu apstrāde saistībā ar kriminālpārskaujamiem un noziedzīgiem nodarījumiem.
- Katram uzņēmumam šobrīd ir būtiski saprast savu pienākumu apjomu, vēl svarīgāk – savas datu saimniecības stāvokli. Tie ir pavisam konkrēti jautājumi, kas jāsaprot: vai gadījumā, ja valdes priekšsēdētājam nozog klēpj datoru, uzņēmums spēj atjaunot klientu datus? Vai datu serveri ielauzies hakeri var informāciju padarīt nepieejamu? Vai uzņēmums spēj atskaitīties klientam, kurš un kādiem nolūkiem ir lietojis viņa datus? Kas notiek ar vairs nevajadzīgu informāciju par bijušajiem klientiem? Tiesības tikt aizmirstam ir viens no radikālākajiem regulas jaunievedumiem. Ja klients aizliedz turpmāku savu datu apstrādi, viņam vairs nedrīkst uzskaitīties trīs reizes dienā ar jautājumiem par mīļāko zivju

ellu. Protams, bankai vai Valsts ieņēmumu dienestam nevarēs pieprasīt izdzēšanu, taču atskaitīties par datu lietošanu gan. Tāpēc arī pašvaldības ir satraukušas par regulas tuvošanos. To rīcībā ir daudz informācijas par iedzīvotājiem, tostarp sensitīvas, bet, sevišķi mazākās pašvaldībās, datu pārvaldības kvalitāte ļoti zema.

Trīs rīcības varianti

Cilvēka dabā ir visu atstāt uz pēdējo brīdi. IT risinājumu un pakalpojumu kompānija „Squalio” aicina tā nedarīt – maijā veidosies „sastrēgums” jeb liels pieprasījums pēc speciālistiem. Prātīgāk ir par uzņēmuma rīcībā esošo datu „higiēnu” sākt domāt jau tagad. Un, iespējams, situācija uzņēmumā nemaz nav tik briesmīga. „Squalio” vadošā juriste **Elīna Ģirne** stāsta, ka uzņēmuma vadītājam ir trīs rīcības varianti datu saimniecības sakārtošanai. Pirmais: daru visu pats. Skaidroju, kas un kā jādarā. Lašu normatīvos aktus. Atrod dokumentu sagataves, iecelju datu aizsardzības speciālistu. Sakārtoju IT lietas un papirus. Otrs variants: izdaru, cik saprotu, un tikai tad prasu ārēju konsultāciju – kādi IT vai juridiski risinājumi ieviešami. Vārbut jātauno tikai programmas licence un jāveic darbinieku instrukcija. Ir vēl trešā iespēja: pašam nedarīt neko, noalgot pilnu auditu, bet tāda slinkošana uzņēmumam gan maksās dārgi – 20 000 eiro un uz augšu.

Kāda pašlaik ir Latvijas iestāžu un uzņēmumu gatavība regulas prasību ieviešanai? Oficiālas statistikas nav. Varētu būt kādi 50%. Elīna Ģirne kopējo situāciju datu aizsardzības jomā raksturo ar analogiju no sporta: „Līdz šim esam fristailā braukuši.” Kā kuram gribas, kā kuram sanāk. Turpmāk tā vairs nevarēs. Taču ir arī labā ziņa – ja uzņēmums līdz šim ievērojis datu „higiēnu”, kā to prasījuši likumi, pielāgošanās regulas prasībām nebūs pārmēru sarežģīta. ●

* Pilns regulas nosaukums ir Eiropas Parlamenta un Padomes Regula (ES) 2016/679 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti. Ar to tiek atcelta Direktīva 95/46/EK (Vispārīgā datu aizsardzības regula).