



Informacinė
valanda NVO

DUOMENŲ APSAUGA klausimai-atsakymai

Ona Valainienė
Teisininkė, sertifikuota duomenų
apsaugos pareigūnė

Kokie praktiniai patarimai dėl vaikų dienos centrų lankytojų ir jų tėvų duomenų apsaugos? Akreditacijos procesui šių duomenų prašo savivaldybės: kaip pagal galiojančias tvarkas jas pateikti?

Galite rinkti ir tvarkyti tik tuos asmens duomenis, kurių tvarkymui turite aiškų teisėtą tikslą ir vieną iš teisinių pagrindų. Tai gali būti prievolė jūsų organizacijai numatyta teisės aktuose (pvz., kad vykdant tam tikrą veiklą turite fiksuoti paslaugos gavėjų lankomumą, ir paskui tą sąrašą kažkiek laiko turite saugoti, nes gali prireikti jį pateikti tikrinančioms institucijoms ar pan.), gali būti sutikimas (pvz., norite tiesiog savo iniciatyva papildomai siųsti informaciją el. paštu apie organizuojamus renginius) ir pan. Svarbu, kad kiekvienu atveju duomenų subjektai (t. y. asmenys, kurių duomenis tvarkote) būtų informuojami, kokius asmens duomenis, kodėl, kaip ir kiek laiko jūs tvarkysite. Jei tvarkote duomenis asmenų iki 16 metų, informacija apie asmens duomenų tvarkymą turi būti pateikiama jų tėvams ar globėjams.

Savivaldybė akreditacijos procesui turėtų prašyti asmens duomenų tokia forma ir tiek, kiek yra tiesiogiai nustatyta teisės aktuose arba išplaukia iš juose įtvirtintų įgaliojimų, pareigų, kurias turi atlikti savivaldybė akreditacijos metu. Vienas iš tokių teisės aktų – socialinės apsaugos ir darbo ministro 2020 m. birželio 30 d. įsakymu Nr. A1-622 patvirtintu Socialinės priežiūros akreditavimo tvarkos aprašu <https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/ebffac16bb0a11ea9a12d0dada3ca61b/asr>



Ar gali būti bendri duomenų valdytojai? Jei taip, tai kokiais atvejais?

Taip, organizacija gali būti bendru duomenų valdytoju, jeigu duomenų tvarkymo tikslus ir priemones ji nustato kartu su kita organizacija. Pvz., kelios organizacijos organizuoja savo paslaugas kaip tam tikrą paslaugų paketą arba diegia bendrą platformą asmens duomenims surinkti ir pan.



Projekto metu vykdome elektroninę dalyvių registraciją į online mokymus. Kadangi suplanavome į projekto veiklas įtraukti tautinių mažumų atstovus, besiregistruojančiųjų prašome anketoje pažymėti tautybę. Ar galime rinkti šiuos duomenis? Kiek laiko juos galime saugoti?

Labai svarbus klausimas, kokių tikslų jums reikalingi šie duomenys, ką jūs darysite su informacija apie žmogaus tautybę. Duomenys apie tautybę yra priskiriami prie specialios kategorijos duomenų, todėl jų negalite tvarkyti, pvz., teisėto intereso pagrindu. Iš to, kiek aprašėte, tikėtina, kad tokius duomenis galėtumėte rinkti sutikimo pagrindu. Sutikimas suponuoja tai, kad registracijos anketoje prašymas pažymėti tautybę negali būti privalomas. Asmuo turi suprasti, kad tai yra neprivaloma ir turi turėti galimybę užbaigti anketos pildymą nenurodydamas tautybės. Asmeniui, pildant anketą, turi būti pateikiama informacija, kokių tikslų yra renkami jo asmens duomenys (įskaitant informaciją apie tautybę), kaip jie bus naudojami ir kiek laiko. Asmens duomenis (įskaitant ir informaciją apie tautybę) galite saugoti ne ilgiau nei yra būtina jūsų nusistatytiems tikslams pasiekti.



Jeigu NVO įstaigoje dirbantys asmenys įgyvendina projektus ir vienaip ar kitaip prieina prie duomenų, klientų ar darbuotojų, tai ką būtų galima paskirti atsakingą asmenį už duomenų apsaugą?

Čia yra pakankama sprendimų laisvė. Svarbu, kad tas asmuo būtų atsakingas už tam tikros kategorijos (ar tai būtų klientų ar darbuotojų) duomenų tvarkymą organizacijoje. „Atsakingas“ reiškia, kad žinotų ir gebėtų paaiškinti, kokių tikslų (tikslais), kokiais būdais asmens duomenys yra tvarkomi, kiek laiko jie tvarkomi, kur laikomi (saugomi), kada ir kaip naikinami, kas organizacijoje jais naudojasi (prieigų kontrolė). Tokie asmenys, paprastai vadinami duomenų šeimininkais (*data owner*), yra atsakingi už asmens duomenų tvarkymo veiklos įrašų (jei organizacijai privaloma tokį turėti) pildymą bei atnaujinimą. Už darbuotojų duomenų apsaugą paplitusi praktika paskirti atsakingu asmenį, kuris kuruoja įdarbinimo ir kitus darbo teisės įmonėje klausimus



Kaip teisingai informuoti bei surinkti sutikimus įrašant zoom seminarą, kuris paskui būtų platinamas tarp dalyvių arba keliamas į soc. medijų kanalus?

Pirmiausia, dalyviai turi būti informuojami iš anksto, prieš registruojantis į seminarą, apie tai, kad dalyvio privatumas dalyvaujant seminare nėra garantuojamas, nes organizatoriai pasilieka teisę platinti seminaro įrašą ... (įvardinti kas ir kur bus platinama). Dalyviui registruojantis turi būti (gali būti dar ir prieš platinant skelbimą apie renginį) pateikiama informacija, jog seminaras bus įrašomas. „Dalyvaudami jūs sutinkate, kad jūsų atvaizdas (jei įjungta kamera, ar nuotrauka), vardas, pavardė (jei nurodote prisijungdami), pasisakymai, komentarai bus įrašomi ir platinami kitiems dalyviams, taip pat skelbiami socialinių medijų kanaluose. Mes šį vaizdo įrašą saugosime xxx. Jūsų dalyvavimas seminare reiškia jūsų sutikimą dėl paminėto asmens duomenų tvarkymo. Jūs turite teisę atšaukti šį sutikimą, tačiau tai neturės įtakos veiksams, atliktiems iki sutikimo atšaukimo. Vaizdo įrašas, kuris buvo paplatintas sutikimo galiojimo laikotarpiu, nebus ištrintas arba bus ištrintas tik jeigu tai techniškai įmanoma nepažeidžiant vaizdo įrašo turinio vientisumo.“ Prie šio teksto turėtų pažymėti, kad susipažino ar sutinka.

Rekomenduojama tą pačią informaciją pakartoti seminarui prasidedant (jau įrašinėjant vaizdą), kad nesutinkantieji turėtų paskutinę galimybę atsijungti.

Visada verta apsvarstyti, ar nėra galimybių asmeniui dalyvauti seminare, užtikrinant jo privatumą, kad sutikimas nebūtų susietas su pačiu dalyvavimu seminare.



Kai fotografuojamas viešas renginys, į kurį nebuvo vykdoma registracija, kaip tokiu atveju, ar galima publikuoti nuotraukas?

Prie įėjimo į renginį gerai matomoje vietoje pastatyti skelbimą, kad renginio metu bus fotografuojama ir nuotraukos bus platinamos ... (nurodyti kur).

Taip pat prasidedant renginiui žodžiu gyvai pasakyti informaciją apie fotografavimą. Galima numatyti vietas žmonėms, kurie nesutinka ir nenori būti fotografuojami, bei susiderinti su fotografais, kad ten jie nefotografuotų.

Galima paminėti šias rekomendacijas fotografuojant:

- Asmenį fotografuoti jam matant ir suvokiant, jog yra fotografuojamas;
- Nereikėtų fotografuoti ir po to viešinti nuotraukų, kurios galėtų asmenį pažeminti, įžeisti ar kompromituoti, taip pat paviešintų jo negales;
- Nefotografuoti asmens, kuris aiškiai parodo, kad nenori būti fotografuojamas (užsidengė ranka, veido mimika, nususuko ar pan);
- Nefotografuoti asmenų veidų, jeigu tai nėra būtina siekiamai žinutei paskleisti, ypač nepilnamečių.



Kokius duomenis, informaciją galima, o ir privaloma pateikti viešosiose ataskaitose, nepažeidžiant BDAR? Kokią informaciją su asmens duomenimis teikiama auditui yra privaloma, ir kaip apsaugoti, užsitikrinti, kad audito įmonės duomenų neperduotų trečioms šalims (išskyrus teisinius procesus, jei rasta pažeidimų)?

Esama įvairių ataskaitų, priklausomai, kokioje srityje veikiate. Pateikinėkite tik tuos asmens duomenis, kuriuos tikrai privalote pateikti (pareiga nurodyti tam tikrus asmens duomenis yra numatyta jums taikomuose teisės aktuose ar pan.). Įprastai ataskaitose nurodoma organizacijos vadovo vardas, pavardė, gali būti buhalterio vardas, pavardė, tam tikrais atvejais teisės aktuose reikalaujama nurodyti valdymo organų narių vardus, pavardes, pareigybes, kitas jų profesines veiklas. Ataskaitose gali būti kalbama apie veiklos rezultatus, strategiją, įvykdytus ar vykdomus projektus, finansinius rodiklius (pajamas, išlaidas), personalą (skaičių, kiek ir kokių pareigybių darbuotojų organizacijoje dirba), atlyginimus (pateikiant subendrintą informaciją), nepateikiant išvis jokių asmens duomenų, t. y. konkretų fizinį asmenį individualizuojančios informacijos.

Auditoriai (audito įmonės) privalo laikytis jiems keliamų standartų ir įstatymų, be kita ko, ir reguliuojančių asmens duomenų apsaugą, reikalavimų. Jie gali prašyti tik tokios informacijos, kuri yra reikalinga tinkamai auditui atlikti. Audito įmonė asmens duomenis gali tvarkyti tik tokiu būdu ir tik tiek, kiek tai yra būtina audito atlikimui. Audito įmonė negali perduoti įmonių informacijos, įskaitant ir asmens duomenų, trečiosioms šalims, jei tai nesusiję su audito atlikimu.

Įprastai audito įmonė yra laikoma savarankišku duomenų valdytoju. Audito įmonė ir audituojama organizacija turi pasirašyti sutartį dėl audito atlikimo. Šioje sutartyje turėtų būti aptariamas ir asmens duomenų perdavimo klausimas bei audito įmonės įsipareigojimai, atsakomybė tvarkyti asmens duomenis laikantis Bendrojo duomenų apsaugos reglamento reikalavimų (vadinasi ir įsipareigojimas neperduoti asmens duomenų trečiosioms šalims, kai tam nėra teisinio pagrindo).



Įgyvendinant projektą dažnu atveju reikalaujami dalyvių sąrašai. Kaip tinkamai tokius sąrašus pildyti, kaip saugoti ir kuriais atvejais dalyvių sąrašai pažeidžia BDAR?

Šiuos klausimus geriausia išsiaiškinti su projektų finansuotojais, jei jie iš anksto nepateikia tokios informacijos, ir jų atsakymus patartina išsaugoti ir turėti raštu. Reikalavimai sąrašams priklausomai nuo projekto gali skirtis. Dalyvių sąrašų pildymo ir saugojimo tikslas paprastai yra projekto įgyvendinimo kontrolė. Nustatant saugojimo laiką svarbu atsižvelgti, kiek laiko jūsų organizacija yra atskaitinga už projekto įgyvendinimą.



„BDAR taikymas nepriklauso nuo organizacijos dydžio, bet nuo atliekamo duomenų tvarkymo pobūdžio. Kita vertus, ne visos BDAR prievolės taikomos mažoms ir vidutinėms įmonėms, pvz. jei dirba mažiau kaip 250 darbuotojų, nereikia tvarkyti duomenų tvarkymo veiklos įrašų.“ Ar tai reiškia, kad jei organizacija maža (dirba keli darbuotojai) – jai nereikia duomenų tvarkymo veiklos įrašų? Ar vis tik reikia atsižvelgti į tai, koks įgyvendinamas projektas, kokie duomenys yra renkami ir saugomi (turint omenyje NVO įgyvendinamus projektus) ir pasirengti atitinkamas tvarkas?

Duomenų tvarkymo veiklos įrašai – tai vienas iš įmonės vidinių dokumentų, einantis šalia kitų tvarkų, kurios turi būti bet kokių atvejų, jei jūsų organizacija tvarko kažkokius asmens duomenis. Tik Duomenų tvarkymo veiklos įrašai tam tikrais atvejais gali būti nepildomi. Bendrasis duomenų apsaugos reglamentas numato eilę sąlygų, iš kurių nors vienai esant, organizacija privalo turėti duomenų tvarkymo veiklos įrašą. Tai gali būti pvz., daugiau kaip 250 darbuotojų, arba duomenų tvarkymas yra reguliarus, arba duomenų tvarkymas apima specialių kategorijų asmens duomenis ir t. t. Taigi, nepriklausomai nuo to, kiek jūsų organizacijoje dirba darbuotojų, jums gali reikėti turėti duomenų tvarkymo veiklos įrašus, jei, pvz., reguliariai įgyvendinate projektus, susijusius su asmens duomenų tvarkymu.



Duomenų tvarkymo principai – užtikrinant tinkamą saugumą (įdiegiamos tinkamos techninės ir organizacinės priemonės) – nuo ko mažai organizacijai pradėti, norint užtikrinti, kad naudojamos tinkamos techninės ir organizacinės priemonės?

Pirmiausia reikėtų inventorizuoti, kur ir kokius asmens duomenis jūs turite ir ką su jais veikiate. Pasitikrinti, ar visi duomenys tvarkomi siekiant teisėtų tikslų ir, ar tam yra teisinis pagrindas (pagrindai), per kiek laiko tikslų pasiekiate, ką darote su duomenimis, kai jie tampa nereikalingi ir pan. Kitas svarbus momentas, kur yra jūsų tvarkomi asmens duomenys. Ar jie saugūs, kas turi prie jų prieigą, ar tikrai tik asmenys, kuriems jų reikia darbo funkcijoms atlikti. Organizacinės priemonės tai yra visos tvarkos, kuriomis jūs apsibrėžiate aukščiau paminėtus klausimus. Techninės – tai fizinis ir technologinis duomenų saugumas.

Kalbant apie IT saugumą labai sunku kažką konkrečiai kalbėti, nežinant jūsų situacijos. Tikriausiai būtų naudinga IT specialisto konsultacija saugumo klausimais. Galima paminėti tokias praktikoje taikomas technologines priemones: antivirusinės programos, saugus interneto ryšys, stiprių slaptažodžių politika, duomenų šifravimas, atsarginių kopijų kūrimas ir pan.



Organizacijos vidiniai dokumentai – ar galima rasti išvardintų tvarkų pavyzdinių dokumentų?

Oficialaus tokio dokumentų rinkinio greičiausiai nerasite. Tačiau galima rasti kitų organizacijų ar valstybės institucijų politikų, tvarkų, pasižiūrėti, kaip kiti apsibrėžia vieną ar kitą klausimą. Tik ne visada yra garantija, kad jos surašytos teisingai.

