FINANSES

Datu nodošana uz trešajām valstīm

2021-02-19

Gabriela Šantare, ZAB "Cobalt", juriste

Kamēr uzņēmējdarbība notiek vien mūsu valsts robežās, viss šķiet saprotami un ierasti. Izaicinājumi rodas, kad sākam darboties plašāk. Tā tas ir teju visās jomās, bet šoreiz plašāk aplūkosim datu aizsardzību un nodošanu uz valstīm ārpus Eiropas Savienības.

Personas datu nodošana uz trešajām valstīm vienmēr bijis izaicinājums. Eiropas Parlamenta un Padomes regulā 2016/679 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti jeb Vispārīgajā datu aizsardzības regulā (Regula) paredzēts, ka personas datus var nodot uz trešajām valstīm, ja tādējādi nesamazinās ar Regulu garantētais fizisku personu aizsardzības līmenis. Tomēr kopš 2020. gada 16. jūlija, kad Eiropas Savienības Tiesa spriedumā lietā C-311/18 atzina par spēkā neesošu Eiropas Savienības-Amerikas Savienoto Valstu Privātuma vairogu (*EU-US Data Protection Shield*), personas datu nodošana uz trešajām valstīm pakļauta īpašai uzraudzībai. Lai saprastu turpmāk pieļaujamo personas datu plūsmu ārpus Eiropas Savienības (ES), Eiropas Datu aizsardzības kolēģija (Kolēģija) publicējusi vadlīnijas, kādos gadījumos un kā var turpināt nodot personas datus citiem pārziņiem vai apstrādātājiem, ja tie atrodas ārpus ES.

Lai gan sākotnēji šķiet, ka Kolēģijas vadlīnijas aizliedz nodot personas datus uz trešajām valstīm, tā nav, tomēr ikvienam personas datu nosūtītājam jābūt skaidrai izpratnei par personas datu plūsmu un konkrētās valsts personas datu aizsardzības garantijām.

Soļi starptautiskā datu nodošanā

Kolēģija publicējusi vadlīnijas, kas sešos soļos skaidro nepieciešamās darbības, kuras jāveic ikvienam datu apstrādātājam vai datu pārzinim, kas plāno nodot vai nodod personas datus ārpus ES. Turpmāk minētie soļi attiecīgajam datu nosūtītājam ir ne vien jāizvērtē, bet arī jādokumentē, lai nepieciešamības gadījumā tos uzrādītu uzraudzības iestādei.

Pirmais solis

Pirmkārt, datu pārzinim vai datu apstrādātājam jāidentificē visi personas datu nodošanas gadījumi ārpus ES. Jāņem vērā, ka datu nosūtīšana uz trešajām valstīm ir ne tikai faktiska datu nodošana, bet arī nodrošina personām trešajās valstīs attālinātu piekļuvi datiem ES.

Lai iegūtu pārliecību un izpratni par personas datiem un to nodošanu uz citām valstīm, jāveido aktuāls un atjaunots personas datu reģistrs.

Otrais solis

Otrkārt, datu pārzinim vai datu apstrādātājam jānoskaidro, uz kādiem datu nodošanas mehānismiem viņš balstās, lai nodotu personas datus uz trešajām valstīm atbilstoši Regulas V nodaļai "Personas datu nosūtīšana uz trešām valstīm vai starptautiskām organizācijām". Iespējamie mehānismi ir, piemēram:

- nosūtīšana atbilstoši Regulas 45. pantam, pamatojoties uz lēmumu par aizsardzības līmeņa pietiekamību;
- nosūtīšana, pamatojoties uz Regulas 46. pantā noteiktajiem mehānismiem, piemēram, standarta līguma klauzulu vai saistošiem uzņēmuma noteikumiem;
- nosūtīšana, pamatojoties uz Regulas 49. pantā paredzētajām atkāpēm, piemēram, datu subjekta piekrišanu.

Trešais solis

Treškārt, ja datu nodošana balstās uz Regulas 46. pantā regulēto mehānismu (nosūtīšana, pamatojoties uz atbilstošām garantijām), datu pārzinim vai datu apstrādātājam, kas vēlas nodot personas datus uz trešo valsti, jāizvērtē, vai izvēlētais mehānisms ir efektīvs. Proti, paļaušanās tikai uz izvēlēto mehānismu var nebūt pietiekama, jo šim mehānismam arī jānodrošina, ka datu nodošanas rezultātā netiek samazināts ar Regulu garantētais personas datu aizsardzības līmenis. Tātad datu nodošanai jābūt efektīvai arī praksē.

Lai noskaidrotu, vai izvēlētais līdzeklis ir efektīvs, jāizvērtē, vai konkrētās trešās valsts tiesību aktos vai praksē ir kāds elements, kas varētu apdraudēt izvēlētā mehānisma efektivitāti. Ja iespējams, personas datu saņēmējam jāsadarbojas un jāpalīdz datu nosūtītājam, sniedzot informāciju, tiesību aktus un avotus par konkrēto valsti. Datu pārzinim vai apstrādātājam jāizmanto arī publiski pieejamie resursi, lai novērtētu konkrētās valsts tiesību aktus un personas datu aizsardzības līmeni. Šajā posmā datu pārzinim vai datu apstrādātājam jāizvērtē saņēmējvalsts tiesību akti, ievērojot apstrādes raksturu, darbības jomu un nolūkus.

Ceturtais solis

Ceturtkārt, ja trešajā solī veiktā izvērtējuma rezultātā secināts, ka izvēlētais Regulas 46. panta mehānisms nav pietiekami efektīvs, jāizlemj, vai personas datu aizsardzību varētu nodrošināt ar papildu mehānismiem. Konkrētais papildu mehānisms un tā piemērotība jāizvērtē katrā atsevišķā gadījumā.

Papildu mehānisms var būt līgumisks, tehnisks vai organizatorisks. Dažādu papildu mehānismu izmantošana var nodrošināt atbilstošu personas datu aizsardzības līmeni. Kolēģija publicējusi neizsmeļošu sarakstu ar iespējamiem papildu mehānismiem, tostarp:

- līgumiski mehānismi:
  - datu saņēmēja pienākums izmantot specifiskus tehniskus līdzekļus;
  - caurspīdīguma pienākumi, kas paredz datu saņēmējam sniegt atskaites un informēt par personas datu apstrādi;
  - pienākums pārskatīt un apstrīdēt/pārsūdzēt jebkura personas datu izpaušanas lūguma, ko pieprasa tiesību aizsardzības iestādes, tiesiskumu;
  - pienākums saņemt datu nosūtītāja vai datu saņēmēja skaidru piekrišanu, lai piekļūtu personas datiem;
- tehniski mehānismi:
  - personas datu šifrēšana;
  - personas datu pseidonimizācija;
  - dalīta personas datu apstrāde;
- organizatoriski mehānismi:
  - izmantot iekšējās politikas, nosakot rīcību, ja no konkrētās valsts iestādēm ir pieprasījums piekļūt personas datiem;
  - saglabāt piekļuves pieprasījumus, tostarp juridisko pamatojumu un personas, kas to pieprasījušas;
  - regulāri publicēt caurspīdīguma atskaites vai kopsavilkumus par valsts iestāžu piekļuves pieprasījumiem;
  - iesaistīt datu aizsardzības speciālistu;
  - izstrādāt un pieņemt personas datu aizsardzības un personas datu privātuma politikas, kuras balstās uz ES sertifikāciju vai starptautiskiem standartiem (piemēram, Starptautiskās standartizācijas organizācijas (*International Organization for Standardization*) standartiem).

Jāņem vērā, ka jebkurā gadījumā par mehānismu efektivitāti un atbilstības nodrošināšanu atbild personas datu nosūtītājs, kam saukt piemērot atbildību par lēmumiem un starptautisko personas datu nosūtīšanu.

Piektais solis

Piektkārt, personas datu nosūtītājiem jāveic visas formālās procesuālās darbības, lai ieviestu atbilstošu personas datu aizsardzību. Procesuālās darbības var atšķirties atkarībā no izvēlētā Regulas 46. panta mehānisma.

Sestais solis

Sestkārt, personas datu nosūtītājam regulāri jāuzrauga tiesību aktu un prakses attīstība trešajā valstī, uz kuru nodos personas datus. Šāda uzraudzība nepieciešama, lai pārliecinātos, vai sākotnējais valsts datu aizsardzības izvērtējums nav mainījies un joprojām ir atbilstošs Regulā noteiktajiem standartiem un garantijām. Turklāt šis pienākums izriet arī no Regulā nostiprinātā pārskatatbildības principa.

Vienlaikus personas datu nosūtītājam jāievieš procedūras, lai varētu ātri apturēt vai pārtraukt personas datu nodošanu uz trešo valsti, ja:

- datu saņēmējs pārkāpis vai neizpilda uzņemtās saistības atbilstoši izvēlētajam Regulas 46. panta mehānismam;
- papildu mehānismi konkrētajā valstī vairs nav efektīvi.

Datu aizsardzības līmeņa novērtēšana

Vienlaikus ar vadlīnijām par papildu mehānismiem personas datu nodošanai uz trešajām valstīm Kolēģija publicēja arī vadlīnijas, kas personas datu nosūtītājam palīdz izvērtēt, vai trešās valsts uzraudzības mehānismi un tiesībsargājošo iestāžu pilnvaras nodrošina atbilstošu personas datu aizsardzības līmeni valstī un Regulā noteiktās datu aizsardzības un datu subjektu garantijas.

Kolēģija paredzējusi četras garantijas, kas jāanalizē personas datu nosūtītājiem, proti, jānosaka, vai:

- personas datu apstrāde balstās uz skaidriem, precīziem un pieejamiem noteikumiem;
- pierādīta nepieciešamība un samērīgums izvirzītajiem leģitīmajiem mērķiem;
- ieviesti neatkarīgi uzraudzības mehānismi;
- indivīdam pieejami efektīvi tiesību aizsardzības līdzekļi.

Lai gan personas datu nodošana ārpus ES kļūst arvien sarežģītāka un izaicinājumiem bagātāka, tā joprojām nav aizliegta. Kolēģijas vadlīnijas sniedz pragmatisku un precīzu izklāstu, kas jāievēro ikvienam datu nosūtītājam, lai izpildītu Regulā noteiktos pienākumus.