PASLAUGŲ TEIKĖJŲ, REGISTRUOTŲ VALSTYBINĖS MOKESČIŲ INSPEKCIJOS *MOSS* SISTEMOJE, ASMENS DUOMENŲ TVARKYMO TEISĖTUMO TIKRINIMŲ REZULTATŲ APIBENDRINIMAS

2016-12-29

Valstybinė duomenų apsaugos inspekcija (toliau – VDAI), įgyvendindama Lietuvos Respublikos valstybės kontrolės 2015 m. balandžio 30 d. valstybinio audito ataskaitoje Nr. VA-P-60-12-7 „Elektroninės prekybos kontrolė“ pateiktą rekomendaciją, atliko 51 Valstybinės mokesčių inspekcijos MOSS sistemoje registruotų paslaugų teikėjų (toliau – bendrovės) asmens duomenų tvarkymo teisėtumo patikrinimą.

Tikrinimo metu nustatyta, kad 9 bendrovės netvarko fizinių asmenų asmens duomenų automatiniu būdu, 42 bendrovėse nustatyta Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo (toliau – ADTAĮ), 37 bendrovėse Lietuvos Respublikos elektroninių ryšio įstatymo (toliau – ERĮ) pažeidimų. 1 bendrovė pažeidimus pašalino tikrinimo metu.

Dėl asmens duomenų tvarkymo teisėtumo

Asmens duomenų tvarkymą reglamentuoja ADTAĮ. ADTAĮ 31 straipsnis nustato, kad asmens duomenys gali būti tvarkomi automatiniu būdu tik kai duomenų valdytojas arba jo atstovas Vyriausybės nustatyta tvarka praneša VDAI. Tikrinimo metu nustatyta, kad iš 42 tikrintų bendrovių 25 bendrovės apie asmens duomenų tvarkymą automatiniu būdu nebuvo pranešusios VDAI ir taip pažeidė ADTAĮ 31 straipsnio reikalavimus. Taip pat nustatyta, kad 2 bendrovės nepatikslino VDAI Asmens duomenų valdytojų valstybės registre pateiktos informacijos (apie bendrovės pavadinimą, kontaktinius duomenis ir tvarkomų asmens duomenų sąrašą ir tikslus).

ADTAĮ 3 straipsnio 1 dalies 1 punkte numatyta, kad asmens duomenys turi būti renkami apibrėžtais ir teisėtais tikslais ir toliau nebūtų tvarkomi tikslais, nesuderinamais su nustatytaisiais prieš renkant asmens duomenis, o 1 dalies 4 punkte – kad duomenys turi būti tapatūs, tinkami ir tik tokios apimties, kuri būtina jiems rinkti ir toliau tvarkyti. Atsižvelgiant į tai, asmens duomenys turi būti gaunami ir tvarkomi tik tokia apimtimi, kuri reikalinga duomenų valdytojo teisėtiems duomenų tvarkymo tikslams. Priešingu atveju būtų pažeidžiami ADTAĮ 3 straipsnio 1 dalies 1 ir 4 punktai. Tikrinimo metu nustatyta, kad 3 bendrovių asmens kodo, asmens tapatybės dokumento kopijų tvarkymas ir šių kopijų teikimas asmens duomenų gavėjams bei asmens duomenų teikimas į trečiąsias valstybes prieštarauja ADTAĮ 3 straipsnio nuostatoms.

Dėl duomenų subjekto teisių ir jų įgyvendinimo

ADTAĮ 24 straipsnio 1 dalyje numatyta, kad duomenų valdytojas privalo suteikti duomenų subjektui, kurio asmens duomenis renka tiesiogiai iš jo, šią informaciją (išskyrus atvejus, kai duomenų subjektas tokią informaciją jau turi):

1) Apie savo (duomenų valdytojo) ir savo atstovo, jeigu šis yra, tapatybę ir nuolatinę gyvenamąją vietą (jeigu duomenų valdytojas ar jo atstovas yra fizinis asmuo) ar rekvizitus ir buveinę (jeigu duomenų valdytojas ar jo atstovas yra juridinis asmuo);

2) Kokiais tikslais ketinami tvarkyti duomenų subjekto asmens duomenys;

3) Kitą papildomą informaciją (kam ir kokiais tikslais teikiami duomenų subjekto asmens duomenys; kokius savo asmens duomenis duomenų subjektas privalo pateikti ir kokios yra duomenų nepateikimo pasekmės, apie duomenų subjekto teisę susipažinti su savo asmens duomenimis ir teisę reikalauti ištaisyti neteisingus, neišsamius, netikslius savo asmens duomenis), kiek jos reikia, kad būtų užtikrintas teisingas asmens duomenų tvarkymas nepažeidžiant duomenų subjekto teisių.

Tikrinimų metu nustatyta, kad tik 17 bendrovių interneto svetainėje tinkamai informuoja duomenų subjektą apie jo asmens duomenų tvarkymą bei duomenų subjekto teisę susipažinti su savo asmens duomenimis ir teisę reikalauti ištaisyti neteisingus, neišsamius, netikslius asmens duomenis. Nustatyta, kad 25 bendrovės prieš pradėdamos tvarkyti asmens duomenis duomenų subjektams nepateikia informacijos apie asmens duomenų tvarkymą, kaip to reikalauja ADTAĮ 24 straipsnio 1 dalis (pvz., duomenų subjektai interneto svetainėse nėra informuojami apie duomenų valdytojo pavadinimą, juridinio asmens kodą, duomenų tvarkymo tikslus, duomenų subjekto teises ir pan.).

ADTAĮ 25 straipsnio 1 dalyje nustatyta, kad duomenų subjektas, pateikdamas duomenų valdytojui ar duomenų tvarkytojui asmens tapatybę patvirtinantį dokumentą, turi teisę gauti informaciją, iš kokių šaltinių ir kokie jo asmens duomenys surinkti, kokiu tikslu jie tvarkomi, kokiems duomenų gavėjams teikiami ir buvo teikti bent per paskutinius vienerius metus.

Tikrinimo metu nustatyta, kad tik 20 bendrovių tinkamai įgyvendina pirmiau nurodytus reikalavimus. ADTAĮ 25 straipsnyje nustatytą duomenų subjekto teisę susipažinti su savo asmens duomenimis privalo įgyvendinti duomenų valdytojas ar duomenų tvarkytojas, tačiau 19 bendrovių perleisdamos savo pareigos įgyvendinimą duomenų subjektui, leisdamos duomenų subjektui prisijungti prie duomenų subjekto sukurtos paskyros, užsakymo, nepilnai įgyvendino ADTAĮ 25 straipsnio reikalavimus, kadangi pats duomenų subjektas, įgyvendindamas savo teisę, negalės gauti informacijos, kokiems duomenų gavėjams teikiami jo asmens duomenys ir buvo teikti bent per paskutinius vienerius metus.

Nustatyta, kad 15 bendrovių sudaro sąlygas netinkamai įgyvendinti ADTAĮ 26 straipsnyje nustatytą duomenų subjekto teisę reikalauti ištaisyti, sunaikinti ar sustabdyti savo asmens duomenų tvarkymo veiksmus (pvz., bendrovėse tvarkomi asmens duomenys gali būti taisomi neturint duomenų subjekto rašytinio prašymo, nėra nustatytas bei reglamentuotas konkretus terminas (rekomenduotina 5 darbo dienos), per kurį bendrovės įgyvendins duomenų subjekto teisę ištaisyti, sunaikinti savo asmens duomenis arba sustabdyti savo asmens duomenų tvarkymo veiksmus.

Dėl asmens duomenų tvarkymo reglamentavimo

Dėl asmens duomenų ADTAĮ 30 straipsnio 1 dalyje nurodyta, kad duomenų valdytojas ir duomenų tvarkytojas privalo įgyvendinti tinkamas organizacines ir technines priemones, skirtas apsaugoti asmens duomenims nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo, taip pat nuo bet kokio kito neteisėto tvarkymo, o 2 dalyje VDAI nustato bendruosius reikalavimus organizacinėms ir techninėms duomenų saugumo priemonėms. VDAI direktoriaus 2008 m. lapkričio 12 d. įsakymu Nr. 1T-71 „Dėl bendrųjų reikalavimų organizacinėms ir techninėms asmens duomenų saugumo priemonėms patvirtinimo“ nustatyti Bendrieji reikalavimai organizacinėms ir techninėms asmens duomenų saugumo priemonės (toliau – bendrieji reikalavimai). Tikrinimo metu nustatyta, kad 18 bendrovių neturi dokumento, reglamentuojančio asmens duomenų tvarkymą, o 14 bendrovių turimi dokumentai neatitinka Bendrųjų reikalavimų 8 punkte nustatytų reikalavimų (pvz., nėra reglamentuoti asmens duomenų tvarkymo tikslai, tvarkomų asmens duomenų sąrašas kiekvienu nustatytu asmens duomenų tvarkymo tikslu (t. y. paslaugų teikimo ir tiesioginės rinkodaros tikslu), asmens duomenų saugojimo tvarka ir terminai, duomenų subjekto teisės ir jų įgyvendinimo tvarka ir kt.).

Dėl asmens duomenų saugojimo termino

Tikrinimo metu nustatyta, kad 11 bendrovių nėra nustatytas asmens duomenų saugojimo terminas, o 3 bendrovėse nustatytas per ilgas asmens duomenų saugojimo terminas, prieštaraujantis ADTAĮ nustatytiems reikalavimams.

Pagal ADTAĮ 4 straipsnį, asmens duomenys saugomi ne ilgiau, negu to reikalauja duomenų tvarkymo tikslai. Kai asmens duomenys nebereikalingi jų tvarkymo tikslams, jie turi būti sunaikinami, išskyrus tuos, kurie įstatymų nustatytais atvejais turi būti perduoti valstybės archyvams. Remiantis minėta ADTAĮ nuostata, duomenų valdytojas turi nustatyti konkretų (ne minimalų ar maksimalų) asmens duomenų saugojimo terminą. Duomenų saugojimo terminas turi būti pagrįstas ir turi būti nustatomas įvertinant poreikį tvarkyti asmens duomenis atsižvelgus į duomenų tvarkymo tikslus.

Dėl asmens duomenų tvarkymo tiesioginės rinkodaros tikslu

ADTAĮ 2 straipsnio 12 dalyje apibrėžta, kad tiesioginė rinkodara yra veikla, skirta paštu, telefonu arba kitokiu tiesioginiu būdu siūlyti asmenims prekes ar paslaugas ir (arba) teirautis jų nuomonės dėl siūlomų prekių ar paslaugų. Tikrinimo metu nustatyta, kad klientų asmens duomenis tiesioginės rinkodaros tikslais tvarko 19 bendrovių, kurios apie tokį asmens duomenų tvarkymą nepranešė VDAI ir pažeidė ADTAĮ 31 straipsnio reikalavimus.

ADTAĮ 14 straipsnio 1 dalyje nustatyta, kad asmens duomenys gali būti tvarkomi tiesioginės rinkodaros tikslais tik po to, kai duomenų subjektas duoda sutikimą. Taip pat ERĮ 69 straipsnio 1 dalyje nurodyta, kad naudoti elektroninių ryšių paslaugas, įskaitant elektroninio pašto pranešimų siuntimą, tiesioginės rinkodaros tikslu leidžiama tik gavus išankstinį abonento ar registruoto elektroninių ryšių paslaugų naudotojo sutikimą.

Duomenų valdytojas, tvarkantis asmens duomenis tiesioginės rinkodaros tikslais, privalo įgyvendinti ADTAĮ 14 straipsnio 2 ir 3 dalyse bei 27 straipsnio 1 dalyje numatytas nuostatas, t. y. privalo nustatyti asmens duomenų saugojimo trukmę, sudaryti aiškią, nemokamą ir lengvai įgyvendinamą galimybę duomenų subjektui išreikšti sutikimą ar nesutikimą dėl jo asmens duomenų tvarkymo

tiesioginės rinkodaros tikslais bei privalo supažindinti duomenų subjektą su jo teise nesutikti, kad būtų tvarkomi jo asmens duomenys.

Tikrinimo metu nustatyta, kad 9 bendrovės pažeidė ADTAĮ 14 straipsnyje ir ERĮ 69 straipsnyje nustatytus reikalavimus, nesudarydamos aiškios ir lengvai įgyvendinamos galimybės duomenų subjektui išreikšti sutikimą ar nesutikimą dėl jo asmens duomenų tvarkymo tiesioginės rinkodaros tikslais, o 4 bendrovėse nebuvo sudaryta galimybė duomenų subjektui pačiam išreikšti savanorišką sutikimą ar nesutikimą dėl jo asmens duomenų tvarkymo tiesioginės rinkodaros tikslais, kaip to reikalauja ADTAĮ 14 straipsnio 3 dalis.

Dėl slapukų naudojimo teisėtumo

ERĮ 61 straipsnio 4 dalyje yra nustatyta, kad saugoti informaciją arba suteikti galimybę naudotis jau saugoma informacija abonento ar faktinio elektroninių ryšių paslaugų naudotojo galiniame įrenginyje leidžiama tik su sąlyga, kad atitinkamam abonentui ar faktiniam elektroninių ryšių paslaugų naudotojui, vadovaujantis ADTAĮ suteikus aiškią ir išsamią informaciją, įskaitant informaciją apie tvarkymo tikslus, jis davė sutikimą. Šios nuostatos nedraudžia techninio saugojimo ar naudojimosi duomenimis, kurio vienintelis tikslas yra perduoti informaciją elektroninių ryšių tinklu, taip pat būtinais atvejais teikti informacinės visuomenės paslaugas, kurias užsako abonentas ar faktinis elektroninių ryšių paslaugų naudotojas.

Tikrinimo metu nustatyta, kad 37 bendrovėse į vartotojo kompiuterį įrašoma laikino galiojimo informacija (t. y. interneto svetainėse yra naudojami slapukai (angl. *cookies*), neatitinka ERĮ 61 straipsnio 4 dalyje nustatytų reikalavimų.

33 bendrovių interneto svetainėse nepateikiama informacija apie naudojamus slapukus bei jų įrašymo tikslus. 25 bendrovėse nėra gaunamas *savanoriškas* vartotojo sutikimas dėl tokios informacijos įrašymo į vartotojo galinį įrenginį.

Tikrinimų metu nustatyta, kad slapukų įrašymo į galinį vartotojo įrenginį tikslai yra susiję ne tik su internetinio puslapio funkcionavimu, todėl bendrovės turi įgyvendinti ERĮ 61 straipsnio 4 dalies reikalavimus: duomenų subjektui turi būti aiškiai ir išsamiai pateikta informacija apie informacijos į vartotojo galinį įrenginį įrašymą (slapukų naudojimo tikslus, slapukų galiojimo terminą bei nurodoma, kokie konkrečiai slapukai naudojami ir kokius duomenis jie fiksuoja) iš karto atsidarius tinklalapį ir gauti asmens savanorišką sutikimą dėl tokios informacijos įrašymo (išskyrus atvejus, jei slapukai yra būtini informacijai perduoti ir teikti informacinės visuomenės paslaugas) bei užtikrinama, kad slapukai būtų įrašomi tik gavus vartojo sutikimą dėl tokios informacijos įrašymo.

Pažymėtina, kad interneto svetainės naudotojo neveikimas (t. y. kai tinklalapyje yra pateikiama tik informacija, kad tęsiant apsilankymą tinklalapyje duomenų subjektas sutinka su slapukų naudojimu) negali būti laikomas tinkamu sutikimu, kadangi duomenų subjekto sutikimas dėl slapukų naudojimo turi būti išreikštas aktyviais veiksmais (pvz., pažymint varnele savo pasirinkimą, paspaudžiant mygtuką „sutinku“). Taip pat naudotojui turi būti sudaryta reali galimybė pasirinkti duoti ar neduoti sutikimą dėl slapukų naudojimo.

Visoms bendrovėms pateikti nurodymai pašalinti nustatytus pažeidimus.