VALSTYBINĖ
DUOMENŲ APSAUGOS
INSPEKCIJA

TIKRINIMŲ REZULTATŲ APIBENDRINIMAS DĖL ĮGYVENDINAMŲ ASMENS DUOMENŲ SAUGUMO PRIEMONIŲ TINKAMUMO, TEIKIANT ĮRENGINIŲ GARANTINIO IR PO GARANTINIO APTARNAVIMO PASLAUGAS

2017 m.

Valstybinė duomenų apsaugos inspekcija (toliau – VDAI), siekdama išsiaiškinti įgyvendinamų asmens duomenų saugumo priemonių tinkamumą, teikiant įrenginių garantinio ir po garantinio aptarnavimo paslaugas, atliko asmens duomenų tvarkymo teisėtumo patikrinimą 9 bendrovėse, teikiančiose įrenginio garantinio ir po garantinio aptarnavimo paslaugas (toliau – Bendrovė).

Tikrinimo metu visose 9 bendrovėse nustatyta Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo (toliau – ADTAĮ) pažeidimų.

Dėl pranešimo apie duomenų tvarkymą

Asmens duomenų tvarkymą reglamentuoja ADTAĮ. ADTAĮ 31 straipsnyje yra nustatyta, kad asmens duomenys gali būti tvarkomi automatiniu būdu tik tuo atveju, kai duomenų valdytojas Lietuvos Respublikos Vyriausybės nustatyta tvarka praneša apie tai VDAI, išskyrus šioje dalyje numatytus atvejus.

Tikrinimo metu nustatyta, kad 5 bendrovės tvarkė asmens duomenis (pvz., kliento vardą, pavardę, adresą (gatvę, miestą), telefono ryšio numerį, įrenginyje esančią informaciją, duomenis apie priimtą prekę, jos gedimus) automatiniu būdu įrenginių garantinio ir po garantinio aptarnavimo paslaugų teikimo tikslu nepranešusios apie tai VDAI, kaip to reikalauja ADTAĮ 31 straipsnis.

Dėl asmens duomenų tvarkymo teisėtumo

ADTAĮ 3 straipsnio 1 dalies 1 punkte numatyta, kad asmens duomenys turi būti renkami apibrėžtais ir teisėtais tikslais ir toliau neturi būti 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 tada, jei reikia, ir tik tokia apimtimi, kuri reikalinga duomenų valdytojo teisėtiems duomenų tvarkymo tikslams.

Tikrinimo metu 2 bendrovėse nustatytas kliento asmens kodo tvarkymas įrenginių garantinio ir po garantinio aptarnavimo paslaugų teikimo tikslu (1 bendrovėje sudaryta galimybė rinkti kliento asmens kodą, neturint tikslo jo tvarkyti automatiniu būdu, o kitos bendrovės dokumentuose reglamentuotas asmens kodo tvarkymas bei teikimas aptarnavimo centrams ir įrenginio gamintojui ar jų įgaliotiems partneriams) neatitinka ADTAĮ 3 straipsnio 1 dalies 1 ir 4 punktuose nustatytų reikalavimų.

Dėl asmens duomenų tvarkymo reglamentavimo

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 priemonėms (toliau – Bendrieji reikalavimai).

Tikrinimo metu nustatyta, kad 3 bendrovės neturi dokumento, reglamentuojančio asmens duomenų tvarkymą garantinio ir po garantinio aptarnavimo paslaugų teikimo tikslu, kaip to reikalauja ADTAĮ 30 straipsnio 1 dalis ir Bendrųjų reikalavimų 8 punktas, o kitų 3 bendrovių dokumentai, reglamentuojantys asmens duomenų tvarkymą, neatitiko ADTAĮ bei Bendrųjų reikalavimų (pvz., nėra reglamentuota įrenginiuose esančios informacijos kopijavimo paslaugos teikimo tvarka, nėra nustatyta kliento įrenginyje esančios informacijos saugojimo tvarka, teikiant klientui jo įrenginyje esančių duomenų išsaugojimo paslaugą: nėra numatyta į kokį įrenginį turi būti perkeliami duomenys, taip pat tokių duomenų saugojimo terminai ir sunaikinimo procedūra ir kt.).

Dėl duomenų subjekto informavimo

ADTAĮ 24 straipsnio 1 dalyje yra nustatyta, 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) Savo (duomenų valdytojo) ir savo atstovo, jeigu šis yra, tapatybę ir nuolatinę gyvenamąją vietą (jeigu duomenų valdytojas ar jo atstovas yra fizinis asmuo) arba nurodyti pavadinimą, juridinio asmens kodą ir buveinę (jeigu duomenų valdytojas ar jo atstovas yra juridinis asmuo);

2) Kokiais tikslais ketinami tvarkyti duomenų subjekto asmens duomenys;

3) Kitą papildomą informaciją, kaip antai, kam ir kokiais tikslais teikiami duomenų subjekto asmens duomenys, kiek jos reikia, kad būtų užtikrintas teisingas asmens duomenų tvarkymas nepažeidžiant duomenų subjekto teisių.

Tikrinimo metu nustatyta, kad 7 bendrovės netinkamai informuoja klientus apie jų asmens duomenų tvarkymą ir klientų duomenų teikimą. Nustatyta, kad klientui nėra pateikiama informacija apie jo asmens duomenų teikimą duomenų gavėjams (t. y. nėra nurodyti konkretūs duomenų gavėjai, duomenų teikimo tikslas, teikiamų asmens duomenų sąrašas ir pan.), taip neužtikrinant duomenų subjektui teikiamos informacijos tikslumo ir teisingumo. Be to, bendrovės nėra sudariusios galimybės klientui išreikšti *savanorišką* sutikimą dėl jo asmens duomenų teikimo, atskirą nuo kitų asmens duomenų tvarkymo tikslų.

Dėl duomenų saugumo priemonių įgyvendinimo

Tikrinimo metu nustatyta, kad 4 bendrovėse įgyvendinamos ne visos organizacinės duomenų saugumo priemonės, užtikrinančios kliento įrenginiuose esančių asmens duomenų saugumą nuo atsitiktinio ar neteisėto atskleidimo, taip pat nuo bet kokio kito neteisėto tvarkymo (pvz., bendrovių dokumentuose numatyta, kad jos neatsako už įrenginyje esančios informacijos saugumą, už taisomoje prekėje esančius asmeninius duomenis ir pan.).

Pastebėtina, kad bendrovei, kaip duomenų valdytojui, tvarkančiam asmens duomenis garantinio ir po garantinio aptarnavimo paslaugų teikimo tikslu, yra nustatyta pareiga įgyvendinti tinkamas duomenų saugumo priemones, nes klientas prieš atiduodamas įrenginį taisyti ne visada gali persikopijuoti įrenginyje esančius asmens duomenis (pvz., įrenginys sugedęs ir neįsijungia).

Dėl asmens duomenų saugojimo termino

Atliekant tikrinimą nustatyta, kad 2 bendrovėse nėra nustatytas ir reglamentuotas asmens duomenų saugojimo terminas, kai duomenys tvarkomi garantinio ir po garantinio aptarnavimo paslaugų teikimo tikslu, 3 bendrovėse nėra nustatytas ir reglamentuotas konkretus perkopijuotų duomenų saugojimo terminas, kai duomenys tvarkomi įrangos garantinio ir po garantinio aptarnavimo tikslu, o tai neatitinka ADTAĮ 30 straipsnio 1 dalies ir Bendrųjų reikalavimų 8.8 punkto bei sudaro sąlygas pažeisti ADTAĮ 4 straipsnį. 1 bendrovėje nustatytas asmens duomenų saugojimo terminas (20 metų) nepagrįstai ilgas nustatytam tikslui pasiekti, o tai prieštarauja 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 įstatymo 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 5 bendrovės, kurios apie tokį asmens duomenų tvarkymą nepranešė VDAI ir pažeidė ADTAĮ 31 straipsnio reikalavimus.

ADTAĮ 14 straipsnio 1 dalyje nurodyta, kad asmens duomenys gali būti tvarkomi tiesioginės rinkodaros tikslais *tik po to, kai duomenų subjektas duoda sutikimą*. Pagal ADTAĮ 2 straipsnio 12 dalį sutikimu laikomas savanoriškas duomenų subjekto valios pareiškimas tvarkyti jo asmens duomenis jam žinomu tikslu. ADTAĮ 14 straipsnio 3 dalis nustato, kad duomenų valdytojas privalo sudaryti aiškią, *nemokamą ir lengvai įgyvendinamą galimybę duomenų subjektui išreikšti sutikimą ar nesutikimą* dėl jo asmens duomenų tvarkymo tiesioginės rinkodaros tikslais.

Tikrinimo metu nustatyta, kad 5 bendrovės nebuvo sudariusios galimybės duomenų subjektui išreikšti atskiro savanoriško sutikimo ar nesutikimo dėl asmens duomenų tvarkymo tiesioginės rinkodaros tikslu ir taip pažeidė ADTAĮ 14 straipsnyje ir ERĮ 69 straipsnyje nustatytus reikalavimus. Nustatyta, kad klientas, pasirašydamas sutartį dėl įrenginio garantinio ar po garantinio paslaugų teikimo, privalėjo sutikti ir su asmens duomenų tvarkymu tiesioginės rinkodaros tikslais. Pažymėtina, kad toks sutikimas yra netinkamas ir neatitinka ADTAĮ 2 straipsnio 12 dalies reikalavimų, kadangi bendrovės nesudaro sąlygų duomenų subjektui išreikšti savanoriško sutikimo/nesutikimo dėl asmens duomenų tvarkymo tiesioginės rinkodaros tikslais, kaip to reikalauja ADTAĮ 14 straipsnio 1 ir 3 dalys.

Visoms bendrovėms pateikti nurodymai pašalinti nustatytus pažeidimus.