DARBINIEKS ĀRVALSTĪS – VAI DATI DROŠĪBĀ?

ANNA VLADIMIROVA-KRJUKOVA,

SIA "ZAB COBALT" vecākā speciāliste, sertificēta personas datu aizsardzības speciāliste Latvijā un Eiropā

Beidzamajos gados situācija darba tirgū un pakalpojumu sniegšanā ir mainījusies – darbinieki tagad var strādāt no jebkuras vietas pasaulē, pielāgojot vidi un apstākļus savām vēlmēm. Tomēr, ja uzņēmuma rīcībā ir personas dati, šāda starptautiska vide rada arī būtiskus datu aizsardzības riskus. Kā tos novērst?

Mūsdienās uzņēmumi, kam rodas grūtības atrast darbiniekus Latvijā, var pieņemt darbā cilvēkus no jebkuras valsts, neprasot viņiem pārcelties uz Latviju. Turklāt ne visiem šādi piesaistītiem cilvēkiem ir darba līgums. Daži darbojas, pamatojoties uz uzņēmuma vai cita līguma pamata, tādējādi viņi drīzāk uzskatāmi par ārpakalpojumu sniedzējiem vai konsultantiem. Šāda hibrīda vide rada datu aizsardzības riskus, ja uzņēmuma rīcībā ir personas dati, kas var būt ne tikai klientu informācija, bet arī citu darbinieku un pakalpojumu sniedzēju vai to kontaktpersonu dati.

Kopš 2021. gada vasaras šādiem personas datu aizsardzības riskiem veltīta īpaša uzmanība saistībā ar izmaiņām prasībās, kas paredzētas starptautiskai datu nodošanai. Lai saprastu, kā šādos apstākļos nodrošināt atbilstību regulai 2016/679 jeb Vispārīgajai datu aizsardzības regulai, jānosaka, pirmkārt, vai personas datus nodod uz trešajām valstīm regulas izpratnē, otrkārt, kā šādā situācijā nodrošināt personas datu aizsardzību saskaņā ar regulu.

VAI DATUS NODOD TREŠAJĀM VALSTĪM?

Saskaņā ar regulu un Eiropas Datu aizsardzības kolēģijas (Kolēģija) vadlīnijām 05/2021 papildu aizsardzība personas datiem atbilstoši regulas 5. nodaļai "Personas datu nosūtīšana uz trešajām valstīm vai starptautiskām organizācijām" ir jānodrošina, ja izpildās visi šie nosacījumi:

- uzņēmums pārsūta personas datus no Eiropas Savienības (ES) un/vai Eiropas Ekonomikas zonas (EEZ) teritorijas uz citām trešajām valstīm vai teritorijām;
- uzņēmumam, kas nodod personas datus uz trešajām valstīm, piemērojas regulas prasības saskaņā ar tās 3. pantu. Parasti tas notiek, kad uzņēmums, kas nodod datus, nodibināts ES vai EEZ. Retākas ir situācijas, kad uzņēmums nodibināts ārpus ES vai EEZ, bet piedāvā preces un/vai pakalpojumus ES;
- trešās valstis vai teritorijas nav iekļautas Eiropas Komisijas (EK) valstu sarakstā ar pietiekamu datu aizsardzības līmeni. Šobrīd šajā sarakstā ir Andora, Apvienotā Karaliste, Argentīna, Dienvidkoreja, Džērsija, Gērnsija, Fēru salas, Izraēla, Japāna, Jaunzēlande, Kanāda (attiecas tikai uz komersantiem), Menas sala, Šveice un Urugvaja;
- personas dati vai šo datu nesēji fiziski atrodas trešajās valstīs (piemēram, dokumenti, serveri ar informāciju, dators ar tajā esošo informāciju, ārējie cietie diski, USB atmiņas vai citi datu nesēji);
- uzņēmums nodod personas datus saņēmējiem trešajās valstīs, kuri nav šī uzņēmuma darbinieki, kas īsteno attālinātu piekļuvi uzņēmumā esošajai informācijai.

Piemēram, Latvijā esošam uzņēmumam ir pienākums ieviest regula 5. sadaļā paredzētos speciālos personas datu

aizsardzības risinājumus, ja tas:

- piesaista darbam cilvēku Ukrainā, kam ir pieejami uzņēmumā esošie personas dati, bet ar kuru nav noslēgts darba līgums (tā vietā var būt uzņēmuma līgums vai jebkurš līdzīgs līgums);
- izmanto Amerikas Savienoto Valstu (ASV) uzņēmuma pakalpojumus, padarot ASV uzņēmumam pieejamus personas datus. Tā bieži notiek, kad uzņēmums izmanto kādus digitālus risinājumus, kuru īpašnieks atrodas ASV;
- nodod citam Ķīnā esošam grupas uzņēmumam darbinieku vai klientu personas datus.

Tomēr, ja Latvijas uzņēmuma darbinieks strādā no Taizemes, Meksikas vai Baltkrievijas, regulas 5. nodaļā paredzētie speciālie datu aizsardzības risinājumi nav jāievieš. Vienlaikus regulas 5. nodaļas nepiemērošana neatceļ pārējās regulas prasības, līdz ar to šāda attālināta darba gadījumā darba devējam ir pienākums izveidot datu aizsardzības sistēmu, kas minimizē datu aizsardzības riskus.

KĀDI SOĻI JĀVEIC?

Veicamo darbu saraksts atkarīgs no tā, vai personas datu nodošanai piemērojamas regulas 5. nodaļas prasības atbilstoši iepriekš aplūkotajam. Ja uzņēmumam jāievieš 5. nodaļas prasības, tam jāveic šādas darbības, kas noteiktas Kolēģijas rekomendācijas 01/2020.

RISINĀJUMA IZVĒLE

Pirmkārt, uzņēmumam jāizvēlas konkrēts regulas 5. nodaļā pieejamais personas datu aizsardzības risinājums (regulas 45., 46. un 49. pants). To var izvēlēties atkarībā no personas datu nodošanas veida. Populārākie risinājumi ir piemērot saistošus uzņēmuma noteikumus (ja datu nodošana notiek uzņēmumu grupā) un EK datu aizsardzības standartklauzulas pārējos gadījumos.

Ja uzņēmumi izmanto privātus pakalpojumu sniedzējus, visbiežāk tie izvēlas tieši beidzamo risinājumu, jo uzskata to par vienkāršāko. Tomēr 2021. gada vasarā situācija mainījās, jo saskaņā ar jauno standartklauzulu versiju to pusēm jāveic rakstveida personas datu nodošanas novērtējums (skat. nākamo sadaļu), kas padara standartklauzulu noslēgšanas procesu ilgāku un sarežģītāku. Ar to jārēķinās arī tiem, kas joprojām paļaujas uz veco EK standartklauzulu versiju, jo līdz šā gada beigām visiem jāpāriet uz 2021. gada 4. jūnija

Uzņēmumam jānodrošina, ka tā izvēlētais personas datu aizsardzības risinājums ir ieviests un darbojas pareizi, un jāveic periodiska novērtējuma un izmantoto risinājumu pārskatīšana.

dokumenta versiju (skat. EK īstenošanas lēmumu 2021/914 par līguma standartklauzulām attiecībā uz personas datu nosūtīšanu trešajām valstīm).

DOKUMENTĒTS NOVĒRTĒJUMS

Otrkārt, uzņēmumam jāizvērtē personas datu nodošana, dokumentējot šo novērtējumu. Kā jau minēts iepriekš, šī novērtējuma veikšana ir obligāta standartklauzulu noslēgšanas sastāvdaļa. Tomēr saskaņā ar Kolēģijas rekomendācijām 01/2020 šis novērtējums jāveic arī pārējos gadījumos, kad dati nodoti trešajās valstīs. Novērtējumam nav konkrētas formas, un tā saturs atkarīgs no katra individuālā gadījuma. Jautājumi, kas jāvērtē, ir trešo valstu publisko iestāžu tiesības piekļūt datiem, trešajā valstī piemērojamās tiesības un likumu piemērošanas prakse, kā arī datu nodošanas juridiskie un tehniskie apstākļi.

PAPILDU MEHĀNISMI

Treškārt, uzņēmumam jāievieš papildu mehānismi datu aizsardzībai. Atkarībā no novērtējuma rezultātiem uzņēmumam ir pienākums izvērtēt un nepieciešamības gadījumā ieviest līgumiskus, organizatoriskus un/vai tehniskus aizsardzības risinājumus. Turklāt skaidrs, ka daži gadījumi, piemēram, datu nodošana uz ASV, vistamāk, jāatbalsta ar tehniskiem aizsardzības līdzekļiem, jo, vērtējot Eiropas Savienības Tiesas (EST) praksi, līgumiski risinājumi nav pietiekami.

Tāpat uzņēmumam jānodrošina, ka tā izvēlētais risinājums ir ieviests un darbojas pareizi, un jāveic periodiska novērtējuma un izmantoto risinājumu pārskatīšana.

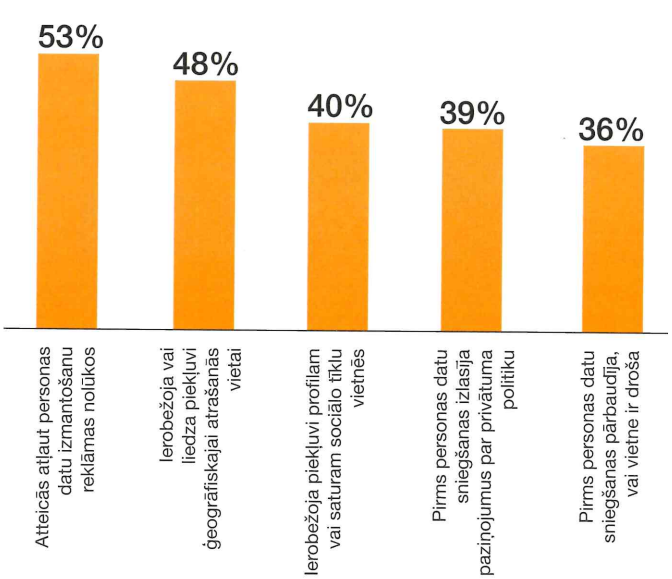
Ņemot vērā aplūkotos uzdevumus, kā arī neseno regulatoru un tiesu praksi, ir skaidrs, ka personas datu nodošana ārpus ES un EEZ tagad ir sarežģītāks process, kurā jāiegulda resursi. Viens no iemesliem šādai tendencei ir problēmas, kuras konstatētas vairāku gadu laikā un pārsvarā saistītas ar pārāk plašu publisko iestāžu pilnvarojumu piekļūt konkrētās valsts jurisdikcijā esošajiem datiem. Šāda situācija izskatīta, piemēram, EST 2020. gada 16. jūlija spriedumā lietā C-311/18.

PIESARDZĪBA JĀIEVĒRO

Ja uzņēmums tomēr neveic regulas 5. nodaļā paredzēto personas datu nodošanu ārpus ES, bet personas datiem piekļūst Latvijā esošā uzņēmuma darbinieki, kas strādā no trešajām valstīm, tam arī jānodrošina personas datu aizsardzība, ievērojot citas vispārīgas regulas prasības. Proti, uzņēmumam jāīsteno atbilstoši organizatoriski un tehniski pasākumi, lai nodrošinātu atbilstību regulas pamatprincipiem, kā arī 24. (pārziņa atbildība), 32. (personas datu drošība), 35. (novērtējums par ietekmi) u.c. pantiem.

Tas nozīmē, ka uzņēmumam jārēķinās ar attālinātu piekļuvi personas datiem vai personas datu izmantošanu trešajā valstī, kurā atrodas darbinieks, izvērtējot drošības riskus un veicot novērtējumu par ietekmi. Atkarībā no situācijas var būt pietiekami, ja uzņēmums ievieš iekšējās vadlīnijas, kas jāievēro, strādājot no ārzemēm, paredzot tajās standartklauzulām līdzīgas garantijas. Tomēr dažos gadījumos situācijai var būt nepieciešami arī sarežģītāki tehniskie risinājumi, kas nodrošina, ka uzņēmuma rīcībā esošie personas dati ir konfidenciāli, pieejami uzņēmumam nepieciešamajā brīdī un ir nodrošināta to integritāte.

KĀ EIROPAS SAVIENĪBAS IEDZĪVOTĀJI PĒRN AIZSARGĀJA SAVUS DATUS INTERNETĀ?



Avots: Europa.eu