

Kā pārliecināties, ka uzņēmuma darbība atbilst datu regulai? (1) 1/32/20

Nesen medijus pāršalca ziņas par līdz šim Latvijā lielākā soda (150 000 eiro) piemērošanu e-komercijas uzņēmumam par pārkāpumiem, kas saistīti ar Vispārīgās datu aizsardzības regulas prasību neievērošanu. Ievērojot uzņēmuma apstākļus, uz kuriem savā lēmumā norādīja Datu valsts inspekcija, šajā rakstā – par prasībām, kas jāievēro jebkurai uzņēmumam, kurš apstrādā personas datus interneta vietnēs, lai nesāņemtu regulā paredzēto sodu.

Regulas normas

Datu regula attiecas uz visiem uzņēmumiem, kas piedāvā preces vai pakalpojumus ES pilsoņiem, un to piemēro jebkurai e-komercijas uzņēmumam, kas izmanto ES dzīvojošo fizisko personu datus. Datu regula attiecas uz visām datubāzēm, kas satur lietotāju informāciju, piemēram, kredītkaršu datus un pirkumu datus.

Atbilstoši datu regulai sodu par konstatētiem pārkāpumiem, tostarp pārkāpumu, par kuru sodu piemēroja Latvijā, var noteikt līdz 20 miljonu eiro apmērā vai – konkrētā uzņēmuma gadījumā – līdz 4% no tā visā pasaulē gūtā apgrozījuma iepriekšējā finanšu gadā.

Kam jāpievērš uzmanība, apstrādājot lietotāju datus interneta vietnēs?

Neatbilstība datu regulai var ne tikai radīt lielus finansiālus zaudējumus, bet arī kaitēt uzņēmuma reputācijai, mazinot iespējas piesaistīt klientus un veikt uzņēmējdarbību turpmāk.

Privātuma paziņojums mājaslapā

Privātuma paziņojums ir publisks dokuments un tajā jābūt aprakstītam, kā uzņēmums piemēro datu aizsardzības principus. Saskaņā ar datu regulu privātuma paziņojumam jābūt kodolīgam, pārskatāmam un nepārprotamam, turklāt tas jā sagatavo vienkāršā valodā, lai jebkura fiziskā persona, kas apmeklē uzņēmuma mājaslapu, tiktu saprotamā veidā informēta par uzņēmuma veikto datu apstrādi.

Visticamāk, lielākā daļa uzņēmumu savās mājaslapās jau ir ieviesuši privātuma paziņojumu, pievēršot uzmanību šādiem aspektiem:

- Vai uzņēmums kopš 2018. gada ir atjaudinājis privātuma paziņojumu, lai tas atbilstu esošajai situācijai un aptvertu visus personas datus, kas ievākti ar brīdi, kad lietotājs apmeklē konkrēto mājaslapu?
- Privātuma paziņojumā jābūt norādītiem skaidriem mērķiem, kuriem uzņēmums izmanto personas datus, piemēram, mārketinga vai grāmatvedības vajadzībām;
- Privātuma paziņojumā jābūt skaidri norādītām mājaslapas lietotāju tiesībām attiecībā uz saviem personas datiem un to izmantošanu;
- Katram datu apstrādes mērķim ir nepieciešams tiesisks pamats, par kuru uzņēmums sniedz informāciju lietotājam;
- Jābūt norādītai informācijai par to, kas un kādā veidā var veikt konkrēto datu apstrādi;
- Lietotājam jābūt pilnīgi skaidrai informācijai par to, vai tā personas datus apstrādā uz

piekrišanas, likuma vai līguma pamata. Jāpievērš uzmanība tam, ka atkarībā no personas datu apstrādes mērķa tiesiskais pamats var mainīties, un šai informācijai jābūt skaidri norādītai mājaslapā.

Vai pirms datu iegūšanas uzņēmums saņem piekrišanu no mājaslapas apmeklētājiem un esošajiem klientiem?

Datu regulas mērķis ir dot klientiem/lietotājiem pilnīgu kontroli pār savu datu izmantošanu internetā, tostarp e-komercijā. Piekrišana ir viens no datu aizsardzības būtiskiem elementiem.

Piemēram, e-komercijas uzņēmumam jābūt likumīgiem risinājumiem piekrišanas iegūšanai un datu turpmākajai apstrādei uz piekrišanas pamata. Privātuma paziņojumā jāietver visa nepieciešamā informācija, kas attiecas uz klientu/lietotāju datu vākšanu, apstrādi, glabāšanu un izmantošanu. Arī veicot fizisko personu datu apstrādi veidlapās, reģistrācijas procesos, e-pastos un uznirstošajos logos (banneros), jānodrošina iespēja lietotājam sniegt vai atsaukt piekrišanu šo datu izmantošanai.

Galvenie jautājumi, kam jābūt skaidriem par personas datu apstrādi piekrišanas gadījumā:

- Vai personas datu iegūšanas tiesiskais pamats ir piekrišana vai arī pastāv cits tiesiskais pamats datu apstrādei?
- Vai kārtība, kādā iegūst datu subjekta piekrišanu, atbilst visiem ar e-komerciju saistītajiem kritērijiem un datu regulā noteiktajiem kritērijiem?
- Vai uzņēmums spēj sagatavot informāciju, piemēram, iesniegšanai uzraudzības iestādē, kas pierāda, ka datu vākšanai un apstrādei ir tiesisks pamats?
- Vai uzņēmums dokumentē visus gadījumus, kuros datus apstrādā uz fiziskās personas piekrišanas pamata?
- Vai uzņēmums ir pārskatījis savus piekrišanas iegūšanas procesus un regulāri tos pārskata/atjaunina?
- Vai ir iespējams pārtraukt datu apstrādi un izdzēst ierakstus, saņemot pieprasījumu no datu subjekta?

(nobeigums – nākamajās Īsziņās)