Kas jāņem vērā, ja personas datu apstrādei izmanto digitālos pakalpojumus

Šajā un pagājušajā gadā uzņēmumi aktīvi gatavojās, kā arī turpina gatavoties Vispārīgās datu aizsardzības regulas (regula) ieviešanai. Lai gan regulas prasības nav absolūti jaunas un iepriekš pamatprincipi jau bija norādīti gan Eiropas Savienības, gan Latvijas normatīvajos aktos, regula satricināja vairāku uzņēmumu izpratni par datu aizsardzību.

JURISTA PADOMS

Viens no aspektiem, kam tika pievērsta uzmanība, ir personas datu konfidencialitāte un citu pušu iesaistīšana apstrādes procesā. Bieži liekas, ja mēs neredzam, ka kāda cita persona fiziski veic darbības ar datiem, tad personas dati ir drošībā un piekļuve tiem ir ierobežota. Tomēr uzņēmuma rīcībā esošo personas datu apstrādē var būt iesaistītas arī vairākas trešās puses, kuras mēs neredzam un ar tām varam arī pat nekomunicēt, bet tās noteikti var ietekmēt uzņēmumu. Proti, runa ir par ārējiem digitālo pakalpojumu sniedzējiem, kuru risinājumus daži no mums izmanto ikdienā, pat to nepamanot, tostarp darba vajadzībām.

Savā darbībā uzņēmumi bieži izmanto dažādus ārpakalpojumu sniedzēju *offline* un *online* risinājumus, piemēram, mākoņdatošanas pakalpojumus, citus datu glabāšanas pakalpojumus, komunikācijas programmatūras (e–pasti, tērzēšanas rīki), sociālos tīklus, *Intranet* portālus un portālus klientiem, darba uzdevumu un procesu optimizēšanas risinājumus, grāmatvedības, apmeklētāju uzskaites un personālvadības programmatūras, informācijas drošības rīkus, korporatīvos transporta nodrošināšanas risinājumus (tostarp taksometru aplikācijas un *GPS* izsekošanas risinājumus), maksājumu veikšanas nodrošināšanas pakalpojumus, klientu atbalsta risinājumus, mārketinga risinājumus (tostarp *CRM* sistēmas, komerciālo paziņojumu izsūtīšanas un aptauju veikšanas rīkus, uzņēmuma lapu apmeklētāju informācijas vākšanas risinājumus) un vairākus citus. Protams, daudz ir atkarīgs no uzņēmuma darbības specifikas, un tas var izmantot īpašus savam biznesam nepieciešamus rīkus.

Aiz visiem šādiem risinājumiem stāv pakalpojumu sniedzējs, un visbiežāk tas ir cits uzņēmums. Lai izmantotu šādu risinājumu, lietotājs noslēdz ar tādu pakalpojumu sniedzēju līgumu (piemēram, akceptē noteikumus un nosacījumus, ieliekot ķeksīti lodziņā pie piekrišanas teksta), ar kuru lietotājs patiesībā iepazīstas diezgan reti. Ja mēs izmantojam konkrētu rīku kādu personas datu apstrādei, tad faktiski bieži mēs uzticam personas datu apstrādi trešajai personai. Regula to neaizliedz, kā arī personas datu apstrādes uzticēšana netiek uzskatīta par negatīvu lietu, galvenais ir to veikt saskaņā ar normatīvo aktu prasībām.

Kāpēc tas ir svarīgi?

No brīža, kad ar personas datiem veic vai potenciāli var veikt jebkuras darbības trešā persona, kura rīkojas uzņēmuma uzdevumā, tiek uzskatīts, ka datu apstrādē ir iesaistīta arī šī trešā persona. Šādus pakalpojumu sniedzējus regula sauc par apstrādātājiem (pirms regulas piemērošanas uzsākšanas bija izmantots termins „operators"), savukārt uzņēmumu, kurš pieņem lēmumu par datiem un dod apstrādātājam norādījumus, – par pārzini. Lai persona kvalificētos kā apstrādātājs, nav obligāti, lai šādai personai būtu iespēja piekļūt personas datiem. Apstrādātājam var būt tikai potenciāla iespēja piekļūt personas datiem vai tas var nodrošināt datu glabāšanu un būt atbildīgs par to, lai dati netiktu izpausti nepilnvarotajai personai vai netiktu nejauši dzēsti.

Saskaņā ar regulu pārzinis ir persona, kura ir atbildīga par personas datu aizsardzības nodrošināšanu. **Tāpēc, ja uzņēmums kā pārzinis nodod datus apstrādātājam, uzņēmums ir atbildīgs par to, ar kādiem nosacījumiem tas notiek un kā apstrādātājs rīkosies ar datiem.** Papildus pie datu pārziņa un pret datu pārzini vēršas datu subjekti, un tam var uzlikt sodu, pat ja pārkāpumu nodarījis apstrādātājs. Ja pārzinis nevēlas piedzīvot nepatīkamas sekas, tostarp attiecībā uz regulā paredzēto sodu uzlikšanu, ir nepieciešams pievērst uzmanību apstrādātāju pārvaldībai.

It īpaši svarīgs var būt jautājums par atbildību, ja ārējo digitālo risinājumu uzņēmums izmanto kopā ar citiem uzņēmumiem, piemēram, viena sadarbības projekta ietvaros. Šajā gadījumā ir aktuāls jautājums ne tikai par to, kā tiek sadalīta atbildība starp diviem partneriem un personu, kas nodrošina izmantoto risinājumu, bet arī kādi datu aizsardzības savstarpēji pienākumi var būt abiem pārziņiem. Sadarbības ietvaros var rasties jautājumi par to, kas ▶

ir atbildīgs par datu saturu, atjaunošanu, par komunikāciju ar datu subjektiem, par drošības risinājumu izvēli, kā arī attiecībām ar apstrādātāju.

Ja atbildības jautājums nav atrunāts starp pārzini un apstrādātāju, kā arī starp diviem uzņēmumiem viena projekta ietvaros (tas ir visbiežāk kopīgajiem pārziņiem) un viņu apstrādātāju, tas var radīt nepatīkamas sekas pirmām kārtām pārziņiem, jo sūdzības un pieprasījumi tiks vērsti pret viņiem.

Kas ir jādara, lai datu apstrādei izmantotu digitālos pakalpojumus?

Pirmkārt, ir svarīgi saprast, kādus ārējos digitālos risinājumus uzņēmums izmanto personas datu apstrādei. Tostarp ir svarīgi saprast, vai visi rīki ir aktuāli vai ir tie, kurus darba vajadzībām noteikti vairs neizmantos. No tādiem pakalpojumiem ir ieteicams atteikties, pārliecinoties, ka dati ir izdzēsti vai ka pakalpojumu sniedzējam ir pienākums nodrošināt datu dzēšanu.

Otrkārt, **pārzinim ir jānodrošina, ka ar apstrādātājiem tiek noslēgts regulas 28. pantam atbilstošs datu apstrādes līgums.** Tā ir viena no visgrūtākajām daļām, jo attiecībās ar digitālo pakalpojumu sniedzējiem ļoti bieži nav klasisku papīra līgumu, kuru slēdz divas puses klātbūtnē. Pirmais izaicinājums šajā gadījumā ir vispār saprast, kā nodrošināt tāda līguma noslēgšanu. Piemēram, var sākt ar iepazīšanos ar pušu starpā jau noslēgtajiem līgumiem (tostarp politikām, noteikumiem un nosacījumiem). Tajos jau var būt iekļauti regulai atbilstoši punkti par datiem. Ja ar pakalpojumu sniedzēju ir tiešs kontakts un ar to ir iespējams sazināties, tad var arī pajautāt, vai tam ir minētā līguma paraugs, kuru puses varētu saskaņot. Savukārt, ja saziņa ar apstrādātāju nav iespējama, tad ir vērts ieskatīties pakalpojumu sniedzēja mājaslapā. Dažos gadījumos tie atsevišķi publisko datu apstrādes līgumu paraugus, kurus pārzinis var prasīt noslēgt, ja uzskata to par nepieciešamu.

Līguma noslēgšanas posmā parasti problēmas rodas, ja digitālā pakalpojuma sniedzēja piedāvātā datu apstrādes līguma nav, un vienoties par līguma noslēgšanu nesanāk, jo nav skaidrs, kā sasniegt pakalpojuma sniedzēja atbildīgo personu saistītajos jautājumos vai tas negrib noslēgt atbilstošo līgumu. Papildu jautājumi var būt saistīti ar tādiem gadījumiem, kad apstrādātājs ir liels digitāls uzņēmums, kuram ir standarta datu apstrādes līgums, kurš var būt arī nelabvēlīgs uzņēmumam, bet ietekmēt to nosacījumus pārzinis nevar. Neskatoties uz vēlmi saņemt noteiktos pakalpojumus, abos minētajos gadījumos izmantot šādu uzņēmumu risinājums bez regulas un pārziņa interešu aizsardzības atbilstošā līguma nav ieteicams. Ja uzņēmums tomēr izmantos tādus pakalpojumus un notiks ar personas datiem saistīts incidents, ir liels risks, ka uzņēmumam var uzlikt sodu par pārkāpumiem, par kuriem uzņēmums var pat nezināt.

Līgumā ir jābūt atrunātiem regulā noteiktajiem nosacījumiem par personas datu apstrādi, piemēram, par datu apstrādes ilgumu, personas datu un datu subjektu kategorijām, drošības un dažām citām niansēm. Vairākiem uzņēmumiem ir izstrādāti standarta datu apstrādes līgumu paraugi, un, saņemot tādu paraugu no sava pakalpojuma sniedzēja, to ir vērts izskatīt un neprezumēt, ka tas atbilst regulai un īpaši uzņēmuma interesēm. Atkarībā no sadarbības būtības ir iespējami dažādi labojumi. Piemēram, ja apstrādātājs sazinās ar uzņēmuma klientiem uzņēmuma vārdā, bet uzņēmums to pa tiešo nedara, tad, iesējams, ir vērts pieprasīt, lai apstrādātājs informētu datu subjektus par viņu datu apstrādi, kā arī nodrošinātu apstrādes pamatu (piemēram, saņemtu piekrišanu vai noslēgtu līgumu ar datu subjektiem). Uzmanību ir nepieciešams pievērst jautājumam par to, ar kādiem nosacījumiem apstrādātājs var piesaistīt apakšuzņēmējus, tostarp kādās valstīs. Uzņēmums var glabāt datus ES, bet apstrādātāja apakšuzņēmējs var atrasties datiem nedrošā trešajā valstī un glabāt datus šajā valstī. Šajā gadījumā datu drošība nebūs garantēta. Cits svarīgs uzdevums ir nodrošināt, ka jautājumu gadījumā pārzinim būs iespēja saņemt no apstrādātāja informāciju par uzticēto personas datu apstrādi, kā arī veikt apstrādātāja auditu. Vairākos gadījumos apstrādātāju interesēs ir ierobežot tādas tiesības, bet pārziņa – paredzēt pēc iespējas stingrākus nosacījumus. Regulas 28. panta 3. punkts paredz, ka apstrādātājam ir pienākums sniegt pārzinim visu nepieciešamo informāciju un ļaut veikt auditus, lai parādītu atbilstību saviem pienākumiem saskaņā ar regulu. Tostarp ir nepieciešams vienoties par audita veikšanas gaitu un iespējamām izmaksām, jo audita ietvars var būt ļoti dažāds.

Apstrādātājam ir pienākums sniegt pārzinim visu nepieciešamo informāciju un ļaut veikt auditus, lai parādītu atbilstību saviem pienākumiem saskaņā ar regulu.

Nākamais solis būtu izskatīt, kādi dati ir palikušajos digitālajos datu apstrādes risinājumos. Proti, ir nepieciešams atbildēt uz jautājumiem par to, vai visi dati, kas tur atrodas, uzņēmumam ir nepieciešami, vai ir vēsturiska informācija, kura glabājas drošības pēc, bet sen vairs nav vajadzīga. Papildus, iespējams, vairs nepastāv datu apstrādes pamats, piemēram, datu subjekts atsaucis savu piekrišanu vai likumā noteiktais glabāšanas termiņš jau notecējis. Ja dati vairs nav nepieciešami un to apstrādei nav pamata, tad datus var dzēst ārā. Ja pats rīks nenodrošina uzņēmumam iespēju pašam datus izdzēst, jāvēršas pie apstrādātāja, tas ir, pakalpojuma sniedzēja. Saskaņā ar regulas 28. panta 3. punktu tam ir pienākums datus izdzēst pēc pārziņa pieprasījuma, izņemot, piemēram, ja apstrādātājam ir pienākums datus glabāt saskaņā ar normatīvo aktu prasībām.

Foto Jānis Deinats

Anna Vladimirova–Krjukova, LL.M., zvērinātu advokātu biroja *COBALT* juriste, sertificēta personas datu aizsardzības speciāliste

Savukārt attiecībā uz sadarbību starp kopīgiem pārziņiem regula paredz citas prasības. Proti, regulas 26. pants nosaka, ka **kopīgiem pārziņiem ir pienākums vienoties par to, ka šādu partneru starpā tiks sadalīti pārziņa noteikti pienākumi, tostarp attiecībā uz datu subjektu tiesībām.** Šādos gadījumos ir ieteicams noslēgt rakstveida vienošanos, paredzot nosacījumus par atbildību. Lai gan regulas 26. pants nav tik detalizēts kā 28. pants par apstrādātājiem, tas automātiski nenozīmē, ka kopīgiem pārziņiem nav par ko vienoties. Tieši otrādi, pārzinim regulā noteikti vairāki pienākumi. Un kopīgiem pārziņiem ir jāvienojas, kas un kādā apjomā ir atbildīgs par konkrētām lietām, tostarp par personas datu apstrādes pamata nodrošināšanu (piemēram, piekrišanas saņemšanu), par komunikāciju ar datu subjektiem, incidenta paziņošanu uzraudzības iestādei, drošības risinājumiem, tostarp par līguma noslēgšanu ar apstrādātāju un to kontroli.

Nepieciešams nodrošināt, ka uzņēmuma darbinieki zina, kā izmantot uzņēmuma digitālos risinājumus un kādus datus drīkst glabāt, cik ilgi un kādā veidā. Tas palīdzēs nodrošināt to, ka arī tiek veikti faktiski pasākumi datu aizsardzībai.

Ņemot vērā digitālo iespēju ātro attīstību, vairāki uzņēmumi vēlas baudīt potenciālus labumus, ko var saņemt, izmantojot jaunus tehniskus rīkus. Tā ir pozitīva tendence, tomēr ir svarīgi atcerēties, ka **personas dati ir savā ziņā aktīvs, kuru nevar uzticēt trešajai personai bez atbilstošas aizsardzības.** Šī aktīva pazaudēšana var būt nepatīkama gan pašam uzņēmumam, gan tā klientiem un sadarbības partneriem. BJP

Materiāls tapis sadarbībā ar COBALT

Vai apdrošinātāju atteikumi vienmēr ir pamatoti?

Slēdzot transportlīdzekļu apdrošināšanas līgumus, auto īpašnieki vēlas nodrošināties, ka, iestājoties apdrošinājuma gadījumam, viņiem nenāksies ciest zaudējumus, jo tiks izmaksāta apdrošināšanas atlīdzība. Tomēr dzīvē apdrošināšanas ņēmējiem nereti nākas saskarties ar apdrošināšanas atlīdzības izmaksu atteikumiem, t.sk. pašu apdrošināšanas ņēmēju pieļautu pārkāpumu dēļ.

Aktuālā tiesu prakse liecina, ka ne vienmēr apdrošinātāju atteikumi ir uzskatāmi par tiesiskiem un pamatotiem. Piemēram, nereti apdrošinātāji strīdus situācijās mēdz nepareizi piemērot apdrošināšanas līguma noteikumus vai arī piemēro tos formāli, nepastāvot cēloņsakarībai starp pieļauto pārkāpumu un apdrošināšanas gadījumu.

Apdrošināšanas atlīdzības izmaksas atteikumi formālu iemeslu dēļ

Tēmas aktualitāti raisīja konkrēts gadījums. Apdrošinātājs atteicās izmaksāt apdrošināšanas atlīdzību par transportlīdzekļa zādzību, jo zādzības brīdī auto nebija veikta valsts tehniskā apskate. Tā kā apdrošināšanas līgums paredzēja, ka atlīdzība netiek izmaksāta par zaudējumiem, kas radušies gadījumos, kad transportlīdzeklim nav bijusi veikta