Datu drošība, strādājot attālināti

Aleksandra Kristiāna Priede, SIA "ZAB Kronbergs Čukste Levin", jaunākā juriste

Strādājot attālināti, nākas sastapties ar dažādām situācijām, piemēram, braucot sabiedriskajā transportā, piezvana sadarbības partneris, ar kuru jāapspriež darba jautājumi vai jānosūta steidzama ziņa "Whatsapp". Arī attālinātā sapulce var sākties tieši tajā laikā, kad vadītājs atrodas kādā sabiedriskā vietā – konferencē vai kafejnīcā. Kā šādas situācijas izskatās no datu aizsardzības un konfidencialitātes puses? Kā rīkoties, lai, strādājot attālināti, nejauši nenodotu konfidenciālu informāciju citiem?

Katrai informācijas kategorijai ir savas drošības prasības, kuras jāievēro, lai netiktu pārkāptas darba devēja, kolēģu, klientu vai pat visas sabiedrības tiesības un intereses.

Informācijas kategorijas

Informācija darba vidē tiek klasificēta, ņemot vērā tās sensitivitāti un nepieciešamību pēc aizsardzības:

- publiskā informācija;

Informācija, kas ar tiesību aktiem iekļaujama fizisko vai juridisko personu pārskatos, saistīta ar valsts pārvaldes funkciju vai uzdevumu izpildi, kā arī – normatīvajos aktos noteiktajos gadījumos – ar valsts vai pašvaldības finanšu līdzekļu vai mantas izmantošanu.

- konfidenciāla informācija;

Jebkāda informācija, kas attiecas ne vien uz komercnoslēpumu saturošu informāciju, bet uz jebkādu informāciju, kurai ar tiesību aktu vai līgumu noteikts neizpaužamas informācijas statuss, tostarp tā var būt informācija, kurai nepiemīt komerciāla vērtība.

- komercnoslēpums;

Neizpaužama saimnieciska rakstura informācija, tehnoloģiskās zināšanas un zinātniska vai cita rakstura informācija, kas nav vispārzināma vai pieejama personām, kuras parasti izmanto šāda veida informāciju; tai ir faktiska vai potenciāla komerciālā vērtība un kuras turētājs ir veicis saprātīgus pasākumus slepenības saglabāšanai.

- personas dati;

Jebkura informācija, kas attiecas uz identificētu vai identificējamu fizisku personu, tostarp vārds, uzvārds, personas kods, atrašanās vietas dati, tiešsaistes identifikatori vai informācija par personas fiziskajām, fizioloģiskajām, ģenētiskajām, psiholoģiskajām, ekonomiskajām, kultūras vai sociālajām pazīmēm.

- valsts noslēpums.

Militāra, politiska, ekonomiska, zinātniska, tehniska vai cita rakstura informācija, kuras nozaudēšana vai nelikumīga izpaušana var radīt kaitējumu valsts drošībai, ekonomiskajām vai politiskajām interesēm.

Kas teikts normatīvajos aktos?

Darbinieku pienākumus informācijas aizsardzībā regulē vairāki normatīvie akti – Darba likums (DL), Vispārīgā datu aizsardzības regula (regula 2016/679 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti), kā arī citi saistoši tiesību akti.

DL

DL 83.pantā paredzēts neizpaušanas pienākums. Šī panta 1.daļā noteikts darbinieka pienākums neizpaust – tostarp nedarīt tieši vai netieši pieejamu – no darba devēja iegūto informāciju, kas uzskatāma par komercnoslēpumu, trešajām personām. No likuma prasībām secināms, ka darbiniekam jebkurā gadījumā jāievēro tāds informācijas aizsardzības līmenis, kas neapdraud darba devēja tiesības. Šāds pienākums ir vispārēji saistošs neatkarīgi no

tā, vai darbs ar konfidenciālo informāciju tiek veikts darba devēja nodrošinātās telpās vai attālināti, tostarp publiskās vietās.

Savukārt DL 55.panta regulējums attiecas uz darba kārtības noteikumiem. Šī panta 2.daļas 5.punktā noteikts, ka darba kārtības noteikumos ir iekļaujama arī informācija par darba aizsardzības pasākumiem uzņēmumā. No tā izriet, ka darba devējam ir tiesības noteikt iekšējās vadlīnijas arī attiecībā uz komercnoslēpuma aizsardzību.

Vispārīgā datu aizsardzības regula

Darbā ar personas datiem jāievēro Vispārīgās datu aizsardzības regulas prasības. Atbilstoši šai regulai personas datiem piešķirama īpaša aizsardzības pakāpe. Par īpašas kategorijas personas datiem uzskatāmi dati, kas atklāj rasi vai etnisko piederību, politiskos uzskatus, reliģisko vai filozofisko pārliecību, dalību arodbiedrībās, kā arī ģenētiskie, biometriskie un veselības dati, dati par personas dzimumdzīvi vai seksuālo orientāciju, kā arī informācija par personas sodāmību.

Vispārīgās datu aizsardzības regulas 32.panta 1.daļā paredzēts – *ņemot vērā tehnikas līmeni, īstenošanas izmaksas un apstrādes raksturu, apmēru, kontekstu un nolūkus, kā arī dažādas iespējamības un smaguma pakāpes risku attiecībā uz fizisku personu tiesībām un brīvībām, pārzinis un apstrādātājs īsteno atbilstīgus tehniskus un organizatoriskus pasākumus, lai nodrošinātu tādu drošības līmeni, kas atbilst riskam*.

Veicot darbu attālināti, īpaši publiskās vietās, ir būtiski ievērot maksimālu drošību attiecībā uz darbībām, kas saistītas ar konfidenciālu informāciju un to saturošām ierīcēm

Papildus Vispārīgās datu aizsardzības regulas 39.apsvērumā paredzēts – *personas dati būtu jāapstrādā veidā, kas nodrošina personas datu pienācīgu drošību un konfidencialitāti, tostarp nepieļaujot neatļautu piekļuvi personas datiem vai to neatļautu izmantošanu un neatļautu piekļuvi aprīkojumam, kas izmantots apstrādei*.

Savukārt attiecībā uz personas datiem Vispārīgā datu aizsardzības regula paredz imperatīvu pienākumu neizpaust un neapstrādāt šādus datus, ja vien nav noteikts leģitīms mērķis un tiesisks pamats to apstrādei.

Citi normatīvie akti

Komercnoslēpumu aizsardzības likuma 5.panta 1.daļā paredzēts, ka *komercnoslēpuma nelikumīga iegūšana, izmantošana vai izpaušana bez komercnoslēpuma turētāja atļaujas ir tiesību pārkāpums*.

Nacionālās kiberdrošības likuma 27.pants nosaka, ka likuma subjektiem ir pienākums veikt atbilstošus un samērīgus tehniskus un organizatoriskus pasākumus, lai pārvaldītu kiberriskus izmantoto elektronisko sakaru tīklu un informācijas sistēmu drošībai, kā arī lai novērstu vai mazinātu kiberincidentu ietekmi uz pakalpojumu saņēmējiem un citiem pakalpojumiem.

Papildus jāņem vērā vēl neapstiprinātie Ministru kabineta noteikumi “Noteikumi par minimālajām kiberdrošības prasībām”, kuru 3.2.nodaļa nosaka kiberdrošības pārvaldības dokumentācijas prasības subjektiem, uz kuriem attiecas Nacionālais kiberdrošības likums. Šīs prasības ietver kiberdrošības politikas izstrādi, informācijas un komunikācijas tehnoloģiju resursu un informācijas sistēmu katalogu, kiberrisku pārvaldības un informācijas un komunikācijas tehnoloģiju darbības nepārtrauktības plānu, kā arī kiberincidentu žurnāla uzturēšanu.

Darbinieku pienākumi informācijas aizsardzībā

Kopš pandēmijas laika arvien populārāks ir attālinātais darbs jeb, atbilstoši DL regulējumam, darba izpildes veids, kad darbs, ko darbinieks varētu veikt darba devēja uzņēmumā, pastāvīgi vai regulāri tiek veikts ārpus tā, tostarp izmantojot informācijas un komunikācijas tehnoloģijas, bet nav saistīts ar regulāru pārvietošanos.

Kiberdrošības jomā viens no apdraudējumu klasifikācijas veidiem ir balstīts uz apdraudējuma avotu – tie var būt iekšējie vai ārējie draudi.

Iekšējie draudi parasti ir riski un ievainojamības, kas rodas uzņēmuma iekšienē. Tie attiecas uz personām, kurām ir piekļuve organizācijas sistēmām, tīkliem vai sensitīvai informācijai, piemēram, darbiniekiem, darbuzņēmējiem vai sadarbības partneriem.

Savukārt ārējie draudi ir riski un potenciāli apdraudējumi, kas rodas ārpus organizācijas un var ietekmēt tās sensitīvās informācijas, sistēmu vai darbības konfidencialitāti, integritāti un pieejamību. Šos draudus parasti rada ārējas struktūras – hakeri, kibernoziedznieki, konkurenti vai citi ļaunprātīgi dalībnieki –, kuri cenšas izmantot organizācijas kiberdrošības sistēmas ievainojamības.

Lai gan ziņās bieži dzirdams par kiberuzbrukumiem jeb ārējiem riskiem, lielie riski rodas arī no iekšējiem faktoriem – darbinieku nepietiekamas vērības vai drošības prasību neievērošanas.

Kas jāievēro darbiniekiem?

Darbiniekiem jāievēro šādi praktiski pasākumi, lai nodrošinātu informācijas drošību:

- aizsardzība pret trešo personu piekļuvi;

Jānovērš piekļuve darba ierīcēm nepilnvarotām personām, tostarp ģimenes locekļiem. Ierīču ekrāni jābloķē, kad tie netiek izmantoti, kā arī papildu drošībai nevajadzētu atstāt piekļuvi lietotāja kontiem izmantotajās programmās un sociālajās platformās. Strādājot publiskā vietā, jāievēro piesardzība mutiskās komunikācijas laikā – gan telefonsarunās, gan videokonferencēs –, lai nepieļautu sensitīvas informācijas nonākšanu trešo personu rīcībā.

- fizisku dokumentu apstrāde;

Fiziskie dokumenti jāglabā drošā vietā. Nedrīkst tos atstāt redzamā vietā, īpaši attālināta darba apstākļos, kur telpas var būt pieejamas arī ģimenes locekļiem.

- datu glabāšana;

Jāizvairās no sensitīvas informācijas glabāšanas neaizsargātās ierīcēs vai tīklos. Jāizmanto uzņēmuma nodrošinātas datu glabāšanas sistēmas ar piemērotu aizsardzību. Strādājot no publiskām vietām, jāizvairās no nedrošiem bezvadu tīkliem (piemēram, publiskiem Wi-Fi tīkliem bez paroles), un ieteicams izmantot mobilo ierīču interneta pieslēgumu (*hotspot*).

- drošu saziņas kanālu izmantošana un informācijas pārsūtīšana.

Jāizvairās no neoficiālām saziņas platformām, piemēram, “WhatsApp”, “Messenger”, ja vien darba devējs nav īpaši atļāvis to lietošanu darba vajadzībām. Sensitīvas informācijas pārsūtīšanai jāizmanto tikai oficiāli darba saziņas kanāli, piemēram, darba e-pasts. Nedrīkst izmantot personīgos e-pastus vai neapstiprinātas ziņapmaiņas lietotnes.

Secināms, ka, veicot darbu attālināti, īpaši publiskās vietās, ir būtiski ievērot maksimālu drošību attiecībā uz darbībām, kas saistītas ar konfidenciālu informāciju un to saturošām ierīcēm. Jāievēro gan darba devēja noteiktās drošības prasības, gan normatīvo aktu prasības, īpaši gadījumos, kad darbs ietver personas datu apstrādi.