

# PERSONĪGĀ DATORA IZMANTOŠANA DARBA VAJADZĪBĀM



## INTS SKALDIS,

ZAB "Ellex Kļaviņš", zvērināta advokāta palīgs



## MIKIJS ZĪMECS,

ZAB "Ellex Kļaviņš" jurists, sertificēts datu aizsardzības speciālists

Izmantojot personīgo datoru darba vajadzībām, piemēram, strādājot no mājām, noder zināt, vai un kādā mērā darba devējs drīkst ietekmēt datora lietošanu. Piemēram, vai darba devējs var noteikt, kādas programmas nepieciešams lejupielādēt datorā, kādām aizsardzības sistēmām jābūt utt. Kā pasargāt uzņēmumu, un kurš ir atbildīgs, lai dati būtu drošībā?

No Darba likuma (DL) izriet, ka darba devējam jāveic nepieciešamie pasākumi, kas saistīti ar darba organizāciju uzņēmumā. Darba devēja pienākums ir nodrošināt apstākļus, lai darbinieks varētu izpildīt darba līgumā noteiktos pienākumus. Piemēram, darba devējs ir atbildīgs par darba vietas, darba aprīkojuma, tostarp, ja nepieciešams, datora un programmatūras, nodrošināšanu, lai darbinieks varētu veikt darba pienākumus.

DL 28. panta 2. daļā paredzēts, ka darba devējam ir pienākums maksāt nolīgto darba samaksu un nodrošināt taisnīgus, drošus un veselībai nekaitīgus darba apstākļus. Atbilstoši DL 49. pantam darbinieka saistības izpildījuma veidu, apmēru, laiku un vietu darba līgumā nosaka darba devējs. Savukārt DL 51. panta 2. daļā paredzēts darba devēja pienākums nodrošināt tādu darba organizāciju un darba apstākļus, lai darbinieks varētu izpildīt viņam noteikto darbu.

Jānorāda, ka darba devējam nav tiesību vienpusēji pieprasīt, lai darbinieks bez vienošanās izmanto savu personīgo

datoru, un darbiniekam nav pienākuma piekrist šādai prasībai. Tāpat darbiniekam bez vienošanās ar darba devēju nav tiesību patvaļīgi darba pienākumu izpildei izmantot personīgo datoru un pēc tam pieprasīt darba devējam segt ar personīgā datora izmantošanu saistītos izdevumus vai zaudējumus.

## VIENOŠANĀS PAR DATORA LIETOŠANU

Atbilstoši Darba aizsardzības likuma (DAL) 1. panta 4. punktam darba aprīkojums ir jebkura ierīce (mašīna, mehānisms), aparāts, darbarīks vai iekārta, ko lieto darbā. Mūsdienās daudzās jomās darbu veic, izmantojot darbinieka personīgo stacionāro vai portatīvo datoru, kā arī nereti darbiniekam nepieciešams strādāt attālināti. Līdz ar to personīgais dators, ko lieto darba pienākumu izpildei, uzskatāms par darba aprīkojumu DL un DAL izpratnē.

## LIKUMS NENOSAKA UN NEAIZLIEDZ

DL nav paredzēti noteikumi, kas jāņem vērā, darbiniekam lietojot personīgo datoru darba vajadzībām. Vienlaikus DL neaizliedz darba devējam un darbiniekam savstarpēji vienoties par kārtību, kādā darbinieks lieto personīgo datoru darba pienākumu izpildei, jo tas ir pat nepieciešams. DL atbilstoši ir prakse, kad darba devējs vienojas ar darbinieku par viņa personīgā datora lietošanu darba izpildei, attiecīgi sedzot ar personīgā datora lietošanu saistītās



izmaksas, ja tādas rodas un ir nepieciešamas darba izpildei. Šāda vienošanās slēdzama rakstveidā un pievienojama darba līgumam.

DL 76. panta 1. daļas 3. punktā paredzēts darba devēja pienākums atlīdzināt darbiniekam izdevumus, kas radušies saistībā ar viņam piederoša aprīkojuma (kas atbilstoši darba līgumam tiek izmantots darba vajadzībām) nolietojanos (amortizāciju). Ja darbinieks strādā attālināti un darba izpildei izmanto personīgo datoru, darba devējam jāsedz izmaksas, kas saistītas ar tā lietošanu. Par šo izmaksu apmēru vai aprēķināšanas kārtību jāvienojas darba līgumā (ja tas slēgts par attālinātā darba veikšanu) vai ar vienošanos, kurā darbinieks un darba devējs nosaka personīgā datora izmantošanu darba vajadzībām.

### VIENOŠANĀS SATURS PAŠU ZIŅĀ

DL nav regulēts vienošanās par darbinieka personīgā datora vai cita aprīkojuma lietošanu saturs. Tomēr, ja darbinieks darba veikšanai lieto personīgo datoru, vienošanās tekstā jāneregulē visi būtiskākie jautājumi, tostarp kārtība, kādā personīgo datoru izmanto darba pienākumu izpildei, kā tiek nodrošināta nepieciešamā programmatūra (vai attiecīgās licences sagādā darba devējs vai darbinieks) un piekļuve darba devēja informācijai, programmatūru izmantošanas kārtība un ierobežojumi darba vajadzībām izmantot noteiktu programmatūru, kā arī datu aizsardzības un konfidencialitātes prasības un noteikumi par izdevumu segšanu.

Tāpat jāvienojas par amortizācijas izdevumu segšanu un izmaksām, kas saistītas ar nepieciešamās programmatūras vai piekļuvju nodrošināšanu. Ja darbinieks strādā attālināti, jāvienojas arī par interneta un ar elektroenerģijas patēriņu saistīto izdevumu segšanas kārtību u.c. izdevumiem, kas varētu rasties.

Lai novērstu iespējamus strīdus, darba devējam un darbiniekam būtiski vispirms izvērtēt, kādi izdevumi varētu rasties saistībā ar personīgā datora

lietošanu, tostarp veicot darbu attālināti, un vienoties, kā tos atlīdzina. Darba devējam jāņem vērā, ka darbinieka izdevumi, kas nepieciešami darba veikšanai, jebkurā gadījumā ir jāatlīdzina. Fakts, ka šādi izdevumi nav neregulēti darba līgumā vai ar atsevišķu vienošanos, neatbrīvo darba devēju no pienākuma tos segt atbilstoši DL 76. pantam. Vienlaikus jānorāda, ka DL plānoti grozījumi, kas ļautu darbiniekam un darba devējam vienoties arī par citādu kārtību, kādā attālinātā darba gadījumā kompensēt darbiniekam radušos izdevumus.

### ZAUDĒJUMU ATLĪDZINĀŠANA

DL 77. pantā paredzēts darba devēja pienākums atlīdzināt darbiniekam zaudējumus, kuri, veicot darbu, radušies saistībā ar viņam piederoša darba aprīkojuma bojājumu vai bojāeju un par kuriem darbinieks nav vainojams, ja viņam piederošā darba aprīkojuma izmantošana ir nolīgta.

Katrā gadījumā darba devējam ir no likuma izrietošs pienākums segt zaudējumus, kas rodas darbiniekam. Piemēram, ja, veicot darbu, bojāts dators, darba devējam būtu jāsedz darbiniekam radušies zaudējumi, ja vien darbinieks pats nav vainojams to nodarīšanā. Būtiski ņemt vērā, ka darba devējam ir pienākums segt tikai zaudējumus, kas radušies, veicot darbu. Tāpēc, ja darbinieks sniedz informāciju par zaudējumiem, darba devējam vispirms jāpārlicinās, vai tie radušies, darbiniekam strādājot. Savukārt, ja darbinieks zaudējumu nodarīšanas laikā personīgo datoru lietojis privātām vajadzībām, darba devējam šādi zaudējumi nav jāatlīdzina. Tāpat darba devējam nerodas atbildība, ja darbinieks lieto personīgo datoru vai programmas darba veikšanai pēc saviem ieskatiem, nevienojoties par to ar darba devēju vai pārkāpjot darba devēja instrukcijas un norādījumus par darba veikšanu.

Savukārt DL 87. panta 1. daļā paredzēts, ka darbinieks pilnībā vai daļēji atbrīvojams no civiltiesiskās atbildības par darba devējam nodarītajiem zaudējumiem, ja arī darba devējs pats, t.i., ar

*Ja, veicot darbu, bojāts dators, darba devējam būtu jāsedz darbiniekam radušies zaudējumi, ja vien darbinieks pats nav vainojams to nodarīšanā.*

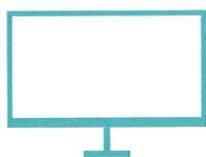
1 429 000

vidējais interneta lietotāju skaits mēnesī no visām platformām kopā,  
no kuriemSalīdzinot ar  
2018. gadu,  
vidējais lietotāju skaits  
palielinājies par

↑ 8000

Vidējais interneta lietotāju skaits mēnesī

1 234 000



1 045 000



125 000



Avots: Gemius.lv

saviem rīkojumiem vai nenodrošinot pienācīgus darba apstākļus vai darba aprīkojumu, bijis vainīgs zaudējumu nodarīšanā.

Piemēram, ja attālinātā darba gadījumā darba devējs ar darbinieku nav vienojies par personīgā datora lietošanu, līcis darbiniekam izmantot personīgo datoru darbam, nav nodrošinājis nepieciešamo programmatūru vai nav veicis pienācīgus darba aizsardzības pasākumus, tad, ja šādas rīcības rezultātā darba devējam nodarīti zaudējumi, ir pamats vērtēt arī paša darba devēja atbildības apmēru.

## DARBA AIZSARDZĪBA

Šobrīd normatīvajos aktos nav sniegta attālinātā darba definīcija. Ar grozījumiem DAL, kas stāsies spēkā 2020. gada 1. jūlijā, paredzēts, ka par attālināto darbu uzskatīs darba izpildes veidu, kad darbs, kuru varētu veikt darba devēja uzņēmuma ietvaros, pastāvīgi vai regulāri tiek veikts ārpus uzņēmuma, tostarp darbs, ko veic, izmantojot informācijas un komunikācijas tehnoloģijas. Ja darbu veic attālināti un darbinieks izmanto personīgo datoru darbam no mājām, darba devējam jānodrošina viņam piemēroti darba apstākļi un jāveic atbilstoši darba aizsardzības pasākumi. Tas

nenozīmē, ka darba devējam jāveic pilnīga darba vietas iekārtošana attālinātā darba veikšanai, bet gan jāpārlicinās, ka darba vieta atbilst darba aizsardzības prasībām. Darbiniekam strādājot ar personīgo datoru un veicot darbu attālināti dažādās vietās, darba devējam atbilstoši grozījumiem DAL būtu jāveic darba vides riska novērtēšana tikai par konkrēto darba veidu. Ja darbinieks un darba devējs vienojas, ka darbinieks attālināto darbu veic pastāvīgi vienā vietā, darba vides riska novērtēšana jāveic par konkrēto darba vietu. Šāda darba vides risku novērtēšana jāveic pirms attālinātā darba uzsākšanas.

Darba vides risku novērtēšanā var tikt iesaistīts pats darbinieks vai viņa pārstāvis, kas pārzina darba vietu, kurā darbiniekam paredzēts strādāt. Darbiniekam ir pienākums sadarboties ar darba devēju darba vides riska novērtēšanā un sniegt viņam pilnīgu informāciju par attālinātā darba veikšanas vietas apstākļiem, kas var ietekmēt viņa drošību un veselību. Tas nepieciešams, lai darba devējs pirms attālinātā darba veikšanas varētu plānot īstenojamos darba aizsardzības pasākumus, piemēram, ergonomikas principu ievērošanu, tīrību darba vietā, izmantojamā darba aprīkojuma pārbaudi un uzturēšanu atbilstošā tehniskā kārtībā u.c.



Ja darbinieks iepriekš nav veicis darbu attālināti, pirms tā uzsākšanas darba devējam jānodrošina viņam neplānotā instruktāža darba aizsardzības jautājumos atbilstoši Ministru kabineta (MK) noteikumu Nr. 749 "Apmācības kārtība darba aizsardzības jautājumos" 8. un 24. punktam, jo darbiniekam mainās darba apstākļi, darba vieta un darba aprīkojums.

Tāpat būtiski atcerēties, ka visos gadījumos, kad darbinieks veic darbu ar datoru, darba devējam ir pienākums garantēt darba aizsardzības prasības un īstenot pasākumus, kas noteikti MK noteikumos Nr. 343 "Darba aizsardzības prasības, strādājot ar displeju", nodrošinot, ka darbinieka darba vieta ir atbilstoši iekārtota un aprīkota un darbinieks, veicot darbu attālināti, ievēro prasības, lai neradītu riskus savai veselībai.

Ja darba devējs veicis darba vides risku izvērtējumu, nodrošinājis atbilstošus darba apstākļus, kā arī veicis darbinieka instruktažu par attālināta darba veikšanu un darba aizsardzības prasībām, strādājot ar displeju, turpmāka darba aizsardzības prasību ievērošana ir darbinieka pienākums. Savukārt darba devējam ir pienākums kontrolēt, vai prasības tiek ievērotas un vai, mainoties apstākļiem, nav nepieciešams īstenot papildu darba aizsardzības pasākumus.

## DATU AIZSARDZĪBA

Organizējot attālināto darbu, darba devējam jāņem vērā arī savu klientu un darbinieku personas datu aizsardzības pienākumi. Arī Latvijas Datu valsts inspekcija nesēn atgādināja par veicamajiem pasākumiem šajā jomā. Īpaša uzmanība darba devējiem jāvelta darbiniekiem, kam, arī strādājot attālināti, darba pienākumi paredz fizisko personu datu apstrādi.

Eiropas Parlamenta un Padomes regulas 2016/679 jeb Vispārīgās datu aizsardzības regulas (Regula) 32. pantā paredzēts, ka gan datu pārzinim, gan datu apstrādātājam jāīsteno atbilstīgi tehniski un organizatoriski pasākumi, lai nodrošinātu datu apstrādes drošības līmeni, kas atbilst datu apstrādes riskam. Tātad, ļaujot darbiniekiem izmantot personīgās ierīces (aprīkojumu) personu

datu apstrādei, darba devējs uzņemas atbildību par darbinieku ierīču un tādējādi arī datu apstrādes drošību. Tas nozīmē, ka, paredzot attālināto darbu, tieši darba devēja pienākums ir nodrošināt darbiniekam visu nepieciešamo programmatūru un ieviest citus risinājumus, lai novērstu iespējamu datu noplūdi vai citus personas datu aizsardzības pārkāpumus.

Darba devējam, izvēloties attālinātā darba risinājumus, jāsaprot, ka darbinieks, izmantojot personīgās ierīces, tostarp personīgos datorus, ievēro sliktāku kiberhigiēnu, nekā strādājot ar darba datoriem, tādējādi visa darbiniekam pieejamā darba devēja informāciju pakļauta lielākam riskam. Ir zināms, ka pārsvarā cilvēki, izmantojot personiskās ierīces, mazāk nopietni ievēro nepieciešamību laikus atjaunināt izmantoto programmatūru, neizmanto antivīrusu programmatūru un datu šifrēšanu, kā arī nereti ierīcēs lejupielādē multimediju failus vai nelicenzētu programmatūru no dažādiem avotiem, kas trešajām pusēm rada iespējas nelikumīgi piekļūt darbinieka ierīcē esošajai informācijai. Turklāt, strādājot attālināti, darbinieki vairāk pakļauti pikšķerēšanas (*phishing*) uzbrukumiem, kas jāņem vērā, veidojot piekļuvi uzņēmuma informācijai. Saskaņā ar vairākiem pētījumiem tieši attālinātā darba darbinieki uzskatāmi par drošības sistēmas vājāko posmu, jo var sniegt piekļuvi uzņēmuma datiem, fiziski esot ārpus uzņēmuma telpām.

Tāpēc darba devējam, īstenojot attālinātā darba risinājumus, jāizvēlas tehniski un organizatoriski pasākumi, ņemot vērā arī darbinieku paradumus personīgo ierīču izmantošanā. Noteikti jāveic atkārtota darbinieku izglītošana par informācijas sistēmu drošību un iespējamiem uzbrukumiem, ar ko darbinieki var saskarties, strādājot no mājām. Pretēji pieņemtajam tas ir ļoti būtisks solis drošības garantēšanai, jo saskaņā ar kiberdrošības kompānijas "Kaspersky" datiem gandrīz 90% gadījumu drošības pārkāpumus (piemēram, datu noplūdēs) vainojama cilvēka darbība vai kļūda.

Paralēli darbinieku izglītošanai par drošības jautājumiem nepieciešams ieviest atbilstošas sistēmas, kas ļauj darbiniekiem droši veikt personas datu u.c. konfidencialas informācijas apstrādi. Izvēloties

šādu sistēmu, vēlams nodrošināt, ka darbiniekam nav nepieciešams izmantot savu personīgo e-pastu, kā arī nav jāglabā uzņēmuma informācija, tostarp personas dati, savā personīgajā ierīcē, t.i., darbinieks darba uzdevumus veic noteiktā programmatūras platformā, kas nesaglabā informāciju darbinieka personīgajā ierīcē, bet gan darba devēja serverī (vai, piemēram, mākoņrisinājuma pakalpojuma platformā).

Viens no vienkāršākajiem risinājumiem, ko darba devējs var ieviest, ir iespēja darbiniekam piekļūt darba datoram, izmantojot personīgo datoru un pieslēdzoties tam ar attālinātās darbvirsmas programmatūru. Tādējādi visu informācijas apstrādi veic ar darba datoru, nevis darbinieka personīgo datoru, samazinot galvassāpes darba devējam, mēģinot nodrošināt darbinieka ierīču drošību (tas gan nesamazina nepieciešamību apmācīt darbinieku ievērot kiberhigiēnu, izmantojot personīgās ierīces).

## PIEKĻUVE UZŅĒMUMA INFORMĀCIJAI


Visbeidzot, darba devējam jāspēj garantēt droša piekļuve uzņēmuma informācijai / personas datiem vai programmatūru platformām, kur darbiniekam jāveic savi darba uzdevumi. Lai samazinātu riskus, kas var rasties, darbiniekam izmantojot nedrošu interneta pieslēgumu, piemēram, datu pārtveršana, pieslēgšanās darba devēja sistēmām būtu jāveic, izmantojot virtuālo privāto tīklu risinājumus.

Papildus, lai darba devējs nodrošinātu savu datu drošību pret veiksmīgās pikšķerēšanas kampaņām, vēlams aktivizēt vai ieviest divu faktoru autentifikāciju sistēmām un datubāzēm, kas darbiniekiem jāizmanto darba uzdevumu veikšanai. Dažādos pētījumos un uzņēmumu praksē secināts, ka divu faktoru autentifikācijas sistēmu ieviešana, izmantojot fizisku autentifikācijas atslēgu, gandrīz līdz nullei samazina iespēju darbiniekiem kļūt par veiksmīgas pikšķerēšanas upuriem.

Tātad darba devējam, lai izpildītu savus pienākumus saistībā ar fizisko personu

datu aizsardzību, kā arī citas konfidencialas informācijas aizsardzību, jāievieš atbilstoši tehniski un organizatoriski līdzekļi, kas samazina datu pārkāpumu rašanās riskus, tostarp iespējams paredzēt darbinieku izglītošanu informācijas drošības un iespējamo risku jautājumos, tehnoloģisko risinājumu ieviešanu, kas darbiniekam samazina nepieciešamību savā personīgajā ierīcē apstrādāt personas datus u.c. informāciju, kā arī nodrošināt iespēju darbiniekam droši pieslēgties nepieciešamajām sistēmām un aizsargāt tās ar papildu atslēgu, ieviešot divu faktoru autentifikācijas metodi.

Papildus jāņem vērā arī datu aizsardzības pienākumi, kas attiecināmi uz darbinieku, kurš veic attālināto darbu. Ja darbinieks darba veikšanai izmanto personīgās ierīces, vēlams izvērtēt nepieciešamību lietot dažāda veida automātiskās uzraudzības vai laika uzskaites programmas, kas var pārmērīgi aizskart darbinieka tiesības uz privātumu. Ja izvērtējot secināts, ka darba devēja leģitīmās intereses veikt šādu uzraudzību ir pārākas pār darbinieka tiesībām uz privātumu, attālinātajai uzraudzībai jābūt proporcionālai tās mērķim. Darba devējam precīzi jādefinē šādas apstrādes mērķis un jānosaka minimālā informācija, kas nepieciešama, lai sasniegtu šo mērķi.

Lai samazinātu ietekmi uz darbinieka privātumu, šāda uzraudzība var tikt piemērota tikai darba vajadzībām nepieciešamajām programmām vai platformām un tikai darba laikā ar iespēju darbiniekam brīvajos brīžos šo programmu atslēgt vai ieviešot līdzvērtīgus risinājumus atbilstoši uzņēmuma vajadzībām un iespējām. Tāpat jāatceras, ka Regulā kā viens no datu apstrādes principiem noteikts pārredzamības princips, kas paredz, ka datu subjektiem (šajā gadījumā – darbiniekiem) jābūt informētiem par savu datu apstrādi. Tas nozīmē, ka attālinātās uzraudzības vai laika uzskaites programmatūras izmantošana nedrīkst būt slepena. Darbinieki jāinformē par šādām datu apstrādes darbībām, to mērķiem, apstrādātajiem datiem, kā arī darbinieku tiesībām saistībā ar datu apstrādi. 



*Lai samazinātu riskus, kas var rasties, darbiniekam izmantojot nedrošu interneta pieslēgumu, piemēram, datu pārtveršana, pieslēgšanās darba devēja sistēmām būtu jāveic, izmantojot virtuālo privāto tīklu risinājumus.*