Pirmoje šio straipsnio dalyje aptarėme technologines problemas, su kuriomis gali susidurti įmonės, leidžiančios darbui naudoti asmeninius įrenginius. Šioje dalyje vertiname teisinius to paties klausimo aspektus.

Darbo funkcijų atlikimas su asmeniniais įrenginiais, ypač telefonais, yra beveik neatsiejama šiuolaikinės darbo kultūros dalis. Visgi, kaip galima buvo įsitikinti jau pirmoje šio straipsnio dalyje, toks darbo būdas turi ir keletą rimtų teisinių iššūkių: pirma, tam tikrais atvejais darbdavys rizikuoja pažeisti darbuotojo privatų gyvenimą, antra, įmonė rizikuoja pažeisti konfidencialumo įsipareigojimus duotus savo partneriams ir trečia, asmeninių prietaisų naudojimas nuotoliniam darbui gali sukelti rimtų BDAR problemų dėl duomenų teikimo už ES ribų.

Riba tarp privataus ir darbinio gyvenimo „išsitrina“

Pagrindinis darbo su asmeniniais prietaisais trūkumas – rizika pažeisti žmogaus privatumą. Naudojantis tais pačias prietaisais ir darbo, ir laisvalaikio tikslais, kontaktai, nuotraukos ir kita informacija susimaišo ir tokiu būdu riba tarp privataus gyvenimo ir darbo tarsi „išsitrina“.

Praktikoje dažnai pasitaiko situacijos, kai darbdavys įtaria, jog darbuotojas pažeidė įmonės vidines tvarkas, bet visi įrodymai yra būtent asmeniniame telefone. Darbdavio galimybės paimti tokį įrenginį ir jame esančius įrodymus vidiniam tyrimui yra labai ribotos. Nebent įmonė iš karto kreiptųsi į policiją ir prašytų pradėti ikiteisminį tyrimą. Bet ir tai negarantuoja sėkmės. Kaip pagrindinį argumentą neperduoti darbdaviui savo telefono, įtariami darbuotojai dažniausiai naudoja savo teisę į privatumą. Ir beveik visada „laimi“ ir darbdaviui tenka atsitraukti.

Pažymėtina, kad Lietuvoje per pastaruosius kelis metus yra buvę incidentų (ypač IT paslaugų bendrovėse), kai darbuotojai tyčia pavogė ir konkurentams perdavė įmonės duomenis ar programinį kodą. Tam, kaip taisyklė panaudodamas asmeninius kompiuterius.

Ši problema dažnai yra nevertinama kaip rimta iki tol, kol nutinka incidentas ir iškyla poreikis paimti įrodymus iš asmeninio įrenginio. Deja, įvykus pažeidimui paprastai jau būna per vėlu ką nors keisti. Jeigu įmonėje nebuvo tinkamai sureguliuota asmeninių prietaisų naudojimo tvarka, belieka tik apgailestauti ir geriau pasirengti ateičiai.

Konfidencialumo pažeidimai

Dar vienas dalykas apie kurį darbdaviams reikėtų pagalvoti yra konfidencialumas. Didžioji dalis sutarčių su paslaugų teikėjais ir partneriais turi konfidencialumo nuostatas, pagal kurias abi šalys paprastai įsipareigoja visą su sutarties sudarymu ir vykdymu susijusią informaciją laikyti paslaptyje ir saugoti nuo neteisėtos prieigos ar atskleidimo trečiosioms šalims. Mažai kas pagalvoja, kad šio įsipareigojimo yra praktiškai neįmanoma įvykdyti, jei leidžiama darbuotojams be jokių papildomų saugumo priemonių naudotis asmeniniais prietaisais darbo tikslais.

Dėl įrenginiuose įdiegtų automatinių informacijos bendrinimo nustatymų konfidencialumo įsipareigojimų pažeidimas praktiškai garantuotas.

Kai dirbama ne ES šalyje, vyksta duomenų teikimas į trečiąsias šalis

Duomenų teikimas į trečiąsias šalis taip pat paminėtinas prie teisinių problemų, kurias gali sukelti nuotolinis darbas, jeigu jam naudojami asmeniniai komunikacijos prietaisai.

Kai dirbama nuotoliniu būdu būnant ne ES šalyse, tokiu atveju, formaliai žiūrint, vyksta duomenų teikimas į trečiąsias šalis. Tai sukelia dar vieną teisinę problemą, nes duomenų teikimas (ypač po Schrems II sprendimo) į nemažą dalį pasaulio valstybių tapo itin rizikingas. Ypač suklusti turėtų tie, kas keliauja į autoritarinio režimo šalis, duomenų teikimas į jas yra, galima sakyti, draudžiamas.

Jeigu įmonėje atsirado darbuotojas, ketinantis dirbti trečiojoje šalyje, darbdavys turėtų imtis papildomų priemonių užtikrinti, kad duomenų teikimas atitiktų BDAR.

Kaip rasti balansą?

Pagrindiniai uždaviniai, kuriuos turi išspręsti darbdavys, svarstantis, ar leisti naudoti asmeninius prietaisus darbui, yra šie: užtikrinti balansą tarp, iš vienos pusės informacijos saugumo, konfidencialumo įsipareigojimų vykdymo ir, iš kitos pusės, darbuotojo teisės į privatų gyvenimą.

Iš pirmo žvilgsnio atrodo sunkiai suderinami dalykai, tokie kaip patogumas, saugumas ir privatumas, visgi yra derinami. Tam paprastai pasitelkiama BYOD (angl. Bring your own device) politika.

Tokio vidinio dokumento esmė – aiškiai apibrėžti darbdavio lūkesčius, informuoti apie grėsmes ir darbuotojo atsakomybę. Taip pat nustatyti darbdavio įsipareigojimus, skirti papildomai lėšų saugumo priemonių instaliavimui, mokymams, įmonės konfidencialios informacijos apsaugai bei kompensacijoms už ryšį.

Galima nustatyti ir įpareigojimą atriboti privačią informaciją nuo darbinės, laiku atnaujinti operacinę sistemą, informuoti apie prarastą įrenginį, leisti darbdaviui patikrinti, ar teisingai laikomasi saugumo reikalavimų, bei susitarti, kokiomis sąlygomis bus patikrinama įrenginyje esanti darbdavio informacija.

Rengiant šią politiką pravartu atsižvelgti į Lietuvos Nacionalinio kibernetinio saugumo centro rekomendacijas.

„Jeigu Jūsų įmonės darbuotojai turi galimybę dirbti nuotoliniu būdu ir tam naudoja savo asmeninius kompiuterius, apsvarstykite galimybę įsigyti verslo naudojamos antivirusinės programos kopiją arba reikalaukite, kad darbuotojai įdiegtų saugią antivirusinę programą į asmeninius prietaisus. Rekomenduojama riboti darbuotojų prieigą prie socialinių tinklų ir asmeninių el. pašto dėžučių, jei to nereikia darbo funkcijoms atlikti. Taip mažinama rizika, kad Jūsų įmonės darbuotojas susidurs su sukčiavimu ir galimai apkrės įmonės kompiuterį ir tinklą“, – skelbia NKSC.

Pabaigai reikia akcentuoti, kad joks dokumentas neužkardys visų grėsmių. Tačiau derinant tai kartu su atitinkamomis techninėmis saugumo priemonėmis, BYOD politikos aprašas gali įnešti aiškumo, disciplinos ir pagelbėti tada, kai prireikia laviruoti tarp darbuotojo teisės į privatumą ir darbdaviui priklausančios informacijos apsaugos.

Advokatų kontoros COBALT vyresnioji teisininkė Renata Vasiliauskienė