2020 m. kovo 21 d.

Nuotolinis darbas ir asmens duomenų apsauga: nauji iššūkiai

Karantino metu darbdaviai yra skatinami sudaryti tinkamas sąlygas darbuotojams dirbti nuotoliniu būdu. Tačiau nuotolinis darbas, be kitų, lemia ir šiuos iššūkius darbdaviams:

- darbuotojų asmens duomenų saugumo užtikrinimas;
- darbdavio konfidencialios informacijos apsauga.

Žemiau dalinamės įžvalgomis, į ką darbdavys turėtų atkreipti dėmesį organizuodamas darbą nuotoliniu būdu.

1 Kaip teisiškai reglamentuoti nuotolinį darbą?

Darbdavys turėtų priimti ir tinkamai darbuotojus supažindinti su šiais vidiniais dokumentais:

- **nuotolinio darbo taisyklės**, reglamentuojančios nuotolinio darbo organizavimo ypatumus, ir
- **įmonės komunikacinių ir technologinių priemonių naudojimo taisyklės**, kuriose būtų išsamiai reglamentuota, kaip, kada ir kokia forma darbuotojas privalo naudotis darbdavio suteiktomis darbo priemonėmis, įskaitant, kokius veiksmus darbuotojas su darbo priemonėmis turi teisę atlikti ir kas yra draudžiama.

2 Kaip užtikrinti duomenų saugumą?

Nuotolinė darbo aplinka ir prieiga prie darbdavio suteikiamos infrastruktūros nėra tokios saugios, kokios galėtų būti darbuotojui fiziškai dirbant darbdavio patalpose. Darbuotojai, dirbantys nuotoliniu būdu, nebūtinai įgyvendins ir laikysis iš jų reikalaujamų saugumo priemonių. Kitaip tariant, neužtikrinus tinkamų techninių saugumo priemonių, kurios, be kita ko, proporcingai ribotų rizikingus darbuotojo veiksmus, neleistino prisijungimo pavojaus rizika didėja. Dėl to gali būti prarasta, sunaikinta ar neteisėtai atskleista darbdavio turima informacija, įskaitant darbuotojų, klientų, partnerių ar kiti darbdavio žinioje esantys fizinių asmenų duomenys.

Siekiant suvaldyti galimą riziką, be tinkamų techninių saugumo priemonių įvedimo, darbdavys turi teisę taikyti **informacinių ir komunikacinių darbo priemonių kontrolę ir stebėseną**. Kitaip tariant, laikydamasis proporcingumo, tikslingumo ir skaidrumo (darbuotojo išankstinio informavimo) principų, darbdavys gali taikyti proporcingą ir būtiną elektroninių ryšių (interneto naršymo, el. pašto, telefono ir kt.) stebėseną ir kontrolę, pavyzdžiui, sekti el. pašto komunikaciją, interneto naršymo istoriją, programos ar įrenginio stebėjimą nematomų programų (debesijos) pagalba, registruoti prieigas prie darbdavio konkrečių sistemų ir kita.

Be kita ko, darbdaviai taip pat turėtų nepamiršti su darbuotoju **pasirašyti susitarimus dėl konfidencialios informacijos apsaugos**, numatančius, kas yra konfidenciali informacija, kokie veiksmai su konfidencialia informacija yra draudžiami ir kita. Susitarime dėl konfidencialios informacijos apsaugos taip pat turėtų būti įtvirtintos nuostatos dėl darbuotojo atsakomybės konfidencialumo išlygos pažeidimo atveju.

3 Ar darbdavys turi teisę stebėti darbuotojo veiksmus, komunikaciją asmeniniame kompiuteryje dirbant iš namų?

Darbdaviui neturint galimybės suteikti darbinio kompiuterio arba darbdaviui leidžiant darbuotojui dirbti su savo asmeniniu kompiuteriu gali kilti didesni pavojai darbdavio teisių ir interesų pažeidimui.

Tokiu atveju, identifikacinių duomenų (pvz., kompiuterio unikalaus identifikatoriaus adresas) ar duomenų srauto stebėsena galėtų būti laikoma teisėta darbdavio interesų apsauga, su sąlyga jog:

- darbdavys yra iš anksto apie tai raštu informavęs darbuotoją ir yra priimtos taisyklės, išsamiai reglamentuojančias informacinių ir komunikacinių technologijų naudojimo bei darbuotojų stebėsenos ir kontrolės tvarką;
- yra įdiegtos ir taikomos tinkamos priemonės, kuriomis atskiriamas kompiuterio naudojimas asmeniniais tikslais nuo su darbu susijusių tikslų;
- atliekant stebėseną nėra renkami ar kitaip tvarkomi asmens duomenys, susiję su darbuotojo privačiu ir šeimos gyvenimu.

Jeigu darbdavys negali užtikrinti aukščiau nurodytų sąlygų egzistavimo, atliekama darbuotojo asmeninio kompiuterio stebėsena ir kontrolė būtų laikoma neteisėta, todėl negalima.

4 Kokių techninių priemonių reikėtų imtis, norint užtikrinti saugumą?

Darbdavys turi imtis techninių ir organizacinių saugumo priemonių, kurių esminės išvardytos toliau.

- **Ryšio saugumas**. Rekomenduojama darbo priemonėse įdiegti ir naudoti tik atnaujintas („*up to date*“) antivirusines programas, naudoti tik saugų, patikimą ir apsaugotą slaptažodžiu Wi-Fi tinklą, o prie elektroninio pašto jungtis tik virtualaus privataus tinklo (VPN) pagalba.

- **Vidinė komunikacija**. Rekomenduojama vidinei komunikacijai tarp darbuotojų naudoti tik patikimas, saugias programas, kuriose, be kita ko, komunikacija yra šifruojama, taip pat siūlytina riboti prieigą prie nepageidaujamų, nesaugių internetinių svetainių, programų ar informacijos.

- **Jungimasis prie bazių.** Jeigu yra naudojamasi programomis, informacinėmis sistemomis, duomenų bazėmis prie kurių vartotojui reikia prisijungti, suvedant prisijungimo duomenis, po kiekvienos baigtos sesijos rekomenduojama iš karto atsijungti bei numatyti automatinį atsijungimą po tam tikro laiko tarpo, kuriuo nesinaudojama atitinkama sistema.

- **Asmeninių įrenginių apsauga.** Tuo atveju, jeigu darbuotojas su darbdavio sutikimu darbui naudoja savo asmeninį kompiuterį ar mobilųjį telefoną, darbdavys turėtų pasirūpinti, kad darbuotojui asmenine teise priklausanti priemonė būtų prijungta prie vidinių darbdavio tinklų, sistemų, išteklių bei joje būtų sukonfigūruotos visos būtinos saugumo priemonės, atitinkančios darbdavio suteikiamų priemonių saugumo lygį.

- **Darbuotojų švietimas.** Darbuotojui naudojantis asmeniniu kompiuteriu ar kita priemone, darbdavys turėtų laikytis proporcingumo principo ir užtikrinti, kad nebūtų pažeistos darbuotojo teisės į asmens duomenų apsaugą bei privatumą. Tam, kad nuotolinio darbo keliami pavojai būtų suvaldyti ir būtų išvengta žmogiškųjų klaidų, darbuotojas taip pat turėtų būti nuolatos mokomas / jam primenama apie įprastą darbdavio informacinių ir komunikacinių technologijų naudojimo tvarką, galimas kibernetines rizikas, tokias kaip, pavyzdžiui, kenkėjiškus laiškus.

- **Saugumo priemonių ir rizikos vertinimas.** Darbdavys turėtų reguliariai atlikti informacinių technologijų saugumo priemonių tikrinimus, pavyzdžiui, įdiegti reikalingus atnaujinimus,

jeigu reikia – pakeisti prieigos teises, nustatyti ir dokumentuoti galimas rizikas, peržiūrėti darbdavio priimtas vidines nuotolinio darbo, darbo priemonių naudojimo taisykles ir jas atnaujinti. Vertinant turimas organizacines ir technines saugumo priemones darbdavys visuomet taip pat turi vadovautis Valstybinės duomenų apsaugos inspekcijos paskelbtomis Tvarkomų asmens duomenų saugumo priemonių ir rizikos įvertinimo gairėmis.

5	Ar taikoma darbdavio pareiga apsaugoti darbuotojo, kaip duomenų subjekto, teises?

Darbuotojams dirbant nuotoliniu būdu, darbuotojai, kaip duomenų subjektai, nepraranda savo teisių. Todėl darbdavys (lygiai taip pat kaip ir darbuotojo darbo „darbo vietoje“ atveju) turėtų turėti visus būtinus vidinius duomenų apsaugos dokumentus, susijusius su darbuotojų duomenų apsauga – darbuotojų asmens duomenų tvarkymo taisykles, darbuotojų teisių įgyvendinimo taisykles, jeigu reikia – informacinių ir komunikacinių technologijų naudojimo bei darbuotojų stebėsenos ir kontrolės darbo priemonėse taisykles ir kita.

Darbuotojui pateikus prašymą pasinaudoti savo, kaip duomenų subjekto, teisėmis, darbdavys turi pareigą įgyvendinti pasirinktą darbuotojo teisę, nebent, vadovaujantis teisės aktais, būtų pagrįstų priežasčių netenkinti tokio darbuotojo prašymo.

6	Kaip apsisaugoti nuo galimų kibernetinių atakų ar kitų kenkėjiškų ir neteisėtų veiksmų?

Viena dažniausiai pasitaikančių kibernetinių atakų ir kartu sukčiavimo formų internete yra duomenų vagystės. Šios paprastai lengvai įvykdamos, vartotojui siunčiant kenkėjiškus elektroninius laiškus (pavyzdžiui, apsimetant darbdaviu, kolega, institucija ir pan.) ar / ir nuorodas į suklastotus (netikrus) interneto tinklalapius. Suklaidintam asmeniui paspaudus ant elektroninio laiško ar / ir internetinės nuorodos, yra išgaunami asmens prisijungimo duomenys, slaptažodžiai ar kita konfidenciali informacija.

Rekomenduojama neatidaryti neaiškių elektroninių laiškų, gautų iš nelauktų ar įtartinų adresatų, bei nespausti jokių internetinių adresų (nuorodų), nurodytų šiuose laiškuose. Tokia rekomendacija turi būti iškomunikuota visiems darbuotojams. Jeigu kyla įtarimas, dėl gauto elektroninės žinutės turinio, jos adresato, nuorodų pateikiamų žinutėje, reikėtų:

- nauju laišku susisiekti su el. laiško siuntėju;
- patikrinti internetinio puslapio adresą (URL), ar jis nėra gramatiškai neteisingai sudarytas (galbūt minimaliai skiriasi nuo Jums žinomo adreso);
- jeigu jau paspaudėte ant nuorodos el. laiške, atkreipti dėmesį, ar nesate nukreipiami į kitą interneto tinklalapį su identišku ar panašiu Jums pažįstamo tinklalapio dizainu (pvz., banko internetinio tinklalapio falsifikatą);
- neįvedinėti ar kitaip nepateikti jokių savo prisijungimo duomenų ar kitos konfidencialios informacijos.

Esame pasiruošusios Jums padėti:

Guoda Šileikytė
Asocijuotoji teisininkė
M +370 620 636 76
E guoda.sileikyte@walless.com

Laura Ziferman
Partnerė | Advokatė
M +370 640 410 36
E laura.ziferman@walless.com