M&A | MOTIEKA AUDZEVIČIUS

#COVID-19

ASMENS DUOMENŲ APSAUGA

Valstybinė duomenų apsaugos inspekcija pabrėžia, kad net ir esant paskelbtai pandemijai bei karantinui, asmens duomenų apsaugos negalima pamiršti, ir pateikia bendras rekomendacijas darbdaviams ir kitiems duomenų valdytojams. Viešojoje erdvėje taip pat abejojama, ar (bei kiek) duomenų valdytojams ir tvarkytojams vėliau bus leidžiama savo veiksmus pateisinti susiklosčiusia situacija (nors, pvz., JK tarnyba (ICO) jau paskelbė, kad tam tikrų terminų nesilaikymas galėtų būti pateisinamas, žr. čia).

Atkreipiame dėmesį į pagrindinius duomenų tvarkymo aspektus šiuo laikotarpiu:

- tam tikrų asmens duomenų tvarkymas, susijęs su esama situacija dėl COVID-19, yra suderinamas su Bendruoju duomenų apsaugos reglamentu (BDAR). Tiksliau, būtų galima saugoti ir tvarkyti vidinius duomenų rinkinius apie darbuotojus, įtraukiant tokią informaciją: (i) ar asmuo buvo išvykęs į rizikos valstybę; (ii) ar asmuo kontaktavo su asmeniu, išvykusiu į rizikos valstybę ar sergančiu COVID-19; (iii) ar asmuo yra namuose dėl karantino (nenurodant priežasties) ir jo karantino laikotarpis; (iv) ar asmuo serga (nenurodant konkrečios ligos ar kt. priežasties). Papildomai atkreipiame dėmesį, jog tokie duomenys neturi būti saugomi ilgiau, nei to reikalauja susiklosčiusi situacija bei taikytini teisės aktai;
- darbdavys taip pat gali tvarkyti tokius su darbuotoju susijusius asmens duomenis kaip darbo nuotoliniu būdu pasirinkimo faktas ir kiti darbuotojo darbui taikomi apribojimai (plačiau apie darbą nuotoliniu būdu žr. žemiau);
- darbdavys ar kitas duomenų valdytojas turi teisę teirautis savo darbuotojų ar lankytojų apie tai, ar jiems yra pasireiškę COVID-19 simptomų, ar yra nustatyta COVID-19 diagnozė. Tačiau pabrėžtina, kad teisė gauti šią informaciją nereiškia, jog darbdaviai gali gautą informaciją dokumentuoti arba sudaryti atitinkamas duomenų rinkmenas;
- bet kokie tvarkomi asmens duomenys valstybės institucijoms visuomenės sveikatos užtikrinimo tikslu turi būti teikiami laikantis BDAR reikalavimų – prašymai pateikti asmens duomenis vertintini kiekvienu konkrečiu atveju atskirai (pvz., tais atvejais, kai prašoma pateikti statistiką, duomenų valdytojas neturėtų teikti konkretų duomenų subjektą identifikuojančių duomenų). Be to, reikėtų kiekvieną asmens duomenų teikimo atvejį dokumentuoti, siekiant vėliau užtikrinti atskaitomybės principo įgyvendinimą;
- bet kuriuo atveju darbdavys neturėtų pažeisti savo darbuotojų (bei kitų duomenų subjektų) teisės į asmens duomenų apsaugą ir reikalauti pateikti asmens duomenis, nebūtinus nustatytos tvarkos vykdymui užtikrinti. Pvz., duomenų valdytojai turėtų susilaikyti nuo darbuotojų ar lankytojų temperatūros rodmenų, medicininių pažymų (pvz., patvirtinančių neigiamą COVID-19 testo rezultatą) ir pan. duomenų rinkimo.

Galiausiai, rekomenduotina darbdaviui imtis aktyvių veiksmų ir informuoti duomenų subjektus apie simptomus, galimas rizikas, jų valdymo būdus, taikytinas priemones, galimybes dirbti nuotoliniu būdu, darbuotojų pareigą informuoti apie pasireiškusius COVID-19 ar panašius simptomus ir kt.

ASMENS DUOMENŲ APSAUGA IR DARBAS NUOTOLINIU BŪDU

Šiuo laikotarpiu itin aktualus klausimas – tinkamas darbo nuotoliniu būdu organizavimas. Reikėtų atkreipti dėmesį, kad šiuo atveju verslui yra svarbūs bei turi būti įvertinti du aspektai:

- **pačių darbuotojų asmens duomenų** apsauga bei jų privatumo gerbimas;
- **kitų duomenų subjektų** (daugeliu atvejų – klientų) **asmens duomenų,** su kuriais darbuotojams tenka dirbti nuotoliniu būdu, tinkama apsauga bei BDAR atitinkantis jų tvarkymas.

Reikėtų nepamiršti, kad darbuotojai, net ir atlikdami darbo funkcijas nuotoliniu būdu, nepraranda teisių į savo privatumą bei tinkamą jų asmens duomenų tvarkymą. Todėl pirmiausiai darbuotojus reikia tinkamai informuoti apie bet kokią stebėseną, kontrolę darbo nuotoliniu būdu metu (t. y. laikytis skaidrumo principo). Pavyzdžiui, apie darbdavio ar netgi paties darbuotojo įrenginių, informacinių bei komunikacinių technologijų naudojimą, šio naudojimo stebėseną ir kontrolę reikėtų iš anksto pranešti; atitinkami duomenys neturi saugomi ilgiau, nei tai yra būtina; prieigą prie jų gali turėti tik tie asmenys, kuriems tokie duomenys yra būtini ir pan.

Dažnai darbdaviai jau turi pasitvirtinę atitinkamas taisykles – atskiras tvarkas (pvz., nuotoliniam darbui ar darbdavio techninių priemonių naudojimui ne darbo vietoje reglamentuoti) arba konkrečias nuostatas kituose vidaus dokumentuose (pvz., darbo tvarkos taisyklėse), tinkamas esamai situacijai. Jeigu tokiems atvejams tinkamų taisyklių nėra, reikėtų svarstyti apie atitinkamų vidaus dokumentų papildymą ar naujų priėmimą.

Antrasis svarbus aspektas yra tinkamas kitų subjektų asmens duomenų tvarkymas darbuotojui namuose atliekant darbo funkcijas. Primintina, jog, be kita ko, pagal BDAR 32 str. tiek duomenų tvarkytojas, tiek duomenų valdytojas visais atvejais turi pareigą užtikrinti tvarkomų asmens duomenų saugumą (nepriklausomai nuo to, kur toks tvarkymas atliekamas).

Įprastai tai žymiai lengviau padaryti, kai darbuotojai savo darbo funkcijas vykdo tik darbo vietoje, darbdavio patalpose, namuose nesinaudoja darbdaviui priklausančiomis priemonėmis. O kaip tinkamai apsaugoti duomenis dirbant namuose? Dėl atsakymo į šį klausimą reikėtų spręsti kiekvienu konkrečiu atveju, atsižvelgiant į dirbant nuotoliniu būdu atliekamas funkcijas, tvarkomų asmens duomenų kiekį, jautrumą ir kitas aplinkybes.

Pateikiame tik keletą bendrų patarimų, rekomendacijų dėl duomenų tvarkymo darbuotojams dirbant namuose (šie patarimai aktualūs tiek pandemijos metu, tiek esant įprastoms sąlygoms darbuotojams darbus atliekant nuotoliniu būdu):

- darbdaviui priklausantys nešiojamieji įrenginiai (telefonai, kompiuteriai, planšetės, USB raktai ir kt.) laikytini saugiai, neturi būti prieinami pašaliniams asmenims. Praradus konkretų įrenginį, turėtų būti galimybių jame esančius duomenis apsaugoti nuo neteisėtus prieigos (pvz., ištrinti juos nuotoliniu būdu, užšifruoti ar pan.);
- laiku atlikti operacinės sistemos, antivirusinių programų ir kt. atnaujinimus;
- prisijungimui prie atitinkamų sistemų naudoti saugius, gerąją praktiką atitinkančius slaptažodžius ar net kelių veiksnių autenfikavimą (*multi-factor authentication* (MFA) arba t*wo-factor authentication* (2FA));
- susirašinėjimui darbo klausimais, komunikacijai su kolegomis, klientais naudoti tik darbinio (ne privataus) el. pašto paskyras, patikimas ir saugias programas. Įvertinti el. laiškų turinio bei jų priedų šifravimo (*encryption*) galimybes;
- įpareigoti darbuotojus naudotis tik saugia prieiga prie interneto, suteikti galimybę prisijungti prie tinklo ar atitinkamų sistemų (tik) naudojantis organizacijos VPN (*virtual private network*);
- apsvarstyti, kaip bus užtikrinamas atsarginių kopijų (*back-ups*) darymas;
- ir t. t.

Papildomai atkreiptinas dėmesys, kad verslas turėtų apsvarstyti aukščiau nurodytus aspektus ne tik siekdamas išvengti asmens duomenų apsaugos pažeidimų (gali būti, kad darbuotojų iš namų tvarkomų asmens duomenų kiekis bus minimalus ar praktiškai tokių tvarkyti netgi neteks), bet ir **apsaugoti savo komercines paslaptis, kitą jautrią, konfidencialią informaciją.**

Galiausiai, įdiegtos priemonės, atsiradusi praktika pravers ir pasibaigus šiam nelengvam laikotarpiui – juk informacinis saugumas tampa vis aktualesnis.