DATU AIZSARDZĪBA
Decembris, 2017

KĀDUS PIENĀKUMUS NOSAKA ES VISPĀRĪGĀ DATU AIZSARDZĪBAS REGULA?

Pēc pusgada, 2018. gada 25 maijā, sāks piemērot ES Vispārīgo datu aizsardzības regulu, kas paaugstina datu pārziņu un apstrādātāju atbildību, kā arī nosaka jaunas prasības uzņēmumiem, iestādēm un organizācijām fizisku personu datu apstrādei. Kādus pienākumus jaunais regulējums uzliek datu pārziņiem (tiem, kas lemj, kādi dati ir jāvāc un kā tie ir jāapstrādā) un datu apstrādātājiem (tiem, kas glabā vai apstrādā datus), ir pirmais jautājums, uz ko ir jāatbild, lai varētu izpildīt Regulas prasības un izvairīties no administratīvajiem naudas sodiem, kas var sasniegt līdz pat 20 miljoniem eiro vai 4% no apgrozījuma.

Atbildības pierādīšana

Regula ievieš jaunu pārskatatbildības principu, kas uzliek pārziņiem pienākumu uzskatāmi parādīt, ka to darbība atbilst datu aizsardzības principiem:

- Likumīgums
- Godprātība un pārredzamība
- Nolūka ierobežojumi
- Datu minimizēšana
- Precizitāte
- Glabāšanas ierobežojums
- Integritāte un konfidencialitāte jeb datu drošība

Lai pierādītu atbilstību Regulas prasībām, ir jāizstrādā un jāsaglabā dokumentācija, kas pierāda veiktos pasākumus, lai nodrošinātu atbilstību, ieskaitot apstrādes darbību reģistru, ietekmes uz datu aizsardzību novērtējumu, datu nodošanas līgumus, līgumus ar apstrādātājiem, mājas lapas privātuma politiku, piekrišanas formas, iekšējās procedūras datu pārkāpuma gadījumā u.c.
Katram datu pārzinim būtu ieteicams nodrošināties ar privātuma politiku, kas ietvertu skaidrus un saprotamus personas datu apstrādes noteikumus.

Tehnisko un organizatorisko pasākumu īstenošana

Regulas prasību izpildi pierāda pārziņa un apstrādātāja veiktie tehniskie un organizatoriskie pasākumi, ieskaitot atbilstošu datu aizsardzības garantiju ieviešana (piem., datu aizsardzība pēc noklusējuma; integrēta datu aizsardzība, šifrēšana un pseidonimizācija), datu aizsardzības speciālista iecelšana, sadarbība ar Datu valsts inspekciju, atbilstība rīcības kodeksam un sertifikācija, apmācību rīkošana darbiniekiem, datu subjektu informēšana, pieprasījumu pārvaldība, kā arī veiktie drošības pasākumi.

Tiesiskā pamata izvērtēšana

Datu apstrādei ir jābūt likumīgai, kas nozīmē, ka ir jābūt kādam tiesiskam pamatam. Apstrādes tiesiskais pamats var būt:

- Piekrišana
- Līguma izpilde
- Juridiskais pienākums
- Personas vitālas intereses
- Sabiedrības intereses un likumīgi piešķirtās oficiālās pilnvaras
- Leģitīmas intereses

Viens no nedrošākajiem tiesiskajiem pamatiem ir piekrišana, ņemot vērā, ka tai ir jābūt brīvai, konkrētai, apzinātai un viennozīmīgai. Piekrišana nav brīva, piemēram, ja no tās ir atkarīga līguma izpilde, tostarp pakalpojuma sniegšana. Piekrišanai ir jābūt dotai ar skaidri apstiprinošu darbību. Lai piekrišana būtu apzināta, persona ir jāinformē par pārziņa identitāti un paredzētās personas datu apstrādes nolūkiem, turklāt piekrišanu var atsaukt jebkurā laikā. Ja nav iespējams ievērot kādu no piekrišanas nosacījumiem, lai varētu veikt datu apstrādi, ir jābūt citam tiesiskam pamatam, kas var būt, piemēram, līguma izpilde vai uzņēmuma leģitīmās intereses.

Datu subjekta tiesību garantēšana

Regula piešķir datu subjektiem plaša apjoma tiesības, kas ir jānodrošina pārziņiem un apstrādātājiem: tiesības saņemt informāciju; piekļuves tiesības; tiesības labot datus; tiesības dzēst datus; tiesības prasīt, lai pārzinis ierobežo apstrādi; tiesības iebilst pret datu apstrādi, kā arī lēmumiem, kuru pamatā ir tikai automatizēta apstrāde, tostarp profilēšana; tiesības uz datu pārnesamību.
Iegūstot datus no datu subjekta vai trešās personas, pārzinim ir pienākums sniegt datu subjektam plaša apjoma informāciju par iegūto datu apstrādi, pārziņa identitāti un kontaktinformāciju, datu aizsardzības speciālista kontaktinformāciju, apstrādes nolūku un juridisko pamatu,

personas datu saņēmējiem, datu subjekta tiesībām un citiem nosacījumiem, kas ir būtiski. Turklāt informācija ir jāsniedz pārredzamā, saprotamā un viegli pieejamā veidā, izmantojot skaidru un vienkāršu valodu. Pārzinim ir arī jānodrošina, ka datu subjekts var ar to sazināties, lai realizētu visas Regulā garantētās tiesības.

Datu reģistrēšana

Lai varētu novērtēt, kādu datu apstrāde tiek veikta, vai un kāds tiesiskais pamats pastāv attiecīgajai datu apstrādei, vispirms ir jāveic datu apzināšana un sagrupēšana jeb datu audits, novērtējot, kādi dati ir uzņēmuma rīcībā un kā tie tiek apstrādāti. Datu apzināšanas rezultātā ir jāspēj atbildēt uz jautājumiem:

Kas? Ko? Kāpēc? Kur? Cik ilgi? Kādā veidā?

Pārzinim ir pienākums reģistrēt tā pakļautībā veiktās apstrādes darbības, kā arī datu apstrādātājam ir jāuztur pārziņa vārdā veikto apstrādes darbību kategoriju reģistrs šādos gadījumos:

- Tas nodarbina vairāk par 250 personām;
- Uzņēmuma vai struktūras veiktā apstrāde varētu radīt risku datu subjektu tiesībām un brīvībām;
- Apstrāde ir regulāra;
- Apstrāde ietver īpašas datu kategorijas vai personas datus par sodāmību un pārkāpumiem.

Būtībā katram datu pārzinim būtu jāapzina, kādus datus tas apstrādā, lai varētu izvērtēt apstrādes riskus un darbības, kas veicamas, lai nodrošinātu un pierādītu atbilstību Regulai. Datu apzināšana ļaus prioritizēt svarīgākos uzdevumus, kas ir jāpaveic līdz Regulas spēkā stāšanās brīdim.

Novērtējums par ietekmi uz datu aizsardzību

Datu pārzinim ir pienākums veikt novērtējumu par ietekmi uz datu aizsardzību, ja apstrāde varētu radīt augstu risku fizisku personu tiesībām un brīvībām, lai izvērtētu augstā riska iespējamību un nopietnību. Par augstu risku liecina tādi faktori kā personisku aspektu sistemātiska un plaša novērošana, tostarp profilēšana, īpašu kategoriju jeb sensitīvo datu apstrāde, sistemātiska publisku vietu videonovērošana u.c.
Uzraudzības iestādēm ir jāizstrādā saraksts ar tiem apstrādes darbību veidiem, attiecībā uz kuriem ir jāveic novērtējums par ietekmi uz datu aizsardzību.
Novērtējumā ir jāietver plānoto apstrādes darbību un apstrādes nolūks, tostarp pārziņa leģitīmo interešu sistemātisks apraksts; novērtējums par apstrādes darbību nepieciešamību un samērīgumu; novērtējums par riskiem datu subjektu tiesībām un brīvībām; pasākumus, kas paredzēti

risku novēršanai; drošības pasākumus un mehānismus, ar ko nodrošina personas datu aizsardzību un pierāda, ka ir ievērota Regula.

Datu aizsardzības speciālista nozīmēšana

Uzņēmumiem ir pienākums iecelt datu aizsardzības speciālistu gadījumā, ja tie veic regulāru un sistemātisku datu subjektu novērošanu plašā mērogā, piemēram, profilēšanu, apstrādā īpašu kategoriju datus, kā arī datus par pārkāpumiem un sodāmību. Tāpat datu apstrādes speciālists ir jāieceļ katrā valsts iestādē, kas veic datu apstrādi. Datu aizsardzības speciālists var būt pārziņa vai apstrādātāja darbinieks, vai arī veikt uzdevumus, pamatojoties uz pakalpojumu līgumu.

Datu drošība un datu pārkāpumu paziņošana

Pārzinim un apstrādātājam ir jāīsteno atbilstīgi tehniski un organizatoriski pasākumi, lai nodrošinātu tādu drošības līmeni, kas atbilst datu apstrādes riskam, un jāizstrādā iekšējā procedūra datu aizsardzības pārkāpumu gadījumos. Pārzinim ir jāspēj par pārkāpumu 72 stundu laikā paziņot uzraudzības iestādei, kā arī gadījumā, ja tas varētu radīt augstu risku fizisku personu tiesībām un brīvībām, bez nepamatotas kavēšanās informēt arī datu subjektus.

ICT Legal palīdzēs Jums nodrošināt Regulas prasību izpildi. Lai saņemtu vairāk informācijas par konkrētiem pakalpojumiem, lūdzam sazināties ar –

Irēnu Ņesterovu
Sertificētu personas datu aizsardzības speciālisti
irena.nesterova@ictlegal.lv
+371 29656586

ICT legal