

VDAR un profesionālā ziņapmaiņa: kāpēc vairums pārkāpj noteikumus, paši to nezinot

Gandrīz katrs birojs, prakse vai konsultāciju uzņēmums sūta klientu dokumentus caur lietotnēm, kuru serveris atrodas ārpus Eiropas Ekonomikas zonas. Bez ļauna prāta, bet daudzos gadījumos pārkāpjot regulu, nevienam viņus par to nebrīdinot.

Dokuments, kas ceļo tālāk nekā jūs domājat

Ikdienas situācija: nodokļu konsultante caur ziņapmaiņu saņem dokumentu ar klienta datiem. Pārdošanas vadītājs caur tērzēšanu pārsūta piedāvājumu kolēģim. Ārste pa to pašu ceļu kopīgo klīnisko ziņojumu ar kolēģi. Nevienam nepadomā divreiz. Tas ir normāli. Tas ir ērti. Tas tiek darīts katru dienu katrā birojā katrā Eiropas pilsētā.

Bet šis dokuments daudzos gadījumos tikko ir aizceļojis uz serveri ASV. Tas tika saglabāts – kaut arī īslaicīgi, kaut arī „aizšifrēts miera stāvoklī” – mākonī, kuru ne profesionālis, ne viņa klients nekontrolē. Tas ir gājis cauri sistēmām, kuras tehniski var indeksēt ar saturu saistītos metadatus. Un Eiropas Vispārīgajai datu aizsardzības regulai par šo ir kas diezgan skaidrs sakāms.

Ko prasa norma

VDAR – un vēlāk arī Eiropas Savienības Tiesas jurisprudence (īpaši 2020. gada „Schrems II” spriedums, C-311/18) – nosaka, ka Eiropas pilsoņu personas datiem ir jābūt pienācīgi aizsargātiem. Ja šie dati pamet Eiropas Ekonomikas zonu, pārzinim ir jāgarantē, ka saņēmējs piedāvā aizsardzības līmeni, kas ir „pēc būtības ekvivalents” Eiropas līmenim. Praksē tas nozīmē, ka klientu datu sūtīšana caur pakalpojumiem, kuru serveri atrodas ASV jurisdikcijā, neveicot ietekmes novērtējumu un neieviešot papildu garantijas – standarta līguma klauzulas, papildu tehniskos pasākumus, piemēram, pārbaudāmu šifrēšanu utt. – var būt regulas pārkāpums. Pat ja līdz šim neviens neko nav teicis.

Un tas nav tikai par ziņu saturu. Metadati – kurš kam ko sūta, kad, cik bieži, no kurienes – saskaņā ar noteikumiem un saskaņā ar atkārtotu Eiropas Datu aizsardzības kolēģijas skaidrojumu arī ir personas dati. Pakalpojums, kas vāc metadatus no lietotāja profesionālās komunikācijas, apstrādā šī lietotāja klientu personas datus, tiem par to nezinot un nedodot nekādu piekrišanu šādai apstrādei.

Parastā domāšanas shēma – „es lietotni izmantoju tikai rakstīšanai; lietotne nav mana klienta datu sniedzēja” – ir juridiski kļūdaina. Ja klienta dati iet caur trešās puses infrastruktūru, tā trešā puse apstrādā tos datus. Un, ja tā to apstrādā, ir jābūt juridiskam pamatojumam, datu apstrādes līgumam un atbilstošām garantijām.

Kurš ir atbildīgs

Jautājums, kurš nes juridisko atbildību, nav akadēmisks. VDAR izšķir *pārzini* (kurš izlemj, kādi dati un kādam nolūkam tiek apstrādāti) un *apstrādātāju* (kurš to dara materiāli pārziņa vārdā). Profesionālis, kurš sūta klientu

dokumentus, ir pārzinis. Ziņapmaiņas lietotnes sniedzējs daudzos gadījumos ir faktiskais apstrādātājs. Bez apstrādes līguma – un bez vairuma klauzulu, kuras šādam līgumam būtu jāsaturs – pārzinis nav izpildījis savu pienākumu.

Piecotīgais skaidrojums saka: „vairums profesionāļu to nezina”. Stingrais skaidrojums saka: „likuma nezināšana neatbrīvo no atbildības”. Un jebkura šajā jautājumā konsultētā specializētā datu aizsardzības advokāta skaidrojums parasti ir stingrs.

Kam tas ir svarīgi konkrēti

Ikvienam profesionālim vai uzņēmumam, kurš kaut vai reizēm operē ar trešo pušu personisko informāciju:

- Advokātiem, kuri saņem klientu dokumentāciju (līgumus, prasības pieteikumus, deklarācijas, mantas pārskatus).
- Ārstiem un citiem veselības aprūpes speciālistiem, kuri kopīgo veselības datus – kuri saskaņā ar VDAR 9. pantu tiek uzskatīti par *īpašām kategorijām* ar pastiprinātu aizsardzības režīmu –.
- Nodokļu konsultantiem un administratīvajiem pārvaldniekiem, kuri operē ar identifikācijas, nodokļu un bankas dati.
- Personāla nodaļām, kuras pārvalda darbinieku darba un personisko dokumentāciju.
- Tirdzniecības pārstāvjiem, kuri saņem kontaktinformāciju un bieži vien jutīgu biznesa informāciju no potenciālajiem un esošajiem klientiem.

Visos gadījumos informāciju aizsargā VDAR. Visos gadījumos, parastajā praksē, šī informācija plūst caur kanāliem, kuru jurisdikcija neļauj tos deklarēt par „pēc būtības ekvivalentiem” Eiropas sistēmai bez papildu garantijām. Ne no ļauna prāta. No ieraduma. Un pateicoties tehnoloģiskajai infrastruktūrai, kura piecpadsmit gadus ērtības ir likusi augstāk par atbilstību.

Argumenti „visi tā dara”

Ir vērts paredzēt biežāko iebildumu: „ja visi tā dara, tā nevar būt īsta problēma”. Tas ir pilnīgi saprotams arguments, bet juridiski tam nav nekāda spēka. Fakts, ka prakse ir izplatīta, nepadara to par atbilstošu regulai. Datu aizsardzības iestādes (piemēram, DVI Latvijā) pēdējos gados ir sodījušas vairākus uzņēmumus tieši par ziņapmaiņas veidiem, kuri līdž pārbaudes brīdim šķita nekaitīgi.

Pašreizējā operatīvā realitāte ir tāda, ka risks varbūtības ziņā ir zems – ļoti reti gadās, ka Iestādes pārbaude auditētu konkrētos vidēja izmēra biroja ziņapmaiņas rīkus –, bet liels ietekmes ziņā, ja tas realizējas. Tas ir risks, kuru vairums uzņemas nezinot, ka viņi to uzņemas. Proti, nenovērtējot, vai izmantotais rīks ir saskaņā ar pārziņa juridisko atbildību.

Digitālās pēdas ir retroaktīvas

Ir otrs arguments, gandrīz simetrisks iepriekšējam, kuru ir vērts paredzēt: „*ja tā būtu nopietna problēma, administrācija jau būtu sākusi to kontrolēt*”. Pašreizējā novērotā realitāte tam sniedz virspusēju taisnību. Pārbaužu par nepiemērotu ziņapmaiņas izmantošanu mazos uzņēmumos un it īpaši pie pašnodarbinātajiem šodien gandrīz nav – nevis tāpēc, ka rīcība būtu atļauta, bet tāpēc, ka administrācijai Latvijā un lielākajā daļā ES trūkst cilvēku resursu, kas nepieciešami miljoniem obligāto subjektu auditēšanai.

To rāda šodienas novērotā prakse. Bet tas nav tas, ko rāda nākamā desmitgade. Divi vektori sakrīt, lai mainītu līdzsvaru salīdzinoši īsos termiņos.

Pirmkārt: digitālās pēdas ir retroaktīvas. Ikvienu ziņu, kas nosūtīta caur lietotni ar centrālo serveri, paliek reģistrēta – vismaz metadatos – infrastruktūrā, kura pastāv. Tas, kas tika nosūtīts pirms sešiem mēnešiem, tehniski joprojām ir auditējams šodien. Tas, kas tiks nosūtīts šodien, būs auditējams pēc pieciem gadiem.

Pašreizējais pārbaužu trūkums nav garantija par pārbaužu trūkumu nākotnē. Tā ir novērtējuma atlikšana, nevis atbrīvošana no tā.

Otrkārt: administratīvā audita kapacitāte augs paātrināti. Mākslīgā intelekta rīku ieviešana kontroles procesos novērš cilvēku resursu sastrēgumu, kurš līdz šim ir sargājais – faktiski, ne juridiski – mazos uzņēmumus un pašnodarbinātos. Sistēmai, kas spēj savstarpēji pārbaudīt masīvus metadatu masīvus, nodokļu deklarācijas, komercreģistrus un pienākumus ziņot par drošības pārkāpumiem, nav vajadzīgi inspektori: tai vajag piekļuvi. Un piekļuve caur prasībām sniedzējiem ar juridisko klātbūtni ES pašreizējā normatīvajā ietvarā ir pilnīgi iespējama.

Tam pievienojas mazāk tehnisks, bet tikpat noteicošs faktors: Eiropas valstis atrodas pastāvīga augoša parāda procesā un tām, gandrīz bez izņēmuma, ir jāpaplašina sava nodokļu bāze. Administratīvā sankcija, kas izriet no VDAR neievērošanas, tīri fiskālā izteiksmē ir augošs un politiski ērts ieņēmumu avots. Tas nav pieņēmums: tā ir novērojama tendence Eiropas datu aizsardzības iestāžu gada pārskatos, kur kopējais sankciju apjoms aug jau vairākus finanšu gadus pēc kārtas.

Operatīvais secinājums pārzinim nav trauksmes celšana, bet gan skaidrs skatījums: **lēmums par to, kā šodien tiek pārvaldīta komunikācija ar klientiem, tiek vērtēts pēc tās gada kontroles kapacitātes, kurā kontrole pienāks, nevis pēc pašreizējās.** Un tā kapacitāte saprātīgā termiņā būs būtiski citādāka nekā šodien. Tas, kurš sāk darīt lietas pareizi šodien, nebūs kārtībā tikai no šodienas: no šī brīža ģenerētā pēda būs atbilstoša normai, un tas retrospektīvi aizsargā gaidāmo posmu. Tas, kurš turpinās kā līdz šim, uzkrās auditējamu pēdu, kuras atbilstība tiks vērtēta pēc nākamo gadu standartiem – un resursiem.

Kas mainās ar citādu arhitektūru

Eksistē tehniskas alternatīvas, kurās dati netiek glabāti trešo pušu infrastruktūrā, bet tā vietā ceļo tieši no sūtītāja ierīces uz saņēmēja ierīci. Šajā arhitektūrā atbilstība VDAR attiecībā uz starptautisko nosūtīšanu nav atkarīga no standarta līguma klauzulām, ne no sniedzēja labās gribas, ne no nākotnes auditiem. Tā ir atkarīga no tā, ka *nav nosūtīšanas*. Un tam, kā nav, nevar pārkāpt.

Šis nav ekskluzīvs risinājums un ne vienīgais iespējamais. Bet tas ir strukturāli citāds, un normatīvā atbilstība pārstāj būt procesuāls pielikums un kļūst par tiešu projekta sekas. Profesionālim, kurš nopietni uztver savu pārziņa atbildību, šī atšķirība ir svarīga.

Nākamais Cuadernos izdevums detalizēti analizēs Schrems II spriedumu un tā praktiskās sekas mazajiem un vidējiem uzņēmumiem, kas atkarīgi no ASV mākoņpakalpojumiem, piecus gadus pēc tā publicēšanas.

Avoti un tiesiskais ietvars

- ES regula 2016/679 (VDAR), īpaši V nodaļa par starptautisko nosūtīšanu.
- EST C-311/18 („Schrems II”), 2020. gada 16. jūlijs.
- EDPB – Ieteikumi 01/2020 par pasākumiem, kas papildina nosūtīšanas instrumentus.
- Datu aizsardzības iestādes (ieskaitot DVI) – Gada pārskati ar sankciju kazuistiku par neatbilstošu tūlītējās ziņapmaiņas izmantošanu profesionālajā vidē.

[← Iepriekšējais Profesionālais noslēpums digitālajā laikmetā](#) [Nākamais](#) [→ Kad vidū neviena nav](#)

Jaunākie lasījumi

- [CUADERNOS LIST PREGUNTAS TITLE](#)
- [CUADERNOS LIST SELFHOST TITLE](#)
- [CUADERNOS LIST IDENTIDAD TITLE](#)

Paņemiet šo rakstu līdzī tur, kur jums nepieciešams.

[↓ Markdown](#) [↓ Parasts teksts](#) [↓ PDF](#)

Fails tiks lejupielādēts jūsu ierīcē. No turienes varat to saglabāt, importēt Solo2 vai kopīgot jebkur. Cuadernos nepieņem lēmumu par galamērķi jūsu vietā.

Vaska zīmogs · SHA-256 6880fcc9fe1adacf28e15c8df59db5065bda318f8b64d42b4b8878158f1e1fc7

Cuadernos Lacre · [Menzuri Gestión S.L.](#) publikācija ·
autors R.Eugenio · rediģējusi [Solo2](#) komanda.

Šī tīmekļa vietne neizmanto sīkfailus un neielādē trešo pušu resursus. Tā izmanto pašizmitinātu anonīmu apmeklējumu skaitītāju (Umami, mūsu Eiropas serverī) un minimālo JavaScript apjomu, kas nepieciešams jūsu gaišā/tumšā motīva izvēlei. Nekādu izsekošanu, nekādas profilēšanas, nekādas datu kopīgošanas. Ja vēlaties mums sekot: [RSS](#).