

Kas ir personas dati?

Vispārīgā datu aizsardzības regula

Tuvojas 25. maijs, kad visā Eiropas Savienībā jāsāk ievērot Vispārīgās datu aizsardzības regulas prasības. Lai gan tās nemaina līdzšinējos fizisko personu datu aizsardzības principus, kuri jau 18 gadus ir noteikti Fizisko personu datu aizsardzības likumā, viena no lielākajām problēmām ir tā, ka tie nav plašākai sabiedrībai zināmi un saprotami.

Īsumā:

- Personas dati ir dažāda informācija, kuru apkopojot var identificēt konkrētu personu.
- Visizplatītākie identifikatori ir vārds, uzvārds, personas kods. Taču tie nav vienīgie dati, kas ļauj identificēt personu.
- Regulā sensitīvo datu uzskaitījums ir izvērsti, papildinot to ar ģenētiskajiem un biometriskajiem datiem.
- Vispārīgā datu aizsardzības regula neaizsargā miruša cilvēka datus.

Personas dati var būt jebkāda informācija

Šobrīd spēkā esošajā Fizisko personu datu aizsardzības [likumā](#) (FPDAL) sniegtā personas datu definīcija ir lakoniska. Tā ir jebkāda informācija, kas attiecas uz identificētu vai identificējamu fizisko personu.

Vispārīgajā datu aizsardzības regulā¹ sniegts plašāks skaidrojums (4. panta 1. punkts). Tās izpratnē identificējama persona ir tāda, kuru var **tieši vai netieši identificēt**, jo īpaši atsaucoties uz identifikatoru, piemēram, minētās personas vārdu, uzvārdu, personas kodu, atrašanās vietas datiem, tiešsaistes identifikatoru, vienu vai vairākiem personai raksturīgiem fiziskās, fizioloģiskās, ģenētiskas, garīgās, ekonomiskās, kultūras vai sociālās identitātes faktoriem.

Svarīgs ir identifikators, kas informāciju sasaista ar konkrētu personu (datu subjektu). Ja tāds ir, tad jebkura informācija, kas ir sasaistīta ar identifikatoru, ir konkrētā datu subjekta personas dati. Tātad personas dati ir dažāda informācija, kuru apkopojot var identificēt konkrētu personu.

Personas dati = identifikators + informācija

Protams, visizplatītākie identifikatori ir vārds, uzvārds, personas kods. Taču tie nav vienīgie dati, kas ļauj identificēt personu. Noslēgtā vidē, piemēram, darba kolektīvā vai mazā pašvaldībā, kā identifikators var būt arī kāda cita vispārīga informācija (ieņemamais amats, atpazīstama rakstura vai ārējā izskata pazīme u. tml.), kas to ļauj sasaistīt ar konkrētu cilvēku.

Jāatzīmē, ka FPDAL un Vispārīgā datu aizsardzības regula neaizsargā miruša cilvēka datus. Tomēr ir izņēmumi. Piemēram, ja mirušas personas dati ir sasaistāmi ar dzīvu personu un var norādīt uz pārmantojamu slimību, tādā gadījumā tie jau uzskatāmi par šīs dzīvās personas datiem.

Personas dati var būt:

- vārds un uzvārds (piem., Jānis Bērziņš);
- darbavieta (piem., Jānis Bērziņš strādā SIA "X");
- ieņemamais amats (piem., SIA "X" direktors);
- mājas adrese (piem., Jāņa Bērziņa deklarētā dzīvesvietas adrese ir Trotuāra iela 15, Rīga);
- e-pasta adrese (piem., janis.berzins@siax.lv);
- personas kods, personu apliecinošu dokumentu numurs;

- atrašanās vietas dati (piem., atrašanās vietas datu funkcija mobilajā tālrunī);
- interneta protokola (IP) adrese;
- sīkfaila identifikācijas numurs;
- ārstniecības iestādē glabāti dati par pacientu u. tml.[2](#)

Jāņem vērā, ka viens pats vārds un uzvārds, kas ir bieži sastopams, piemēram, Jānis Bērziņš, vēl nebūs personas dati, ja nav papildu informācijas, par kuru Jāni Bērziņu ir runa. Taču, ja šis konkrētais vārds un uzvārds ir sasaistīts ar papildu identifikatoru, piemēram, personas kodu, darbavietu u. tml., tie ir personas dati, jo konkrētā persona jau ir identificējama.

Pēc līdzīga principa VDAR 30. apsvērumš paredz, ka fiziskas personas var tikt saistītas ar tiešsaistes identifikatoriem, ko izmanto viņu ierīcēs, lietojumprogrammās, rīkos un protokolos, piemēram, ar IP adresēm, sīkdatņu identifikatoriem vai citiem identifikatoriem (radiofrekvences identifikācijas marķējumiem). Tādējādi, iespējams, tiek atstātas pēdas, kuras, jo īpaši savienojumā ar unikāliem identifikatoriem un citu informāciju, ko saņem serveri, var izmantot, lai veidotu fizisku personu profilus un identificētu tās.

Personas dati nav:

- Jāņa Bērziņa parādsaistības ir 10 000 eiro (šajā gadījumā trūkst identifikatora, kas nepārprotami norādītu, par kuru Jāni Bērziņu ir runa);
- mirušais Jānis bija labs darbinieks (nav personas dati, jo persona ir mirusi);
- SIA "X" ir maksātspējīgs uzņēmums (uzņēmums nav fiziska, bet juridiska persona);
- uzņēmuma reģistrācijas numurs;
- Trotuāra iela 15, Rīga;
- janis958@inbox.lv vai info@siax.lv (kamēr nav identificējama sasaiste ar kādu personu);
- anonimizēti dati.

Minētie piemēri var kļūt par personas datiem, tiklīdz tiek sasaistīti ar konkrētu personu. Piemēram, ja kādā datubāzē ir norādīts, ka Jānis Bērziņš strādā SIA "X" un viņa e-pasta adrese ir janis958@inbox.lv, tie kļūst par personas datiem, kuriem atkarībā no izmantošanas mērķa piemēro Vispārīgo datu aizsardzības regulu.

Savukārt attiecībā uz anonimizētiem datiem Eiropas Komisijas skaidrojumā[3](#) ir norādīts: personas dati, kas padarīti anonīmi tādā veidā, ka fiziskā persona vairs nav identificējama, vairs nav uzskatāmi par personas datiem. Lai dati būtu patiešām anonimizēti, anonimizēšanai ir jābūt neatgriezeniskai. Tikmēr personas dati, kas ir tikuši identificēti, šifrēti vai pseidonimizēti, bet kurus var izmantot, lai atkārtoti identificētu personu, joprojām ir uzskatāmi par personas datiem un to apstrādei piemēro Vispārīgo datu aizsardzības regulu.

Kas ir sensitīvi dati

Gan FPDAL, gan Vispārīgajā datu aizsardzības regulā ir izdalītas īpaši aizsargājamās personas datu kategorijas, kas ir uzskatāmas par sensitīviem datiem. No citiem datiem šie atšķiras ar to, ka satur privātu un intīmu informāciju, kas var tikt ļaunprātīgi izmantota pret konkrētās personas interesēm, piemēram, diskriminējot darba tirgū. Tāpēc to apstrāde tiek ierobežota, bet apstrādes pārkāpumu gadījumā sagaidāms bargāks sods.

Atšķirība no iepriekšējā regulējuma ir tā, ka regulā sensitīvo datu uzskaitījums ir izvērstš, papildinot ar ģenētiskajiem un biometriskajiem datiem, lai veiktu fiziskas personas unikālu identifikāciju (piemēram, pirkstu nospiedumi, sejas digitālās fotogrāfijas, kas uzņemtas identifikācijas nolūkos, u. c.).

Līdz ar to Vispārīgā datu aizsardzības regula īpaši aizsargā:

- datus, kas atklāj rasi vai etnisko piederību, politiskos uzskatus, reliģisko vai filozofisko pārliecību, dalību arodbiedrībās;

- ģenētisko datu, biometrisko datu, lai veiktu fiziskas personas unikālu identifikāciju, veselības datu vai datu par fiziskas personas dzimumdzīvi vai seksuālo orientāciju apstrādi.

Šādu īpašo kategoriju personas datu **apstrādi regula aizliedz**, izņemot tās 9. panta 2. punktā noteiktajos gadījumos, piemēram:

- persona ir devusi nepārprotamu piekrišanu savu personas datu apstrādei;
- persona savus datus ir apzināti publiskojusi;
- tiesību akti paredz noteiktu datu apstrādi konkrētā nolūkā, lai īstenotu pārziņa vai datu subjekta tiesības nodarbinātības, sociālās aizsardzības, veselības aprūpes jomā;
- tiesību akti paredz konkrētu datu apstrādi sabiedrības interesēs, piemēram, arhivēšanas nolūkos, zinātniskās vai vēstures pētniecības, statistikas nolūkos u. tml.;
- aizstāvēt savas likumīgās tiesības, ceļot prasību tiesā;
- aizsargājot personas vitālās intereses, ja datu subjekts ir fiziski vai tiesiski nespējīgs dot savu piekrišanu, u. c.

Piemērs: tautas skaitīšana

Centrālā statistikas pārvalde ne retāk kā reizi 10 gados veic tautas skaitīšanu, kuras ietvaros iedzīvotājiem jāaizpilda apsekojuma anketa. Tajā ir iekļauti lauki, kuros jānorāda arī sensitīvi dati, piemēram, tautība. Tautas skaitīšana tiek veikta sabiedrības interesēs, un to paredz likums (Statistikas likums un saistītie Ministru kabineta noteikumi), kas cita starpā paredz veikt pasākumus sensitīvo datu aizsardzības nolūkos.

Svarīgi atcerēties! Neatkarīgi no tā, kādas kategorijas personas datus plānots apstrādāt, **jebkuras personas datu apstrādes pamatam ir jābūt tiesiskam.**

Īsumā:

- Personas datu apstrāde ir jebkura ar personas datiem vai personas datu kopumiem veikta darbība vai darbību kopums, ko veic ar vai bez automatizētiem līdzekļiem.
- Regula neattiecas uz tādu datu apstrādi, kas skar juridiskas personas datus, piemēram, informāciju par uzņēmuma nosaukumu un kontaktinformāciju.
- Regulas noteikumi neattiecas uz mirušu personu datiem.
- Regulas noteikumus nepiemēro tādai personas datu apstrādei, kuru fiziska persona veic tikai personiskām vai māsājniecības vajadzībām.

Jebkura ar personas datiem veikta darbība

Vispārīgā datu aizsardzības regula¹ (VDAR) sniedz definīciju, ka personas datu apstrāde ir jebkura ar personas datiem vai personas datu kopumiem veikta darbība vai darbību kopums, ko veic ar vai bez automatizētiem līdzekļiem. Piemēram, personas datu vākšana, reģistrācija, organizēšana, strukturēšana, glabāšana, pielāgošana vai pārveidošana, atgūšana, aplūkošana, izmantošana, izpaušana, nosūtīt, izplatot vai citādi darot tos pieejamus, saskaņošana vai kombinēšana, ierobežošana, dzēšana vai iznīcināšana.

Vispārīgā datu aizsardzības regula aizsargā personas datus neatkarīgi no izmantotās tehnoloģijas. Tā ir "tehnoloģiski neitrāla" un attiecas gan uz automatizētu, gan manuālu apstrādi, ja vien dati ir strukturēti saskaņā ar kādiem iepriekš noteiktiem kritērijiem (piemēram, sakārtoti alfabētiskā secībā).

Neatkarīgi no datu uzglabāšanas veida – vai tie apkopoti datorizētā sistēmā, papīra kartotēkā, izmantojot videonovērošanu, – visos gadījumos personas datiem piemēro Vispārīgās datu aizsardzības regulas noteiktās aizsardzības prasības.

Taču regula neattiecas uz tādu datu apstrādi, kas skar juridiskas personas datus, piemēram, informāciju par uzņēmuma nosaukumu, uzņēmējdarbības formu un kontaktinformāciju. Tāpat regulas noteikumi neattiecas uz mirušu personu datiem. Tomēr ir iespējami izņēmuma gadījumi, kad mirušās personas dati var kļūt par

dzīvas personas datiem. Piemēram, ja mirusī persona sirgusi ar pārmantojamu slimību, tad šāda rakstura informācija var tikt uzskatīta par mirušās personas pēcnācēju personas datiem, uz ko attiecas datu aizsardzības prasības. Vienlaikus regula paredz, ka dalībvalsts var paredzēt stingrākus papildu noteikumus par mirušu personu datu apstrādi. Piemēram, Latvijā Pacientu tiesību likums aizliedz izpaust jebkādu informāciju, kas attiecas uz pacientu, arī pēc viņa nāves.

Personas datu apstrādes piemēri

Personas datu apstrādes piemēru uzskaitījums regulā nav izsmeļošs. Katrs no mums ikdienā saskaras ar savu vai citu personu datu apstrādi visdažādākajās situācijās. Piemēram, kā norāda Datu valsts inspekcijas Eiropas Savienības un starptautiskās sadarbības nodaļas vadītājs **Lauris Linabergs**, strādājot kādā iestādē vai privātā uzņēmumā, ir iespējams, ka saskarsieties ar šādu personas datu apstrādi:

- personālvadība (piem., darbinieka personas lietas izveidošana un glabāšana);
- videonovērošanas veikšana;
- darbinieka e-pasta caurlūkošana, interneta izmantošanas kontrole;
- atsauksmju par darbinieku sniegšana telefoniski;
- informācijas iegūšana no Iedzīvotāju reģistra par personas dzīvesvietu;
- informācijas sniegšana Valsts ieņēmumu dienestam par darbiniekiem;
- valdes locekļu reģistrēšana Uzņēmumu reģistrā;
- dokumentu, kas satur personas datus, iznīcināšana, glabāšana.[2](#)

Tikmēr Eiropas Komisijas skaidrojumā[3](#) izceltas citas vispārējas personas datu apstrādes iespējas, ar kurām saskaramies ikdienā, piemēram, lietojot internetu, interneta banku vai iepērkoties veikalā, izmantojot klienta karti:

- reklāmas e-pasta ziņojumu/īszīņu sūtīšana;
- personas fotoattēla izlikšana/publicēšana tīmekļvietnē;
- IP adrešu vai MAC adrešu glabāšana u. c.

Datu apstrāde personiskām vajadzībām

Vispārīgās datu aizsardzības regulas noteikumus nepiemēro tādai personas datu apstrādei, kuru fiziska persona veic tikai personiskām vai mājsaimniecības vajadzībām, ar nosacījumu, ka tā nav saistīta ar profesionālu vai komerciālu darbību. Tiklīdz fiziska persona attiecīgos personas datus izmanto ārpus personīgās dzīves robežām, piemēram, sociālām, kultūras vai finanšu darbībām, ir jāievēro Vispārīgās datu aizsardzības regulas prasības.

"Katrai personai mājās ir ļoti daudz citu cilvēku datu, piemēram, telefons, kur ierakstīti draugu un paziņu kontakti, bilžu albums, kur atrodamas draugu fotogrāfijas, adrešu grāmatiņa, kurā pierakstītas draugu dzīvesvietas adrese, mājas kāpņu telpu ieejas kodi u. tml. informācija. Arī tie ir dati, ko apstrādājat. Taču, ja jūs kā fiziska persona tos apstrādājat tikai savām vajadzībām, tad uz jums regula neattiecas," [intervijā](#) LV portālam skaidroja Iekšlietu ministrijas padomniece datu jautājumos Moldovas Republikā **Jekaterina Macuka**. "Taču, ja nolēmsiet veidot savu kaimiņu kartotēku, aprakstīt viņu dzīvi un to visu publicēt internetā, tādā gadījumā regula uz jums attieksies."

Vienlaikus Vispārīgo datu aizsardzības regulu piemēro pārziņiem un apstrādātājiem, kas piedāvā līdzekļus [platformas] personas datu apstrādei personiskām vai mājsaimniecības vajadzībām (VDAR 18. apsvēruma). Piemēram, tas attiecas uz sociālo tīklu uzturētājiem, dažādu mobilo aplikāciju, mākoņdatošanas un tamlīdzīga veida tīmekļa pakalpojumu sniedzējiem.

Svarīgi atcerēties! Jebkurai datu apstrādei ir jābūt likumīgai un godprātīgai.

Jebkurai personas datu apstrādei ir jābūt tiesiskam pamatam. Vispārīgajā datu aizsardzības regulā noteikti seši vispārīgi tiesiskie pamati: piekrišana, līguma izpilde, juridisks pienākums, sabiedrības intereses, vitālo interešu aizsardzība, leģitīmo interešu ievērošana.

Lai aizsargātu personas, kuras dati tiek apstrādāti, intereses, pārzinim jāievēro regulā minētie datu apstrādes principi: likumīgums, godprātīga un pārredzamība, nolūka ierobežojums, datu minimizēšana; precizitāte, glabāšanas ierobežojums, integritāte un konfidencialitāte, pārskata atbildība.

Kopumā Vispārīgā datu aizsardzības regula¹ (turpmāk – regula) būtiski nemaina līdzšinējos personas datu apstrādes pamatprincipus, kuri jau daudzus gadus nostiprināti Fizisko personu datu aizsardzības likumā (FPDAL).

Piemēram, FPDAL [10. panta pirmās daļas pirmajā punktā](#) un tāpat arī regulas 5. panta pirmās daļas a) punktā ir noteikts datu apstrādes **likumības un godprātības princips**. Proti, jebkurai personas datu apstrādei ir jābūt tiesiskam pamatam. Savukārt pārzinis, veicot personas datu apstrādi, nodrošina godprātīgu attieksmi pret personas datiem. Godprātības princips būtībā ietver arī visus pārējos principus, jo tie visi ir vērsti uz to, lai pārzinis nodrošinātu godīgu attieksmi pret datu subjektu – personu, kuras dati tiek apstrādāti.

Personas datu apstrādes tiesiskie pamati

Vispārīgās datu aizsardzības regulas 6. pantā ir noteikti seši vispārīgi tiesiskie pamati. Tātad, lai personas datu apstrāde būtu likumīga pēc 25. maija, kad visā Eiropas Savienībā sāks tieši piemērot regulas prasības, tai jāatbilst vismaz vienam no tiem:

- **Piekrišana.** Persona (datu subjekts) ir devusi piekrišanu savu personas datu apstrādei vienam vai vairākiem konkrētiem nolūkiem.

Piemēram, veikalā tiek piedāvāts noformēt klienta karti, kurā norādāt savu e-pasta adresi un dzimšanas datus, piekrītot, ka Jums tiks sagatavoti un nosūtīti personalizēti pakalpojumu piedāvājumi, īpašas atlaides dzimšanas dienā u. tml.

- **Līguma izpilde.** Datu apstrāde izriet no uzņēmuma līgumsaistībām ar klientu vai, ievērojot personas pieprasījumu, datu apstrāde nepieciešama, lai attiecīgu līgumu noslēgtu.

Piemēram, persona vēlas iegādāties mājokli un noslēgt hipotekārā kredīta līgumu ar banku. Pirms līguma noslēgšanas kredītdevējs ar personas piekrišanu apstrādā noteiktus personas datus, lai novērtētu klienta materiālo stāvokli un maksātspēju.

- **Juridisks pienākums.** Personas datu apstrāde ir nepieciešama pārzinim, lai veiktu ES vai valsts tiesību aktā noteiktu pienākumu.

Pieņemot darbā cilvēkus, darba devējam ir jāievēro vairākos normatīvajos aktos noteiktās prasības. Piemēram, lai darbiniekiem tiktu nodrošinātas sociālās garantijas, darba devējam ir jāsniedz personas dati Valsts ieņēmumu dienestam.

Ja pircējs vēlas saņemt rēķinu par preces iegādi interneta veikalā, atbilstoši likuma “Par grāmatvedību” prasībām pārdevējam nepieciešams apstrādāt ne tikai pircēja vārdu, uzvārdu, piegādes adresi, kontaktinformāciju, bet arī personas kodu.

- **Sabiedrības intereses.** Datu apstrāde nepieciešama, lai izpildītu sabiedrības interesēs īstenojamu uzdevumu vai īstenotu oficiālas pilnvaras, kas noteiktas ES vai valsts tiesību aktā.

Piemēram, Latvijas Zvērinātu advokātu kolēģijai ir Latvijas Republikas Advokatūras likumā noteiktas pilnvaras veikt disciplināras procedūras pret kolēģijas locekļiem.

- **Vitālo interešu aizsardzība.** Personas datu apstrāde ir nepieciešama, lai aizsargātu fiziskās personas vitāli svarīgas intereses, tai skaitā dzīvību un veselību.

Piemēram, ja pēc satiksmes negadījuma slimnīcā tiek nogādāta persona bezsamaņā, ārstam nav nepieciešama piekrišana, lai uzmeklētu pacienta dokumentus, lai pārbaudītu personas identitāti un datubāzē pieejamās ziņas par tās slimību vēsturi, kā arī lai sazinātos ar cietušā tuviniekiem.

- Pārziņa vai trešās personas **legitīmo interešu ievērošana.** Šāds personas datu apstrādes pamats ir pieļaujams tikai tad, ja ir pārbaudīts, ka tādējādi netiek būtiski ietekmētas personas, kuras dati tiek apstrādāti, intereses vai pamattiesības un pamatbrīvības, jo īpaši, ja datu subjekts ir bērns. Šo punktu nepiemēro personas datu apstrādei, ko veic valsts un pašvaldības iestādes, pildot savus uzdevumus.

Piemēram, uzņēmums/organizācija uzrauga, kā tās darbinieki lieto informācijas tehnoloģiju ierīces, lai nodrošinātu iekšējā tīkla drošību.

Kā norādīts Eiropas Komisijas skaidrojumā², novērtējums, vai uzņēmuma/organizācijas legītimās intereses ir svarīgākas par attiecīgās personas, kuras dati tiek apstrādāti, interesēm, ir atkarīgs no situācijas apstākļiem. Piemērā minētajā gadījumā personas datu apstrāde būtu pieļaujama tikai tad, ja tiek izvēlēta vismazāk ierobežojošā metode attiecībā uz darbinieku privātumu, piemēram, ierobežojot piekļuvi noteiktām tīmekļvietnēm.

Ar trešajām personām būtu jāsaprot ne tikai konkrētas un identificējamās trešās personas, bet arī personu loks vai sabiedrība kopumā. *Piemēram, publicējot informāciju (fotogrāfiju) par bīstamu noziedznieku, kurš ir izsludināts meklēšanā.*³

Personas datu apstrādes principi

Tiesiskais pamats (**likumība**) un **godprātība** ir tikai divi no pamatprincipiem, kas jāievēro, apstrādājot personas datus. Vispārīgās datu apstrādes regulas 5. pants definē vēl virkni citu. Tādējādi, lai aizsargātu personas, kuras dati tiek apstrādāti, intereses, pārzinim ir jānodrošina:

- **Pārredzamība.** Pārredzamības principa pamatā ir prasība, ka visa informācija un saziņa, kas saistīta ar personas datu apstrādi, ir datu subjektam viegli pieejama skaidrā un vienkāršā valodā, ņemot vērā datu subjekta briedumu, citas īpašības, lai personai, kuras dati tiek apstrādāti, būtu saprotams, kas viņas datus vāc, kādā apjomā, kādā nolūkā dati tiek apstrādāti, cik ilgi tie tiks glabāti u. tml. Tas cita starpā arī nozīmē, ka informācijai par datu apstrādi ir jābūt pēc iespējas koncentrētai, nevis izklāstītai sīkā drukā uz neskaitāmām lapām.
- **Nolūka ierobežojumi.** Tas nozīmē, ka personas dati tiek vākti konkrētam, skaidram un likumīgam mērķim. To turpmāko apstrādi neveic ar minēto mērķi nesavienojamā veidā. Šis princips nepieļauj datu ievākšanu un apstrādi bez konkrētas nepieciešamības un mērķa. Datus neievāc nolūkā – “varbūt kādreiz noderēs”.

Piemēram, ja iegādājoties preci veikalā, noslēdzot līgumu par preces piegādi, esam nodevuši pārdevējam informāciju par savu vārdu un uzvārdu, adresi un tālruņa numuru, šo informāciju bez papildu piekrišanas ir aizliegts izmantot, lai personai vēlāk nosūtītu reklāmas bukletus vai īsziņas.

- **Datu minimizēšana.** Personas dati tiek apstrādāti tikai atbilstoši paredzētajam mērķim un tam nepieciešamajā apjomā. Tas nozīmē iepriekš noteikto likumīgo mērķi īstenot ar minimāli nepieciešamo datu apjomu tā sasniegšanai.

Piemēram, lai nodrošinātu komunikāciju ar klientu, sniedzot pakalpojumu, ir nepieciešama kontaktinformācija: e-pasta adrese vai tālruņa numurs. Taču no datu aizsardzības viedokļa būtu pārmērīgi prasīt gan e-pastu, gan tālruņa numuru, ģimenes locekļa tālruņa numuru u. c. kontaktinformāciju.

- **Glabāšanas ierobežojums.** Personas dati tiek apstrādāti tādā veidā, kas pieļauj personas identifikāciju tik ilgi, līdz tiek sasniegts attiecīgās personas datu apstrādes mērķis.

Ja pakalpojuma līgums ar klientu tiek izbeigts un pamat nolūks – sniegt pakalpojumu klientam – ir sasniegts, dati šim nolūkam vairs nav nepieciešami un apstrādājami. Vienlaikus ir iespējams, ka datus nepieciešams apstrādāt papildu nolūkiem, lai izpildītu likumā noteiktās grāmatvedības prasības vai aizstāvētu uzņēmuma leģitīmās intereses. Piemēram, pēc interneta veikalā iegādātās preces piegādes pakalpojuma sniedzējs klienta personas datus var glabāt tik ilgu laiku, kas ir nepieciešams, lai risinātu noteikta veida civiltiesiskus strīdus (ja prece nav piegādāta, tā nav bijusi kvalitatīva u. tml.).

- **Precizitāte.** Ir jāveic visi saprātīgi pasākumi, lai nodrošinātu, ka neprecīzi dati, ņemot vērā nolūkus, kādos tie tiek apstrādāti, bez kavēšanās tiktu dzēsti vai laboti. Tikai precīzi dati var nodrošināt godprātīgu un taisnīgu lēmumu pieņemšanu attiecībā uz datu subjektu.

Bieži uzņēmumi gadiem ilgi uzkrāj dažādus klientu datus. Liela daļa no tiem vairs nav aktuāla – personas maina tālruna numuru, dzīvesvietu, darbavietu, uzvārdu, nomirst. Šādu neaktuālu personas datu glabāšana neatbilst Vispārīgās datu aizsardzības regulas noteikumiem.

- **Integritāte un konfidencialitāte.** Personas dati tiek apstrādāti, nodrošinot atbilstošu drošību, tostarp aizsardzību pret neatļautu vai nelikumīgu apstrādi, nejaušu nozaudēšanu, iznīcināšanu vai sabojāšanu, izmantojot atbilstošus tehniskos vai organizatoriskos pasākumus.

Latvijā arī līdz šim ir bijuši spēkā Ministru kabineta noteikumi⁴, kuri nosaka organizatoriskus un tehniskus pasākumus, kādi pārziņiem ir jāievēro, apstrādājot datus. Tā ir virkne drošības pasākumu, kas nodrošina, ka pārziņa rīcībā esošais datu kopums nav pieejams citām personām, tai skaitā uzņēmuma darbiniekiem, kuru darba pienākumi neparedz konkrēto personas datu apstrādi.

- **Pārskata atbildība.** Šis princips zināmā mērā ir jaunums. Tas paredz datu pārziņa pienākumu uzskatāmi parādīt, kā viņš ievēro datu aizsardzības principus, ņemot vērā to, ka datu subjektam pašam ne vienmēr ir zināšanas un līdzekļi, lai kontrolētu savu datu apstrādi.

Datu apstrāde nav aizliegta. Taču, tāpat kā līdz šim, lai būtu drošība, ka personu datu apstrāde ir likumīga, katram pārzinim ir godīgi jāatbild uz trim jautājumiem:

1. Kāds ir personas datu apstrādes mērķis – vai tas ir likumīgs un godprātīgs?
2. Kādu datu apstrāde ir nepieciešama, lai sasniegtu mērķi? Kāds ir iespējamais mazākais datu apjoms, lai mērķi varētu sasniegt?
3. Vai mērķa sasniegšanai nepieciešamo personas datu apstrādei ir tiesisks pamats? Jebkurai personas datu apstrādei ir nepieciešams pamatojums.

Publikācijā izmantoti Datu valsts inspekcijas un Eiropas Komisijas sagatavotie materiāli.

[1 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 ko atceļ Direktīvu 95/46/EK \(Vispārīgā datu aizsardzības regula\).](#)

[2 Eiropas Komisija. 2018. gada ES datu aizsardzības noteikumu reforma.](#)

[3 Plašāk: Ivo Krievs. Pārziņa vai trešās personas leģitīmās intereses kā personas datu apstrādes tiesiskais pamats. Jurista Vārds. 14. novembris, 2017/Nr. 47 \(1001\).](#)

[4 Ministru kabineta noteikumi Nr. 40 "Personas datu aizsardzības obligātās tehniskās un organizatoriskās prasības".](#)

FIZISKO personu datu aizsardzības normatīvi – tiesiskā bāze – ES eksistē jau no 1995.gada, savukārt [Direktīvas 95/46/EK](#) noteikumi Latvijas normatīvajos aktos tika transponēti ar [Fizisko personu datu aizsardzības likuma](#) (Datu aizsardzības likums) palīdzību 2000.gadā.

Tomēr ikdienas prakse liecina, ka tiesību subjekti ne vienmēr pietiekami saprot šīs jomas nozīmīgākos pamatjēdzienus.

Pārzinis un personas datu operators (operators)

Termina "pārzinis" un tā mijiedarbības ar jēdzienu "operators" skaidrai izpratnei ir svarīga loma personas datu apstrādes jomu regulējošo normatīvo aktu piemērošanā. Šo terminu pareiza attiecināšana uz konkrētajiem tiesību subjektiem nosaka, kas būs atbildīgs par personas datu apstrādes noteikumu ievērošanu, kuras valsts normatīvie tiesību akti tiks piemēroti un kā datu subjekts var izmantot savas tiesības praksē.

Pārzinis ir fiziskā vai juridiskā persona, valsts vai pašvaldības institūcija, kas pati vai kopā ar citiem nosaka personas datu apstrādes mērķus un apstrādes līdzekļus. Noteikt, kura persona uzskatāma par pārzini, ir iespējams, tikai analizējot katra atsevišķa gadījuma faktiskos apstākļus, jo pārziņa statusa piešķiršana konkrētajai personai ir faktiskās sekas, ko rada šīs personas lēmums veikt fizisko personu datu apstrādi, kā arī šādas apstrādes mērķu (t.i., kāpēc šie dati tiks apstrādāti) un līdzekļu (t.i., kā šādi dati tiks apstrādāti) noteikšana.

Savukārt operators (Regulas tekstā – "apstrādātājs") ir fiziska vai juridiska persona, valsts iestāde, aģentūra vai jebkura cita struktūra, kura pārziņa vārdā apstrādā personas datus. Operatora esamība personas datu aizsardzības procesā ir atkarīga no pārziņa lēmuma. Pārzinis nosaka, vai fizisko personu dati tiks apstrādāti paša pārziņa organizācijas ietvaros (piemēram, ar viņa personāla palīdzību), vai arī datu apstrāde (kopumā vai daļēji) tiks deleģēta ārējai organizācijai (operatoram). Tātad operators ir atsevišķa, patstāvīga persona (subjekts), kas neietilpst pārziņa organizācijā, bet kas apstrādā datus pārziņa vārdā.

Personas datu apstrādes veikšanu pārzinis var operatoram uzticēt tikai ar rakstisku līgumu. Operators ir tiesīgs apstrādāt fizisko personu datus tikai attiecīgajā līgumā noteiktajā apjomā un tajā paredzētajiem mērķiem. Ja personas datu apstrāde iziet ārpus līgumā noteiktā uzdevuma, operatora statuss tiks pārkvalificēts uz pārziņa statusu attiecībā uz to personas datu daļu, kas tiek apstrādāta ārpus pilnvarojuma. Tādējādi operators pēc būtības ir pārziņa pilnvarotā persona vai faktiskais datu apstrādes īstenotājs. Tas nozīmē, ka operators patstāvīgi nepieņem lēmumu, vai tiks uzsākta datu apstrāde, kā arī nenosaka, kādiem mērķiem šāda apstrāde tiks veikta.

Piemērs

Juridiskā persona (veikals) drošības nodrošināšanai noslēdz līgumu ar apsardzes kompāniju, saskaņā ar kuru apsardzes kompānija uzstāda videonovērošanas kameras veikala telpās, kā arī veic šo kameru tehnisko apkalpošanu. Šādā gadījumā veikals ir uzskatāms par pārzini, jo tas ir pieņēmis lēmumu par videonovērošanas kameru uzstādīšanu (t.i., lēmumu par to, ka veikala apmeklētāju dati tiks apstrādāti ar to ārējā izskata video reģistrācijas palīdzību) un noteicis šādas apstrādes mērķi, proti, drošības nodrošināšana. Savukārt apsardzes kompānija šajā gadījumā ir uzskatāma par operatoru, jo tā rīkojas tikai uz pārziņa rīkojuma pamata un viņa interesēs.

Piemērs

Juridiskā persona (potenciālais darba devējs) meklē jaunu darbinieku un noslēdz līgumu ar rekrutēšanas kompāniju, kura darba devēja vārdā veiks jauna darbinieka meklēšanu un atlasīšanu. Pakalpojuma sniegšanas procesā rekrutēšanas kompānija apstrādās fizisko personu – potenciālo darbinieku – personas datus (piemēram, vārdu, uzvārdu, kontaktinformāciju un citus datus, kas norādīti CV vai iegūti citādi). Šajā gadījumā potenciālais darba devējs ir uzskatāms par pārzini, bet rekrutēšanas kompānija – par operatoru.

Jānorāda, ka fiziskā persona, kas apstrādā citu fizisko personu datus personiskām vai mājas un ģimenes vajadzībām (piemēram, ierakstot kontaktinformāciju telefona grāmatā) un neizpauž šos datus trešajām personām, nav uzskatāma par pārzini. Uz šādu personu neattieksies normatīvo aktu noteikumi personas datu aizsardzības jomā. Taču, ja fiziskā persona tomēr izpauž minētos datus trešajām personām, piemēram, publicē informāciju (fotogrāfijas) par citām fiziskajām personām internetā, tad šāda datu apstrāde netiks uzskatīta par tādu, kas veikta personiskām vai mājas un ģimenes vajadzībām. Rezultātā iepriekš minētais izņēmums nebūs piemērojams.

Personas dati un datu subjekts

[Datu aizsardzības likums](#) un Regula reglamentē (aizsargā) tikai fizisko personu datu apstrādi. Līdz ar to datu aizsardzība, kas noteikta ar iepriekš uzskaitītajiem normatīvajiem aktiem, nav attiecināma uz juridiskajām personām (arī gadījumos, kad juridiskās personas nosaukums satur fizisko personu vārdu un uzvārdu). Salīdzinot ar [Datu aizsardzības likumu](#), Regula satur detalizētāku termina "datu subjekts" definīciju, taču koncepta būtība mainīta netiek.

Datu subjekts ir identificēta fiziska persona vai fiziska persona, ko tieši vai netieši var identificēt, lietojot līdzekļus, ko pārzinis vai jebkura cita fiziska vai juridiska persona varētu pamatoti izmantot, īpaši atsaucoties uz identifikācijas numuru, atrašanās vietas datiem, tiešsaistes identifikatoru vai vienu vai vairākiem šai personai raksturīgiem fiziskās, fizioloģiskās, ģenētiskās, garīgās, saimnieciskās, kultūras vai sociālās identitātes faktoriem. Tādējādi datu subjekts ir:

- fiziska persona, kuras identitāte jau ir noteikta vai
- tāda fiziska persona, kura vēl nav identificēta, bet kuras identitāti var noteikt, iegūstot papildu informāciju.

Personas dati savukārt ir jebkāda informācija, kas attiecas uz datu subjektu. Personas dati nav tikai vārds, uzvārds un personas kods, bet arī jebkura cita informācija. Jēdziens "personas dati" ietver gan objektīvo informāciju (piemēram, personas kods, veselības dati, nacionalitāte utt.), gan subjektīvo informāciju (piemēram, kredītiestādes viedoklis par konkrētā klienta uzticamību, darba devēja viedoklis par darbinieku utt.).

Lai informācija tiktu uzskatīta par "personas datiem", tai nav obligāti jābūt patiesai vai pierādītai. Rezultātā par "personas datiem" var tikt uzskatīta jebkura informācija, kas atsevišķi vai kopsakarā ar citiem datiem apraksta personu tādā veidā, kas ļauj to nošķirt no citām personām un identificēt to kā konkrētu individu.

Piemērs

E-pasta adrese, kas satur vārdu, uzvārdu un darbavietas nosaukumu, jau ļauj identificēt konkrēto personu (īpaši gadījumos, kad juridiskās personas mājaslapa satur informāciju par tās darbiniekiem) un tādējādi ir uzskatāma par personas datiem.

Datu subjekta piekrišana

Viens no personas datu apstrādes principiem paredz, ka jebkurai fizisko personu datu apstrādei ir jābūt likumīgai. Personas datu apstrādei jābūt balstītai uz noteiktu tiesisko pamatu, t.i., jāizpildās vismaz vienam no 6 nosacījumiem, kas minēti Datu aizsardzības likuma [7.pantā](#) (Regulas 6.pants). Neskatoties uz dažām formulējuma atšķirībām, Regula un [Datu aizsardzības likums](#) paredz vienādus tiesiskos pamatus, kuriem izpildoties datu apstrāde ir likumīga (t.i., pārzinis ir tiesīgs to veikt), proti:

- datu subjekts ir devis piekrišanu savu personas datu apstrādei vienam vai vairākiem konkrētiem nolūkiem;
- apstrāde ir nepieciešama līguma, kurā datu subjekts ir līgumslēdzēja puse, izpildei vai pasākumu veikšanai pēc datu subjekta pieprasījuma pirms līguma noslēgšanas;
- apstrāde ir nepieciešama, lai izpildītu pārzinim uzliktu juridisku pienākumu (šādā gadījumā tādām juridiskām pienākumam jābūt paredzētam ES vai ES dalībvalsts tiesību aktos. Piemēram, saskaņā ar [Noziedzīgi iegūtu](#)

[Īdzekļu legalizācijas un terorisma finansēšanas novēršanas likumu](#) finanšu iestādei ir pienākums veikt klienta identifikāciju un iegūt tādas fiziskās personas datus, kā, piemēram, vārds, uzvārds un personas kods.);

- apstrāde ir nepieciešama, lai aizsargātu datu subjekta īpaši svarīgas intereses;
- apstrāde ir nepieciešama, lai veiktu uzdevumu sabiedrības interesēs vai pārzinim likumīgi piešķirtu valsts varas īstenošanas pilnvaru ietvaros (arī šādā gadījumā pamatam jābūt paredzētam ES vai ES dalībvalsts normatīvajos aktos);
- apstrāde ir nepieciešama pārziņa likumīgo interešu ievērošanai, izņemot, ja datu subjekta intereses vai pamattiesības un brīvības, kurām nepieciešama aizsardzība, ir svarīgākas, īpaši, ja datu subjekts ir bērns.

Datu subjekta piekrišana kā pamats datu apstrādei

Praksē bieži pārzinis pamato fiziskās personas datu apstrādi ar konkrētās personas piekrišanu, bet ne vienmēr tas ir attaisnoti. Šis tiesiskais pamats var šķist drošāks no visiem iepriekš minētajiem pamatiem, jo datu subjekts it kā pats dod piekrišanu savu datu apstrādei. Taču šāds secinājums ne vienmēr atbilst patiesībai. Turpmāk izklāstīti daži aspekti, kurus nepieciešams ievērot attiecībā uz datu subjekta piekrišanu kā tiesisko pamatu datu apstrādes veikšanai.

Datu subjekta piekrišana ir jebkura brīva, konkrēta, apzināta (*informed*) un nepārprotama (*explicit*) norāde uz datu subjekta vēlmēm, ar kuru datu subjekts vai nu paziņojuma, vai skaidras apstiprinošas darbības veidā sniedz piekrišanu savu personas datu apstrādei. Tādējādi par datu subjekta piekrišanu ir uzskatāms ne tikai rakstisks paziņojums (piemēram, atsevišķa dokumenta veidā), bet arī jebkura cita datu subjekta aktīva darbība, kas konkrētajos apstākļos skaidri norāda, ka fiziskā persona ir piekritusi savu datu apstrādei (par šādu aktīvu piekrišanu ir uzskatāma, piemēram, atzīmes (ķeksīša) veikšana dialoga logā internetā, neobligātas kontaktinformācijas norādīšana paziņojumu saņemšanai utt.). Svarīgi, lai piekrišana būtu aktīva (skaidri izteikta), nevis pasīva, tāpēc klusēšana vai bezdarbība nav uzskatāma par piekrišanas izteikšanu. Rezultātā nedrīkst būt šaubu, ka dot piekrišanu savu datu apstrādei bija fiziskās personas nodoms.

Datu subjekta piekrišanai jābūt brīvai. Ja fiziskajai personai reāli nebija brīvas izvēles (dot piekrišanu vai nedot), piekrišana nav uzskatāma par spēkā esošu tiesisku pamatu datu apstrādes veikšanai. Tas nozīmē, ka arī piekrišanas došanas atteikuma gadījumā fiziskā persona nedrīkst būt pakļauta negatīvām sekām. Piemēram, aizpildot anketu kādas juridiskās personas (veikala, restorāna) atlaižu kartes saņemšanai, fiziskā persona var norādīt savu kontaktinformāciju (e-pasta adresi vai mobilā telefona numuru), ja tā vēlas saņemt paziņojumus un citu informāciju par atlaižu programmu. Norādot kontaktinformāciju (aktīvas darbības veikšana), fiziskā persona dod savu piekrišanu tam, ka konkrētā juridiskā persona izmantos šo kontaktinformāciju paziņojumu sūtīšanas mērķiem. Ja atlaižu kartes saņemšana nav atkarīga no tā, vai persona ir vai nav norādījusi kontaktinformāciju, tad šādu piekrišanu var uzskatīt par brīvu. Ja fiziskā persona nevar saņemt atlaižu karti, nenorādot kontaktinformāciju, piekrišanu nevar uzskatīt par brīvu, jo fiziskajai personai nav reālu izvēles tiesību.

Datu subjekta piekrišanai jābūt apzinātai (informētai). Piekrišana var būt apzināta tikai gadījumos, kad fiziskajai personai ir visa nepieciešamā informācija lēmuma pieņemšanai (dot piekrišanu vai nedot). Noteikt, vai fiziskajai personai tika sniegta visa nepieciešama informācija, var, tikai analizējot katra konkrēta gadījuma apstākļus. Fiziskajai personai jāsniedz pilnīga un skaidra informācija par to, kas tieši ietekmē viņas lēmumu par piekrišanas došanu, piemēram, informācija par to, kādi dati un kādā nolūkā tiks apstrādāti, informācija par fiziskās personas tiesībām un negatīvām sekām atteikuma dot piekrišanu gadījumā utt.

Piemērs

Piekrišana nebūs uzskatāma par informētu, ja tās formulējums ir šāds: “Es, [vārds, uzvārds], dodu savu piekrišanu SIA [nosaukums] savu personas datu apstrādei ar mērķi [...] saskaņā ar [...] likuma [...] pantu.” Šādā gadījumā fiziskajai personai piekrišanas došanas brīdī kā minimums vēl jāsniedz tās tiesību normas aktuālā redakcija, uz kuru ir atsauce piekrišanas tekstā.

Datu subjektam ir tiesības jebkurā brīdī atsaukt savu piekrišanu. Šādas tiesības datu subjektam bijušas vienmēr, lai gan [Datu aizsardzības likumā](#) uz to tiešas norādes nav. Savukārt Regulas 7.panta 3.daļā konkrēti

noteikts, ka datu subjektam ir tiesības jebkurā brīdī atsaukt savu piekrišanu datu apstrādei. Piekrišanas atsaukšana neietekmē uz piekrišanas pamata pirms tās atsaukšanas veiktas datu apstrādes likumīgumu.

Pēc tam, kad datu subjekts ir atsaucis piekrišanu, pārzinis vairs nav tiesīgs turpināt šī datu subjekta personas datu apstrādi, ja vien nepastāv kāds cits no minētajiem tiesiskajiem pamatiem. Taču šajā gadījumā būs apšaubāma piekrišanas kā datu apstrādes tiesiskā pamata sākotnējā izmantošana. Ja personas datu apstrāde jau sākotnēji varēja tikt veikta uz cita tiesiskā pamata, tad situāciju, kad fiziskā persona it kā dod savu piekrišanu datu apstrādei, var uzskatīt par maldīgu vai sākotnēji netaisnīgu.

Piemērs

Fiziskā persona ar konkrētu pakalpojuma sniedzēju noslēdz līgumu par telekomunikācijas pakalpojumu saņemšanu un nodod tā apstrādei tādus datus kā vārds, uzvārds, personas kods un dzīves vietas adrese. Pakalpojuma sniedzējam ir nepieciešams saņemt šos datus līguma noslēgšanai un tā turpmākai izpildei (pakalpojums tiks sniegts konkrētajai fiziskajai personai, tās dzīves vietas adresē tiks uzstādīts nepieciešamais aprīkojums, fiziskajai personai tiks sagatavots rēķins par pakalpojumiem utt.). Šādā gadījumā konkrētās personas dati tiks apstrādāti nevis tāpēc, ka persona ir devusi savu piekrišanu, bet tāpēc, ka bez šo datu apstrādes pakalpojuma sniegšana nebūs iespējama. Pretējā gadījumā piekrišanas atsaukšana pēc būtības izraisa attiecīgā pakalpojuma pārtraukšanu un pakalpojuma līguma izbeigšanu.

Fiziskās personas piekrišana šādos apstākļos nav uzskatāma par brīvu, jo tai nav izvēles – ja persona vēlas saņemt konkrētu pakalpojumu, noteikta apjoma personas datu nodošana pakalpojuma sniedzējam ir neizbēgama. Jāatzīmē, ka arī līguma tekstā ietverta piekrišana nebūs uzskatāma par piekrišanu datu apstrādi reglamentējošo normatīvo aktu kontekstā.

Te aplūkoju tikai dažus fizisko personu datu apstrādes jomas pamatjēdzienus, kuru pareiza izpratne, manuprāt, ietekmē šīs nozares izpratni kopumā. Bez iepriekš minētajiem aspektiem ir arī daudzas citas nianšes, kas jāņem vērā, apstrādājot fizisko personu datus, bet to analīze šī raksta ietvaros netika veikta.

4% no apgrozījuma – sods, lai iebiedētu

Daudzi ir satraukti, jo [Regulā](#) par pārkāpumiem paredzēts sods, kas var sasniegt 20 milj. eiro vai 4% no uzņēmuma apgrozījuma. Tas ir maksimālais sods, kas galvenokārt paredzēts, lai [Regulu](#) tiešām ņemtu vērā. Lai gan soda apmērs ir iespaidīgs mārketinga rīks dažādu konsultantu arsenālā, tomēr nevajadzētu ļauties panikai un cerēt, ka kāds no ārpuses atnāks un radīs perfektu kārtību.

Labākais instruments datu apstrādes atbilstības nodrošināšanai [Regulas](#) prasībām ir pašiem pēc būtības iedziļināties savos procesos un tos sakārtot, galvenokārt tāpēc, ka neviens no ārpuses nezina attiecīgā uzņēmuma vajadzības un nepieciešamības tik labi, kā paši uzņēmuma darbinieki un vadība.

Šajā gadījumā efektīvs risinājums ir pastāvīga datu speciālista piesaiste vai savu darbinieku apmācība, izpētot uzņēmuma procesus un rodot atbilstošākos risinājumus. Ja uzņēmums spēs parādīt, ka tas pastāvīgi rūpējas par datu aizsardzību, un vēlēsies aizsargāt tā pārziņā esošos datus, visticamāk, pat incidenta gadījumā uzņēmumam netiks piemērots maksimālais sods.

"Datu inventarizāciju" labāk veikt pašiem

[Regula](#) attiecināma tikai uz fiziskās personas datiem, tomēr vienlaikus – ne tikai. Tāpēc vispirms katram uzņēmumam būtu jāveic datu audits jeb uzņēmumā esošo datu inventarizācija. To, ņemot vērā jau minētos iemeslus attiecībā uz savu procesu un vajadzību pārzināšanu, ieteicams veikt pašiem, nevis pieaicināt speciālistu. Tāpat arī uzņēmuma darbiniekiem ir jāizprot savas datu plūsmas — tas palīdzēs drošāk darboties ar datiem nākotnē, jo būs izpratne par to, kas un kāpēc tiek apstrādāts.

Ja tiks piesaistīts eksperts no ārpuses, pašiem darbiniekiem un vadībai var nebūt vēlēšanās iedziļināties procesos, bet, kad konsultants aizies, uzņēmums var neapzināti izdarīt datu aizsardzības pārkāpumu, jo trūks izpratnes. Datu aizsardzība ir nepārtraukts process, jo par datu apstrādes atbilstību [Regulai](#) ir un būs jā rūpējas pastāvīgi. Tāpat tas ir arī interesants process — pašiem izprast, kāpēc un kādi dati atrodas uzņēmuma rīcībā un, iespējams, sakārtojot apstrādātos datus, arī uzlabot savus procesus, tādējādi paaugstinot sniegto pakalpojumu kvalitāti un uzlabojot uzņēmuma tēlu klientu vidū.

Ar ko sākt datu sakārtošanu?

Sākotnēji jākonstatē, kādi dati ir uzņēmuma rīcībā.

Atsevišķi ieteicams izvērtēt personāla datus, kas atrodas visās informācijas sistēmās, papīra formātā, grāmatvedībā u.c. Arī klientu dati, ja tie ir fiziskās personas, var būt pietiekami apjomīgi.

Ja klienti ir tikai juridiskās personas, ieteicams pievērst uzmanību tam, ka arī juridisko personu dati var saturēt fiziskās personas datus, piemēram, ja līgumā starp 2 uzņēmumiem ietverti paraksttiesīgo personu vai pilnvaroto personu dati, kontaktpersonu dati u.tml.

Lielu apjomu var veidot arī sadarbības partneri – kādi viņu dati tiek glabāti un kādas ir datu drošības mērķiem nepieciešamās datu apstrādes, piemēram, video novērošana, piekļuves sistēmu telpām organizācija utt.

Tiesības tikt aizmirstam ir pārprastas

[Regulu](#) pavada mīts, ka visi datu subjekti tagad varēs pieprasīt pārziņiem bez ierunām izdzēst to datus. Šīs tiesības ir pārprastas. Pieprasīt izdzēst datus varēs tikai tad, ja datu uzglabāšanai nav tiesiska pamata vai datu apstrāde ir pārmērīga.

Tātad, ja datu subjekts pieprasa dzēst viņa datus, uzņēmējam jāspēj paskaidrot, kāpēc viņš glabā šos datus. Pamatojums var būt dažāds: līgumsaistību izpilde, likuma prasību izpilde, dažādas pārziņa leģitīmas intereses u.tml. Piemēram, [likumā](#) "Par grāmatvedību" uzņēmumam paredzēts noteiktu laiku glabāt dažādus attaisnojuma dokumentus. Pamatoti būtu uzglabāt datus arī pēc tiesisko attiecību izbeigšanas, lai strīdus gadījumā uzņēmumam būtu iespēja pierādīt, ka tas ir, piemēram, izpildījis līguma saistības.

Šajā gadījumā vajadzētu padomāt par noilguma termiņiem. [Regulā](#) noteikts, ka pārzinim ne vēlāk kā 1 mēneša laikā ir jāsniedz atbilde datu subjektam, tāpēc, lai pieprasījumu saņemšanas gadījumā nebūtu panikā jādoma tiesiskie pamati un cita pamatojošā informācija, jau laikus ieteicams piefiksēt uzņēmumā apstrādātos datus un izvērtēt atbilstošāko tiesisko pamatojumu to apstrādei, proti, kāpēc tie tiek uzglabāti.

Ja nav iespējams atrast pamatojumu datu apstrādei, labāk no tiem atbrīvoties, tādējādi nepakļaujot sevi nelikumīgas datu apstrādes riskam un sodam. Šādi datu subjektu pieprasījumi noteikti būs, un ar to ir jā rēķinās.

Regula liek būt atbildīgākiem

[Regula](#) ir salīdzinoši elastīga, kas, manuprāt, ir ļoti labi. Tas uzņēmējiem liek būt atbildīgākiem. [Regula](#) liek pašiem domāt līdzī, nevis aklī izpildīt normatīvo aktu prasības. Tajā iekļautie principi ir ļoti cieši saistīti ar ikdienas biznesu un tā vajadzībām, piemēram, lai īstenotu datu minimizācijas jeb proporcionalitātes principu, uzņēmumā ir jāsaprot, kāds ir minimālais apstrādājamo datu apjoms biznesa mērķu sasniegšanai, un jāņem vērā, ka [Regulā](#) nav atbalstīts princips "vispirms savācam visu, ko varam savākt, bet pēc tam domāsim, ko ar datiem darīsim". Slēdzot līgumus ar klientu, ieteicams ievākt tikai datus, kas patiešām nepieciešami līguma izpildei vai pakalpojumu sniegšanai. Tas jāņem vērā, arī pieprasot informāciju no pretendentiem darba attiecībās. Tāpat svarīgi savlaikus informēt klientus, sadarbības partnerus un darbiniekus, kādam nolūkam viņu dati pieprasīti, ko ar tiem darīs, cik ilgi uzglabās un kāpēc.

Būtiskākais !

Aplūkojot [Regulas](#) saturu, šķiet, ka "klupšanas akmeņi" varētu būt, piemēram, spēja pareizi definēt tiesisko pamatu datu apstrādei, datu minimizācijas jeb proporcionalitātes izvērtējums, leģitīmās intereses definēšana u.c.

Problēmātiski varētu būt arī atrast visus datus, kas uzņēmumā tiek apstrādāti, jo nereti nav izpratnes, kas ir dati. Tāpēc jāņem vērā, ka dati nav tikai personas kods, adrese, telefona numurs u.c. Ja darbinieks izmanto uzņēmuma auto un tajā ir globālās pozicionēšanas sistēma, tad dati, ko sistēma fiksē, jau ir darbinieka personas dati, jo atspoguļo, kur šī persona ikdienā pārvietojas. Dati ir arī interneta vēsture darbinieka datorā, ja ir skaidri zināms, kurš darbinieks strādā ar attiecīgo datoru, u.tml.

Īpašu uzmanību ieteicams pievērst uzņēmuma komunikācijai ar datu subjektu, proti, kā viņš tiks informēts par savu datu apstrādi un citiem aspektiem, kas noteikti [Regulā](#). Kā jau minēts, vislabāk to noteikt jau līgumā vai privātuma noteikumos, proti, informēt datu subjektu par jautājumiem, kas saistīti ar viņu datu apstrādi, – kurš datus apstrādās, kādi ir tiesiskie pamati, kādi mērķi, cik ilgi glabās, vai dati varētu tikt sūtīti ārpus Eiropas Savienības u.tml.

"Kašķīgs klients"

Uzņēmējiem, kas strādā ar klientiem, veido datu bāzes u.tml., ieteicams uzglabāt tikai nepieciešamāko informāciju. Nereti klientu datu bāzēs tiek ievietoti arī papildu komentāri, piemēram, "pa dienu neatbild, zvanīt tikai vakaros", "ļoti prasīgs un kašķīgs" u.c., kas arī uzskatāmi par personas datiem. Ieteiktu pārvērtēt, vai šāda veida subjektīvo informāciju uzņēmumam tiešām nepieciešams apstrādāt, jo tad, ja klients pieprasīs informāciju par to, kādus datus par viņu uzglabā, tas viss klientam būs jādara zināms. Pieļauju, ka informācijas, ka klients ir novērtēts kā kašķīgs, sniegšana uzņēmumam varētu radīt reputācijas riskus.

Par pārkāpumu labāk ziņot pašiem

Būtiskākais datu apstrādes pārkāpums noteikti ir datu noplūde. Medijos nereti parādās ziņas, ka kāda datu bāze ir "uzlauzta", tomēr šajā aspektā lielāko risku rada nevis IT resursu apdraudējums, jo IT speciālisti galvenos riskus ir minimizējuši vai novērsuši, bet gan cilvēciskais faktors — darbinieks. Turklāt bieži darbinieki izdara pārkāpumus datu aizsardzības jomā, neapzinoties, ka tas ir nepareizi. Tāpēc ir ļoti svarīgi darbiniekus apmācīt, kas ir dati un ko ar tiem drīkst vai nedrīkst darīt. Tāpat vajadzētu izvērtēt, kuri darbinieki piekļūst datiem, iespējami samazinot darbinieku skaitu, kuriem ir piešķirta piekļuve datiem, piemēram, sadalot darbiniekiem lomas, lai nebūtu tā, ka klientu konsultants redz arī informāciju par savu kolēģu darba algām, ko vajadzētu redzēt tikai personāla struktūrvienībai un grāmatvežiem.

Jānorāda, ka [Regulā](#) pieprasīts par incidentiem (datu noplūde, datu nejauša nosūtīšana nepareiziem adresātiem u.c.) informēt Datu valsts inspekciju (DVI) un atsevišķos gadījumos arī pašu datu subjektu, līdz ar to jāizstrādā arī iekšēja kārtība, kā incidenti tiks fiksēti un kā notiks ziņošana, lai nenokavētu ziņošanas termiņu — 72 stundas no incidenta konstatēšanas brīža.