



Darbuotojų asmens duomenų tvarkymas, organizuojant darbą nuotoliniu būdu

2020-04-09

Pasaulyje susiklosčius neeilinei situacijai, susijusiai su COVID-19 plitimu, daugelyje valstybių, įskaitant Lietuvą, įvestas karantinas, dėl kurio darbdaviams kilo didelių iššūkių, susijusių su veiklos tęstinumo užtikrinimu. Vienas tokių iššūkių – nuotolinis darbas. Darbdaviai susiduria su klausimais dėl nuotolinio darbo organizavimo būdų, formų, darbuotojams paskirtų užduočių vykdymo kontrolės, efektyvaus darbo užtikrinimo priemonių. Esanti, nors ir išskirtinė, situacija šalyje nepašalina darbdavio pareigos nuotolinio darbo organizavimo metu užtikrinti ir tinkamą savo darbuotojų asmens duomenų apsaugą. Valstybinė duomenų apsaugos inspekcija (toliau – Inspekcija), matydama, su kokiais iššūkiais susiduria darbdaviai ir reaguodama į padidėjusias gaunamų paklausimų šia tema apimtis, parengė metodinę informaciją apie darbuotojų asmens duomenų tvarkymą, organizuojant darbą nuotoliniu būdu.

Asmens duomenų apimtis

Bendrasis duomenų apsaugos reglamentas (toliau – BDAR) įtvirtina pareigą tvarkyti tik tuos asmens duomenis, kurie yra būtini konkrečiam tikslui pasiekti. Taigi, organizuojant nuotolinį darbą, pirmiausiai, reikėtų įvertinti:

- **Kokie darbuotojai, atsižvelgiant į funkcijų ir atliekamų užduočių specifiką, gali dirbti nuotoliniu būdu?** Priklausomai nuo konkrečios veiklos, šiuo atveju papildomai gali būti tvarkomi tokie asmens duomenys kaip, pavyzdžiui, darbo nuotoliniu būdu faktas ir režimas.

- **Kokios darbo priemonės yra būtinos nuotoliniam darbui organizuoti?** Jei darbuotojui reikia išduoti priemones nuotoliniam darbui užtikrinti (kompiuteris, mobilusis įrenginys, šifruoto

nuotolinio prisijungimo atmintukai, kt.), tokiu atveju papildomai gali būti tvarkomi susisteminti rinkiniai apie tokių priemonių išdavimą, sąlygas.

- **Ar organizuojant darbą nuotoliniu būdu yra būtina jungtis prie duomenų valdytojo (duomenų tvarkytojų) resursų ar įrankių¹?** Jei atsakymas teigiamas, reikėtų įvertinti kiekvieną resursą ar įrankį atskirai, atsižvelgiant į tai, ar šie resursai jau yra naudojami įprastoje darbdavio veikloje ir, jei taip, kokie asmens duomenys dėl tokio naudojimo yra tvarkomi, nepriklausomai nuo to, ar prie resurso ar įrankio jungiamasi nuotoliniu būdu. Svarbu įvertinti ir tai, ar jungiantis prie šių resursų nuotoliniu būdu reikalinga tvarkyti papildomus duomenis ir kokiais tikslais.

Tuo atveju, jei dėl nuotolinio darbo būtina pradėti naudoti naujus resursus ar įrankius, būtina įvertinti ne tik paties resurso ar įrankio patikimumą, tačiau taip pat, kokie asmens duomenys, naudojantis šiuo resursu ar įrankiu, būtų tvarkomi ir kokiais tikslais. Primintina, kad, naudojantis elektroniniais resursais ar įrankiais, be prisijungimo duomenų (pavyzdžiui, prisijungimo vardas ir jo sąsaja su konkrečiu darbuotoju, taip pat žurnalo įrašų (angl. *log*)) ir prieigos teisių, taip pat tvarkomi ir kiti asmens duomenys, pavyzdžiui, susiję su užduočių vykdymu, atlikimu, rezultatais.

Pastaba! Darbdaviai turi įvertinti, kokius asmens duomenis būtina tvarkyti, organizuojant nuotolinį darbą, ir nesiimti perteklinio asmens duomenų tvarkymo veiksmų.

Darbuotojų stebėseną

Darbo organizavimas nuotoliniu būdu savaime nereiškia darbdavio pareigos imtis darbuotojų stebėsenos priemonių (stebėti susirašinėjimą elektroniniu paštu, fiksuoti veiksmus, naudojantis darbdavio suteiktu kompiuteriu ar mobiliuoju įrenginiu, įrašinėti pokalbius ar kt.), taip pat nereiškia, kad tokios priemonės yra būtinos ar proporcingos. Nors darbuotojo veiksmų, naudojantis darbdavio resursais ar įrankiais darbo metu, stebėseną savaime nėra laikytina pažeidimu, tačiau ji turi būti vykdoma laikantis BDAR reikalavimų. Darbdavys **prieš pradėdamas** konkretaus darbuotojo stebėseną turi:

- **Įvertinti darbuotojo stebėsenos proporcingumą siekiamiems tikslams, t. y. ar darbdavio interesai yra viršesni už darbuotojo interesus ir pagrindines teises ir laisves**

Atkreipiame dėmesį, kad darbuotojo stebėseną *negali būti pagrįsta darbuotojo sutikimu*, nes dėl darbdavio ir darbuotojo santykiams būdingos priklausomybės nėra tikėtina, kad duomenų subjektas galėtų neduoti savo darbdaviui sutikimo, kad būtų tvarkomi jo asmens duomenys, be baimės ar realios rizikos patirti neigiamą poveikį dėl savo nesutikimo. Taigi, esant darbuotojo ir darbdavio padėties disbalansui, darbuotojo sutikimas paprastai neatitiktų laisvos valios kriterijaus.

Atsižvelgiant į tai, darbdavys, siekdamas vykdyti darbuotojo stebėseną, paprastai galėtų remtis BDAR 6 straipsnio 1 dalies f punktu, o ši teisėto asmens duomenų tvarkymo sąlyga įpareigoja duomenų valdytoją atlikti interesų pusiausvyros testą, siekiant įvertinti, ar jo interesai persveria darbuotojo interesus ir pagrindines teises ir laisves. Informaciją apie interesų pusiausvyros testo atlikimą ir jam keliamus reikalavimus skaitykite nuomonėje „Dėl duomenų valdytojo teisėtų interesų“².

- **Atlikti poveikio duomenų apsaugai vertinimą (toliau – PDAV)**

¹ Šiame metodiniame dokumente tai apima prisijungimą prie darbo vietos, informacinių sistemų, duomenų bazių ar kt.

² 29 straipsnio duomenų apsaugos darbo grupės, įkurtos 1995 m. spalio 24 d. Europos Parlamento ir Tarybos Direktyvos 95/46 EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo pagrindu, 2014 m. balandžio 9 d. Nuomonėje „Dėl duomenų valdytojo teisėtų interesų“, kuri pasiekama šiuo adresu: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_lt.pdf.

PDAV *privalo būti atliktas* tuo atveju, kai asmens darbuotojų asmens duomenys tvarkomi darbuotojo stebėsenos ar kontrolės tikslais: asmens vaizdo ir (ar) garso duomenų tvarkymas darbo vietoje ir (ar) duomenų valdytojo patalpose ar teritorijose, kuriose dirba jo darbuotojai; asmens duomenų, susijusių su darbuotoju, komunikacijos, elgesio, vietos ar judėjimo stebėseną, tvarkymas. Atliekant PDAV turėtų būti išsamiai ir visapusiškai įvertinti galimi pavojai ir priemonės, tokio pavojaus sumažinimui (suvaldymui). Tuo atveju, jei atlikus PDAV konstatuojama, kad tvarkant duomenis kiltų didelis pavojus, jei duomenų valdytojas nesiimtų priemonių pavojui sumažinti, duomenų valdytojas turi kreiptis į Inspekciją išankstinių konsultacijų³.

• Parengti darbuotojų stebėsenos tvarką (taisykles) ir supažindinti su jomis darbuotojus

Darbdavys *privalo išsamiai dokumentuoti* darbuotojų stebėsenos, jei ji atliekama laikantis BDAR reikalavimų, tvarką: kokie darbuotojai, kokiais atvejais ir kokiomis sąlygomis bus stebimi. Pavyzdžiui, ar bus stebimi visi darbuotojai (jei ne – kaip bus atrinkta, kurie darbuotojai bus stebimi), ar bus stebimas naudojimas visais darbdavio resursais ar įrankiais (jei ne, kokie konkrečiai resursai ar įrankiai bus stebimi), ar bus vykdoma nuolatinė ar periodinė stebėseną (jei periodinė, koks bus jos periodiškumas ir nuo ko jis priklausys) ir t. t.

Darbuotojai turi būti pasirašytinai ar kitu informavimo faktą įrodančiu būdu supažindinti su tokia tvarka ir ji turi būti aiški, kad darbuotojai suprastų jų asmens duomenų tvarkymo darbdavio veikloje apimtį, pasekmes ir kad vėliau jiems nebūtų netikėta, kaip naudojami jų asmens duomenys, tokiu būdu užtikrinant tinkamą skaidrumo principo įgyvendinimą.

Papildomai rekomenduojame vadovautis 29 straipsnio duomenų apsaugos darbo grupės, įkurtos 1995 m. spalio 24 d. Europos Parlamento ir Tarybos Direktyvos 95/46 EB dėl asmens duomenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo pagrindu, 2017-06-08 nuomone Nr. 2/2017 „[Dėl duomenų tvarkymo darbe](https://vdai.lrv.lt/uploads/vdai/documents/files/Nuomonedelduomenutvarkymodrabe20170608wp249lt(2).pdf)“, su kuria galite susipažinti šiuo adresu: [https://vdai.lrv.lt/uploads/vdai/documents/files/Nuomonedelduomenutvarkymodrabe20170608wp249lt\(2\).pdf](https://vdai.lrv.lt/uploads/vdai/documents/files/Nuomonedelduomenutvarkymodrabe20170608wp249lt(2).pdf)

Darbuotojų informavimas

Skaidrumo principo reikalavimai (BDAR 5 straipsnio 1 dalies a punktas) įpareigoja darbdavį informuoti darbuotojus apie jų asmens duomenų tvarkymą ne tik pirminiame duomenų tvarkymo etape, tačiau ir vėlesniuose duomenų tvarkymo etapuose. Kitaip tariant, jei dėl nuotolinio darbo keičiasi darbuotojų asmens duomenų tvarkymas (apimtis, trukmė, tikslai, kt.), apie kurį jie buvo informuoti, darbdavys turi parengti privatumo pranešimą, susijusį su darbuotojų asmens duomenų tvarkymu, jiems dirbant nuotoliniu būdu (atsižvelgiant į BDAR 13 straipsnį), arba atnaujinti turimą privatumo pranešimą, aiškiai identifikuojant, kas konkrečiai keičiasi.

Darbdavys be pirmiau nurodytų pareigų taip pat turi tinkamai *instrukuoti* darbuotojus:

- Kaip tinkamai naudotis darbdavio resursais ar įrankiais nuotoliniu būdu;
- Kokios yra darbuotojų pareigos, vykdant funkcijas nuotoliniu būdu (operacinių sistemų naudojimas ir atnaujinimas, reikalavimai antivirusinėms programoms, slaptažodžių pasirinkimas ir keitimas, interneto grėsmės, pareiga atsijungti nuo resurso ar įrankio, kai juo nėra naudojama, tokiu būdu ribojant trečiųjų asmenų neteisėtas prieigas prie asmens duomenų ir darbdavio resursų ar įrankių);
- Į ką ir kokia tvarka kreiptis įvykus saugumo incidentui ar asmens duomenų saugumo pažeidimui ir pan.

³ <https://www.e-tar.lt/portal/lt/legalAct/e941c990ab7b11e88f64a5ecc703f89b>.

Saugumo priemonės

Darbdavys, organizuodamas darbą nuotoliniu būdu, taip pat turėtų įvertinti šiuos aspektus:

- Jei nuotolinio darbo metu naudojami susirašinėjimo įrankiai (pavyzdžiui, *Teams*, *Hangout*, *Jaber*, *Telegram* ar kt.), darbdavys turi įvertinti, kaip toks susirašinėjimas (visas ar tik nesusijęs su darbo procesu) bus naikinamas ir kas už tai atsakingas?
- Ar darbdavio resursais ar įrankiais naudojamosi tik turint autorizuotas (individualias) prieigas (svarbu užtikrinti, kad kiekvienas naudotojas turėtų atskirą prieigą)?
- Kaip užtikrinama prieigų kontrolė (kiek asmenų gali turėti administratoriaus teises, kas gali suteikti, keisti ir naikinti prieigas, kt.)?
- Koku būdu yra naudojami darbdavio resursai ar įrankiai (internetu svetainė, interneto platforma, aplikacija ar į kompiuterį įdiegiama programinė įranga)?
- Kokie asmens duomenys bus surinkti darbdavio resurso ar įrankio naudojimo metu, kur ir kiek laiko jie bus saugomi?
- Kokios techninės saugumo priemonės yra įdiegtos (įvertinti, kad darbuotojų namuose nėra papildomų tinklo saugumo priemonių, pavyzdžiui, ugniasienės)?
- Ar konkretus resursas ar įrankis užtikrina galimybę įgyvendinti duomenų subjektų teises, įtvirtintas BDAR?

Taip pat rekomenduojame laikytis Nacionalinio kibernetinio saugumo centro bazinių kibernetinio saugumo rekomendacijų dirbantiems nuotoliniu būdu, kuriose aptarti pagrindiniai duomenų, įskaitant asmens duomenų, saugumo aspektai. Rekomendacijas galite rasti šiuo adresu: https://www.nksc.lt/naujienos/bazines_kibernetinio_saugumo_rekomendacijos_dirban.html.