



BDAR: naujos galimybės, naujos prievolės



Ką kiekviena **jmonė** turi žinoti apie ES
bendrajį duomenų apsaugos reglamentą

Printed by Bietlot in Belgium

Nei Europos Komisija, nei joks Komisijos vardu veikiantis asmuo nėra atsakingas už toliau pateikiamos informacijos naudojimą.

Liuksemburgas: Europos Sąjungos leidinių biuras, 2018

© Europos Sąjunga, 2018

Pakartotinai naudoti leidžiama nurodžius šaltinį.

Pakartotinio Europos Komisijos dokumentų naudojimo politika reglamentuojama Sprendimu 2011/833/ES (OL L 330, 2011 12 14, p. 39).

Print ISBN 978-92-79-79432-2 doi:10.2838/753721 DS-01-18-082-LT-C

PDF ISBN 978-92-79-79425-4 doi:10.2838/181472 DS-01-18-082-LT-N

TURINYS

SKYRIUS 1.

VERSLO GALIMYBĖ 2

SKYRIUS 2.

KAS YRA BDAR 4

SKYRIUS 3.

JŪSŲ PRIEVOLĖS PAGAL BDAR..... 8

SKYRIUS 4.

AR PASIRENGĘ LAIKYTIS NAUJŲ REIKALAVIMŲ? 18



SKYRIUS 1.



VERSLO GALIMYBĖ

BDAR reglamentuojama, kaip įmonės tvarko ir valdo asmens duomenis. Naujasis teisės aktas įsigalios 2018 m. gegužės 25 d. ir bus taikomas visoms įmonėms ir organizacijoms (pvz., ligoninėms, viešojo administravimo institucijoms ir pan.). Tai yra didžiausias ES duomenų apsaugos taisyklių pakeitimas per daugiau nei 20 metų.

BDAR ne tik suteikia piliečiams galimybę labiau kontroliuoti savo duomenų naudojimą, bet ir gerokai




supaprastina įmonių teisinę aplinką. Tai pasiekama nustatant vienodą duomenų apsaugos teisės aktų sistemą visoje ES. Kitaip tariant, užuot kiekvienai šaliai turėjus savo duomenų apsaugos įstatymus, dabar visoje ES taikomas vienas reglamentas. Taigi, skirtingose šalyse veikiančiai įmonei nebereikia laikytis kelių – dažniausiai skirtingų – teisės aktų. Dabar tam, kad galėtų teikti savo paslaugas bet kur ES, jai reikia laikytis tik BDAR.

Kuo BDAR gali būti naudingas jūsų įmonei

-  **Viena Sąjunga – vienas teisės aktas.** Vienas taisyklių rinkinys leis įmonėms paprasčiau ir pigiau užsiimti verslu ES.
-  **Vieno langelio principas.** Daugeliu atvejų įmonėms reikės bendrauti tik su viena duomenų apsaugos institucija (DAI).
-  **Europos žemėje – europietiškos taisyklės.** ES nepriklausančiose šalyse įsisteigusios įmonės, siūlančios prekes ar paslaugas ES, privalo laikytis tų pačių taisyklių kaip Europos įmonės.
-  **Rizika pagrįstas požiūris.** BDAR vengiama nustatyti apsunkinančią bendrą prievolę. Vietoj to prievolės pritaikomos pagal atitinkamas grėsmes.
-  **Inovacijai tinkamos taisyklės.** BDAR yra technologijų atžvilgiu neutralus teisės aktas.

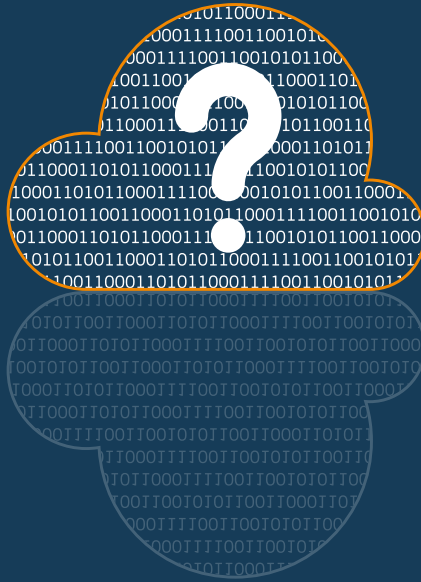
Svarbiausia – pasitikėjimas

Žmonės yra susirūpinę savo asmens duomenų apsauga, todėl jų pasitikėjimas skaitmenine aplinka tebėra mažas. Remiantis „Eurobarometro“ apklausa:

-  8 iš 10 žmonių mano, kad jie negali visapusiškai kontroliuoti savo asmens duomenų;
-  6 iš 10 teigia nepasitikintis internetinėmis įmonėmis;
-  daugiau nei 90 proc. europiečių teigia norintis vienodų teisių į duomenų apsaugą visose ES šalyse.

BDAR suteikia naują galimybę jūsų verslui padidinti vartotojų pasitikėjimą pasitelkiant rizika pagrįstą asmens duomenų valdymą.

„Taigi, įmonės, kurios nesugeba tinkamai apsaugoti asmens duomenų, gali prarasti vartotojų pasitikėjimą, kuris yra būtinas skatinant žmones naudotis naujais gaminiais ir paslaugomis.“



SKYRIUS 2.

KAS YRA BDAR

Ar BDAR taikomas man?

Trumpai tariant, BDAR taikomas **bet kuriai** įmonei, kuri:

tvarko asmens duomenis automatizuotomis arba **neautomatizuotomis** priemonėmis (jeigu duomenys rūšiuojami pagal kriterijus).

Net jeigu jūsų įmonė tvarko duomenis tik kitų įmonių vardu, jums vis tiek reikia laikytis šių taisyklių.

BDAR taikomas, jeigu:

- 📍 jūsų įmonė tvarko asmens duomenis ir yra įsisteigusi ES, nepriklausomai nuo to, kur tvarkomi patys duomenys;
- 📍 jūsų įmonė yra įsisteigusi ES nepriklausančioje šalyje, tačiau siūlo prekes ar paslaugas arba stebi fizinių asmenų elgesį ES.

Kas yra asmens duomenys?

Asmens duomenys yra bet kokia informacija, susijusi su gyvu asmeniu, kurio tapatybė yra arba gali būti nustatyta. Tai gali būti:

- 📍 vardas, pavardė;
- 📍 adresas ir telefono numeris;
- 📍 buvimo vieta;
- 📍 duomenys apie sveikatą;
- 📍 pajamos ir bankininkystės duomenys;
- 📍 kultūriniai prioritetai;
- 📍 ... ir ne tik.

BDAR taikomas ir asmens duomenims, iš kurių pašalinta asmeninė informacija arba kuriems yra suteikti

pseudonimai, bet kuriuos vis tiek galima panaudoti iš naujo nustatant asmens tapatybę. Tačiau asmens duomenys, kurių anonimiškumas užtikrintas taip, kad asmens tapatybė nebegali būti nustatyta, nebelaikomi asmens duomenimis, todėl jiems netaikomas BDAR.

BDAR taip pat yra technologijų atžvilgiu neutralus teisės aktas. Tai reiškia, kad juo apsauga suteikiama asmens duomenims, nepriklausomai nuo naudojamos technologijos ar asmens duomenų saugojimo būdo. BDAR jums taikomas, nesvarbu, ar jūsų įmonė tvarko ir saugo asmens duomenis naudodama sudėtingą IT sistemą ar popierinius failus.

„BDAR jums taikomas, nesvarbu, ar jūsų įmonė tvarko ir saugo asmens duomenis naudodama sudėtingą IT sistemą ar popierinius failus.“

Būkite ypač atsargūs su specialių (neskelbtinų) kategorijų asmens duomenimis

Jeigu tarp jūsų renkamų asmens duomenų yra informacija apie asmens sveikatą, rasę, lytinę orientaciją, religiją, politinius įsitikinimus ar priklausymą profesinėms sąjungoms, šie duomenys laikomi neskelbtiniais. Jūsų įmonė gali tvarkyti šiuos duomenis tik tam tikromis sąlygomis. Jums gali tekti imtis papildomų apsaugos priemonių, kaip antai šifravimo.

Kas yra asmens duomenų tvarkymas?

Remiantis BDAR, į asmens duomenų tvarkymo apibrėžtį patenka tokie veiksmai kaip asmens duomenų rinkimas, naudojimas ir trynimasis.

Stebite savo patalpas per vaizdo stebėjimo kameras? Verslo tikslais naudojate duomenų bazę, kurioje yra asmens duomenų? Siunčiate reklaminius elektroninius

laiškus? Ištrinate (skaitmenines) darbuotojų bylas arba sunaikinate dokumentus? Skelbiate asmenų nuotraukas savo interneto svetainėje arba socialinės žiniasklaidos kanaluose?

Jeigu į kurį nors iš šių klausimų atsakėte „taip“, jūsų įmonė tikrai tvarko asmens duomenis.

Kaip BDAR padeda mažinti išlaidas?

BDAR atsižvelgiama į įmonių poreikius. Pavyzdžiui, reglamentu siekiama panaikinti administracinius reikalavimus, kad sumažėtų išlaidos ir administracinė našta:

- ☝ **nebeliks išankstinių pranešimų.** Reforma panaikinami dauguma išankstinių pranešimų priežiūros institucijoms, o kartu ir su tuo susijusios išlaidos;
- ☝ **duomenų apsaugos pareigūnai.** Įmonėms dažniausiai reikia paskirti DAP, jeigu jų pagrindinė veikla apima neskelbtinų duomenų tvarkymą dideliu mastu arba didelio masto, reguliarią ir sistemingą asmenų stebėseną. Viešojo administravimo institucijos privalo paskirti DAP;

- ☝ **poveikio duomenų apsaugai vertinimai.** Įmonės privalo atlikti poveikio duomenų apsaugai vertinimą, jeigu siūloma duomenų tvarkymo veikla kelia didelį pavojų asmenų teisėms ir laisvėms;
- ☝ **įrašų saugojimas.** Įmonėms, kuriose dirba mažiau kaip 250 darbuotojų, nereikia saugoti įrašų, jeigu duomenų tvarkymas nėra jų įprasta veikla arba nėra susijęs su neskelbtiniais duomenimis.

„Reglamentu siekiama panaikinti administracinius reikalavimus, kad sumažėtų išlaidos ir administracinė našta.“



SKYRIUS 3.

JŪSŲ PRIEVOLĖS PAGAL BDAR

BDAR nustatomos įmonėms taikomos tiesioginės duomenų apsaugos prievolės ES lygmeniu. Remiantis BDAR, įmonė gali tvarkyti asmens duomenis tik tam tikromis sąlygomis. Pavyzdžiui, duomenų tvarkymas turi būti vykdomas sąžiningai ir skaidriai, nurodytu bei teisėtu tikslu ir naudojant tik tuos duomenis, kurių reikia šiam tikslui pasiekti. Jis taip pat turi būti pagrįstas vienu iš šių teisinių pagrindų:

- ☝ atitinkamo asmens **sutikimu**;
- ☝ jūsų ir asmens **sutartyje nustatyta prievole**;
- ☝ **teisine prievole**;
- ☝ siekiama apsaugoti asmens **gyvybinius interesus**;
- ☝ siekiama įvykdyti **užduotį visuomenės intereso labui**;
- ☝ jūsų įmonės **teisėtais interesais**, tačiau tik patikrinus, ar tai neturi didelio poveikio asmens, kurio duomenis tvarkote, pagrindinėms teisėms ir laisvėms. Jeigu asmens teisės yra viršesnės už jūsų interesus, jūs negalite tvarkyti jo asmens duomenų.

Svarbu: kaip gauti sutikimą naudoti asmens duomenis

BDAR numatomos griežtos duomenų tvarkymo remiantis sutikimu taisyklės. Jų tikslas – užtikrinti, kad asmuo suprastų, su kuo jis sutinka. Tai reiškia, kad sutikimas turi būti **laisva valia duotas, konkretus, pagrįstas informacija** ir **vienareikšmis** atsakas į aiškia ir paprasta kalba pateiktą prašymą. Be to, sutikimas turi būti duotas **vienareikšmiu veiksniu**, pavyzdžiui, pažymint žymimąjį langelį internetinėje formoje arba pasirašant formą.

Jeigu remdamiesi sutikimu tvarkote su **vaiku** susijusius asmens duomenis, reikia gauti tėvų sutikimą. Tačiau skirtingose šalyse amžiaus limitas svyruoja nuo 13 iki 16 metų, todėl patartina pasitikslinti nacionaliniuose įstatymuose.

„Nepamirškite! Gavę sutikimą tvarkyti asmens duomenis, tai galite daryti tik tais tikslais, dėl kurių buvo prašoma sutikimo. Be to, privalote suteikti galimybę atšaukti savo sutikimą.“

Nustatykite savo vaidmenį ir atsakomybę

Nustačius, kad BDAR taikomas jūsų verslui ir kad yra tvarkomi asmens duomenys, kitas žingsnis – nustatyti savo vaidmenį.

Duomenų apsaugos taisyklėmis išskiriami duomenų valdytojo ir duomenų tvarkymo vaidmenys – jiems taikomos skirtingos prievolės. Duomenų valdytojas nustato asmens duomenų tvarkymo tikslą ir priemones, o duomenų tvarkytojas tik tvarko asmens duomenis duomenų valdytojo vardu. Tačiau tai nereiškia, kad duomenų tvarkytojas gali slapstyti už duomenų valdytojo.

Pagal BDAR reikalaujama, kad duomenų valdytojas pasitelktų tik tokį duomenų tvarkytoją, kuris suteikia pakankamų garantijų. Šios garantijos turi būti pateiktos duomenų valdytojo ir duomenų tvarkytojo rašytinėje sutartyje. Į sutartį taip pat turi būti įtrauktos įvairios privalomos nuostatos, įskaitant, pavyzdžiui, nuostatą, kad duomenų tvarkytojas tvarko asmens duomenis tik pagal dokumentais pagrįstus duomenų valdytojo nurodymus.

Prievolės, kuriomis saugomos asmenų teisės

BDAR numatoma įvairių prievolių, kuriomis siekiama apsaugoti asmens teisę kontroliuoti savo asmens duomenis.

Jūsų prievolė: skaidrios informacijos pateikimas

Įmonės privalo pateikti asmenims informaciją apie tai, kas, ką ir kodėl tvarko. Reikia aiškiai pateikti bent šią informaciją:

- 👤 kas esate;
- 👤 kodėl tvarkote duomenis;
- 👤 koks yra teisinis pagrindas;
- 👤 kas gaus duomenis (jeigu taikytina).

Tam tikrais atvejais taip pat reikia nurodyti:

- 👤 DAP kontaktinius duomenis;
- 👤 teisėtą interesą (kai teisėtas interesas yra duomenų tvarkymo teisinis pagrindas);
- 👤 duomenų perdavimo ES nepriklausančiai šaliai pagrindą;
- 👤 kiek laiko duomenys bus saugomi;
- 👤 asmens teises į duomenų apsaugą (t. y. teisę susipažinti su duomenimis, juos taisyti, ištrinti, apriboti jų naudojimą, nesutikti su duomenų tvarkymu, teisę į duomenų perkeliamumą ir pan.);
- 👤 kaip atšaukti savo sutikimą (jeigu duomenys tvarkomi sutikimo pagrindu);
- 👤 ar yra kokia nors įstatymais numatyta ar sutartinė prievolė pateikti duomenis;
- 👤 informaciją apie sprendimo logiką, svarbą ir pasekmes, jeigu sprendimas priimamas automatizuotomis priemonėmis.

„Įmonės privalo pateikti asmenims informaciją apie tai, kas, ką ir kodėl tvarko.“

Jūsų prievolė: teisė susipažinti su duomenimis ir teisė į duomenų perkeliamumą

Asmenys turi teisę reikalauti nemokamai ir prieinama forma susipažinti su savo asmens duomenimis. Gavę tokį prašymą turite:

- ☝ informuoti asmenį, ar tvarkote jo asmens duomenis;
- ☝ pateikti informaciją apie duomenų tvarkymą (kaip antai duomenų tvarkymo tikslą, atitinkamų asmens duomenų kategorijas, duomenų gavėjus ir pan.);
- ☝ pateikti tvarkomų asmens duomenų kopiją.

Be to, jeigu duomenys yra tvarkomi remiantis sutikimu ar sutartimi, asmuo gali prašyti grąžinti jo asmens duomenis arba perduoti juos kitai įmonei. Tai vadinama teise į duomenų perkeliamumą. Duomenys turi būti pateikti dažnai naudojamu kompiuterio skaitomu formatu.

Nors šios dvi teisės yra glaudžiai susijusios, jos nėra tapačios. Taigi, privalote pasirūpinti, kad šios teisės nebūtų painiojamos, ir atitinkamai informuoti asmenį.

Jūsų prievolė: teisė ištrinti duomenis (teisė būti pamirštam)

Tam tikromis aplinkybėmis asmuo gali reikalauti, kad duomenų valdytojas ištrintų jo asmens duomenis, pavyzdžiui, kai duomenys nebėra reikalingi duomenų tvarkymo tikslui pasiekti. Tačiau jūsų įmonė neprivalo vykdyti tokio asmens reikalavimo, jeigu:

- ☝ tvarkyti duomenis yra būtina, kad būtų užtikrinta asmens žodžio ir informacijos laisvė;
- ☝ asmens duomenis turite tvarkyti, kad įvykdytumėte savo teisinę prievolę;
- ☝ yra kitų su viešuoju interesu susijusių priežasčių saugoti asmens duomenis, kaip antai visuomenės sveikata ar moksliniai ir istoriniai tyrimai;
- ☝ asmens duomenis turite tvarkyti, kad galėtumėte pareikšti teisinį reikalavimą.

Jūsų prievolė: teisė ištaisyti duomenis ir teisė nesutikti




Jeigu asmuo mano, kad jo asmens duomenys yra neteisingi, neišsamūs ar netikslūs, jis turi teisę prašyti juos ištaisyti arba papildyti be nepagrįsto delsimo.

Asmuo taip pat gali bet kada nesutikti, kad jo asmens duomenys būtų tvarkomi konkrečiu tikslu, kai jūsų įmonė juos tvarko remdamasi savo teisėtu interesu arba

vykdydama užduotį viešojo intereso labui. Jeigu jūsų teisėtas interesas nėra viršesnis už asmens interesą, privalote nutraukti jo asmens duomenų tvarkymą. Panašiai asmuo gali reikalauti apriboti savo asmens duomenų tvarkymą, kol nenustatyta, ar jūsų teisėtas interesas viršija jo interesą. Tačiau tiesioginės rinkodaros atveju jūs visada turite nutraukti asmens duomenų tvarkymą, jeigu to reikalauja atitinkamas asmuo.

Patarimas dėl automatizuoto sprendimų priėmimo, įskaitant profiliavimą

Asmenys turi teisę reikalauti, kad jiems nebūtų taikomas tik automatizuotu duomenų tvarkymu grindžiamas sprendimas. Tačiau ši taisyklė turi kelias išimtis, pavyzdžiui, kai asmuo aiškiai sutinka, kad būtų priimtas automatizuotas sprendimas. Išskyrus atvejus, kai automatizuotas sprendimų priėmimas yra grindžiamas įstatymu, jūsų įmonė privalo:

-  informuoti asmenį apie automatizuotą sprendimų priėmimą;
-  suteikti asmeniui teisę prašyti, kad automatizuotomis priemonėmis priimtą sprendimą peržiūrėtų žmogus;
-  suteikti asmeniui galimybę ginčyti automatizuotomis priemonėmis priimtą sprendimą.

Pavyzdžiui, jeigu bankas automatizuotomis priemonėmis priima sprendimą dėl paskolos suteikimo tam tikram asmeniui, tas asmuo turi būti informuotas apie automatizuotą sprendimo priėmimą ir jam turi būti suteikta galimybė ginčyti tokį sprendimą bei reikalauti žmogaus įsikišimo.




Rizika grindžiamos prievolės

Be prievolių, kuriomis siekiama apsaugoti asmens teises, BDAR taip pat numatoma įvairių prievolių, kurių taikymas priklauso nuo keliamos rizikos.

Jūsų prievolė: duomenų apsaugos pareigūno (DAP) paskyrimas

DAP stebi, kaip laikotės BDAR nuostatų. Viena pagrindinių DAP užduočių yra informuoti darbuotojus, kurie tvarko asmens duomenis, apie jų prievoles ir konsultuoti juos šiais klausimais. DAP taip pat bendradarbiauja su DAI ir atlieka kontaktinio asmens funkcijas bendraujant su DAI ir fiziniiais asmenimis.

Jūsų įmonė turi paskirti DAP, jeigu:

-  reguliariai ar sistemingai stebite asmenis arba tvarkote specialių kategorijų duomenis;
-  duomenų tvarkymas yra jūsų pagrindinė veikla;
-  tai darote dideliu mastu.

Pavyzdžiui, jeigu tvarkote asmens duomenis dėl reklamos paieškos sistemose pagal žmonių elgesį internete, BDAR numatoma pareiga paskirti DAP. Tačiau, jeigu savo klientams siunčiate reklaminę medžiagą tik kartą per metus, DAP jums nebūtinai. Panašiai, jeigu esate gydytojas, kuris renka duomenis apie pacientų sveikatą, jums greičiausiai nereikia DAP. Tačiau, jeigu tvarkote ligoninei skirtus asmens duomenis apie genetiką ir sveikatą, DAP turite paskirti.

Jūsų prievolė: pritaikytoji ir standartizuotoji duomenų apsauga

BDAR pristatomi du nauji principai: pritaikytoji duomenų apsauga ir standartizuotoji duomenų apsauga.

Pritaikytoji duomenų apsauga padeda užtikrinti, kad įmonė, planuodama naują asmens duomenų tvarkymo būdą, į duomenų apsaugą atsižvelgtų jau ankstyvuosiuose etapuose. Remiantis šiuo principu, duomenų valdytojas turi imtis visų reikalingų techninių ir organizacinių priemonių, kad įgyvendintų duomenų apsaugos principus ir apsaugotų asmenų teises. Viena iš tokių priemonių gali būti, pavyzdžiui, pseudonimų suteikimas.

Pritaikytoji duomenų apsauga mažina su privatumu susijusius pavojus ir didina pasitikėjimą. Įmonė, kuri kurdama naujas prekes ar paslaugas iš karto atsižvelgia į duomenų apsaugą, gali jau ankstyvuosiuose etapuose išvengti galimų duomenų apsaugos problemų. Be to, tokia praktika padeda didinti informuotumą apie duomenų apsaugą visuose įmonės skyriuose ir visais jos lygmenimis.

Standartizuotoji duomenų apsauga padeda užtikrinti, kad numatytuose nustatymuose jūsų įmonė visada pasirinktų labiausiai privatumą apsaugančius parametrus. Pavyzdžiui, jeigu galimi du privatumo parametrai ir vienas iš jų neleidžia kitiems susipažinti su jūsų asmens duomenimis, būtent šis parametras turėtų būti numatytasis.

„Pritaikytoji duomenų apsauga mažina su privatumu susijusius pavojus ir didina pasitikėjimą.“

„Standartizuotoji duomenų apsauga padeda užtikrinti, kad numatytuose nustatymuose jūsų įmonė visada pasirinktų labiausiai privatumą apsaugančius parametrus.“

Jūsų prievolė: tinkamas pranešimas apie duomenų saugumo pažeidimą

Duomenų saugumas yra pažeidžiamas, kai asmens duomenys, už kuriuos jūs atsakote, yra netyčia arba neteisėtai atskleidžiami leidimo neturintiems gavėjams arba yra laikinai nepasiekiami ar pakeičiami.

Labai svarbu, kad įmonė imtųsi tinkamų techninių ir organizacinių priemonių, siekdama išvengti galimų

duomenų saugumo pažeidimų. Tačiau, jeigu duomenų saugumo pažeidimas kelia pavojų asmens teisėms ir laisvėms, turite apie jį pranešti savo DAI per 72 valandas nuo sužinojimo apie tokį pažeidimą.

Priklausomai nuo to, ar duomenų saugumo pažeidimas kelia *didelį* pavojų susijusiems asmenims, įmonei taip pat gali tekti informuoti visus asmenis, nukentėjusius nuo tokio duomenų saugumo pažeidimo.

Asmens duomenys siunčiami už ES ribų?

BDAR yra taikomas Europos ekonominėje erdvėje (EEE), kurią sudaro visos ES šalys, taip pat Islandija, Lichtenšteinas ir Norvegija. Jeigu asmens duomenys siunčiami už EEE ribų, BDAR taikoma apsauga keliauja kartu su duomenimis. Tai reiškia, kad įmonės, eksportuodamos duomenis į užsienį, privalo užtikrinti tam tikras saugumo priemones.

BDAR numatomi įvairūs mechanizmai, taikomi duomenų perdavimui į trečiąsias šalis. Remiantis BDAR, toks duomenų perdavimas leidžiamas, kai:

1. ES laikoma, kad atitinkamos šalies apsauga yra pakankama;
2. jūsų įmonė, pavyzdžiui, imasi reikalingų priemonių, kad užtikrintų tinkamas saugumo priemones, kaip antai įtraukia specialias nuostatas į sutartis su asmens duomenų importuotoju iš ES nepriklausančios šalies;
3. jūsų įmonė, pavyzdžiui, remiasi konkrečiais duomenų perdavimo pagrindais (vadinamosiomis nukrypti leidžiančiomis nuostatomis), kaip antai asmens sutikimu.

Daugiau informacijos apie tarptautiniam duomenų perdavimui taikomas taisykles pateikiama Europos Komisijos komunikate „Keitimasis asmens duomenimis ir jų apsauga globalizuotame pasaulyje“: <http://eur-lex.europa.eu/legal-content/lt/TXT/HTML/?uri=CELEX:52017DC0007&from=lt>.

Ar reikia atlikti poveikio duomenų apsaugai vertinimą (PDAV)?

PDAV yra privalomas, kai dėl numatomo duomenų tvarkymo gali kilti didelis pavojus asmenų teisėms ir laisvėms, pavyzdžiui, kai naudojamos naujos technologijos.

Remiantis BDAR, didelis pavojus kyla bent šiais atvejais:

- 🔴 automatizuoto duomenų tvarkymo ir profiliavimo mechanizmai naudojami sistemingam ir plačiam asmenų vertinimui;
- 🔴 viešoji erdvė yra sistemingai stebima dideliu mastu (pvz., vaizdo stebėjimo kameromis);
- 🔴 neskelbtini duomenys (pvz., duomenys apie sveikatą) tvarkomi dideliu mastu.

PDAV tikslas – nustatyti galimus pavojus asmenų teisėms ir laisvėms, kol asmens duomenys dar nepradėti tvarkyti ir nekilo pavojus. Iš anksto sumažinus pavojų galima išvengti žalos ir sumažinti išlaidas.

Jeigu PDAV nurodytomis priemonėmis nepavyksta pašalinti visų nustatytų didelių pavojų, prieš pradėdant vykdyti numatomą duomenų tvarkymo veiklą būtina pasitarti su DAI.

**„PDAV yra privalomas,
kai dėl numatomo
duomenų tvarkymo gali kilti
didelis pavojus asmenų teisėms
ir laisvėms.“**

Ką turite padaryti

Atsakyti į prašymus

Jeigu jūsų įmonė gauna asmens, kuris nori pasinaudoti savo teisėmis, prašymą, turite į jį atsakyti nepagrįstai nedelsdami, per vieną mėnesį nuo prašymo gavimo. Atsakymo terminas gali būti pratęstas iki dviejų mėnesių, jeigu gautas sudėtingas arba ne vienas prašymas, tačiau apie tokį pratęsimą asmeniui būtina pranešti. Be to, prašymai patenkinami **nemokamai**. Jeigu prašymą atmetate, turite asmenį informuoti apie atmetimo priežastis ir jo teisę pateikti skundą DAI.

Įrodyti, kad atitinkate reikalavimus ir saugote įrašus!

Vienas pagrindinių BDAR principų yra užtikrinti, kad įmonės gali įrodyti savo atitiktį reikalavimams. Tai reiškia, kad turite įrodyti, kad jūsų įmonė veikia pagal BDAR nuostatas ir vykdo visas taikytinas prievoles, visų pirma gavusi DAI prašymą arba DAI patikros metu.

Vienas iš būdų tai padaryti yra saugoti išsamius įrašus, kuriuose, pavyzdžiui, nurodyta ši informacija:

- 👤 duomenis tvarkančios įmonės pavadinimas ir kontaktiniai duomenys;
- 👤 asmens duomenų tvarkymo priežastis (-ys);
- 👤 asmens duomenis teikiančių asmenų kategorijų aprašymas;
- 👤 asmens duomenis gaunančių organizacijų kategorijos;
- 👤 asmens duomenų perdavimas kitai šaliai ar organizacijai;
- 👤 asmens duomenų saugojimo laikotarpis;
- 👤 asmens duomenų tvarkymo metu naudojamos apsaugos priemonės, jeigu tokių yra.

Be to, jūsų įmonė taip pat turėtų nustatyti ir reguliariai atnaujinti rašytines procedūras bei gaires, taip pat su jomis supažindinti savo darbuotojus.



SKYRIUS 4.

AR PASIRENGĘ LAIKYTI NAUJŲ REIKALAVIMŲ?

BDAR paliekama apsisprendimo teisė dėl asmens duomenų tvarkymo. Pirmasis žingsnis yra nustatyti savo dabartinę duomenų tvarkymo veiklą ir dar kartą įvertinti savo vidaus veiklos procesus. Visų pirma, reikia:

- ☀️ nustatyti, kokius duomenis turite, kokiu tikslu ir kokiu teisiniu pagrindu;
- ☀️ įvertinti visas esamas sutartis, visų pirma tarp duomenų valdytojų ir duomenų tvarkytojų;
- ☀️ įvertinti visas vietas, kurioms duomenys perduodami tarptautiniu lygmeniu;

☀️ peržiūrėti savo įmonės bendrą valdymą (t. y. kokių IT ir organizacinių priemonių imatės), įskaitant tai, ar turite arba norite paskirti duomenų apsaugos pareigūną.

Šiame procese svarbu pasirūpinti, kad tokiose peržiūrose dalyvautų įmonės aukščiausi vadovai, kurie teiktų informaciją, nuolat atnaujintų duomenų politiką ir konsultuotų dėl jos pakeitimų.

Tvarkote duomenis ne vienoje šalyje?

Tarpvalstybinio duomenų perdavimo atveju kompetentinga institucija gali būti ne jūsų nacionalinė DAI, o kitos šalies priežiūros institucija. Paprastai tai yra

ES šalies, kurioje yra jūsų įmonės pagrindinė buveinė (priimanti sprendimus dėl duomenų tvarkymo priemonių ir tikslų), DAI.

Kai nesilaikoma reikalavimų

Už BDAR nuostatų pažeidimą gali būti taikomos didelės baudos, už kai kuriuos pažeidimus – iki 20 milijonų eurų arba 4 proc. jūsų įmonės bendros metinės pasaulinės apyvartos. DAI gali taikyti papildomas taisomąsias priemones, kaip antai nurodyti nutraukti asmens duomenų tvarkymą. Taip pat turėtumėte pagalvoti apie žalą reputacijai, kurią patirtumėte nesilaikydami nustatytų reikalavimų.

Žinoma, išlaidos, patiriamos pažeidus BDAR nuostatas, yra daug didesnės nei investicijos, kurių reikėtų, kad jų laikytumėtės.



Turite klausimų? Abejonių? Susisieki su savo nacionaline DAI.

Raskite savo nacionalinę duomenų apsaugos instituciją internete

http://ec.europa.eu/justice/data-protection/article-29/structure/data-protection-authorities/index_en.htm

SVARBUS PRANEŠIMAS

Šioje brošiūroje pateikiama informacija ir patarimai padės geriau suprasti ES duomenų apsaugos taisykles.

Tai yra tik konsultacinė priemonė – teisinę galią turi tik Bendrojo duomenų apsaugos reglamento (BDAR) tekstas. Tik BDAR yra nustatomos privačių asmenų teisės ir pareigos. Ši konsultacinė priemonė nesukuria jokių vykdytinų teisių ar lūkesčių.

Privalomas ES teisės aktų aiškinimas yra Europos Sąjungos Teisingumo Teismo išimtinė kompetencija. Šiose gairėse išreikštos nuomonės neturi įtakos galimai Komisijos pozicijai Teisingumo Teisme.

Nei Europos Komisija, nei joks jos vardu veikiantis asmuo nėra atsakingi už brošiūroje pateiktos informacijos panaudojimą.

Kadangi šioje brošiūroje atspindėta jos rengimo metu buvusi padėtis, ją reikėtų laikyti „gyvuoju dokumentu“, kuris gali būti tobulinamas ir kurio turinys gali būti keičiamas be įspėjimo.

Kaip susisiekti su ES

Asmeniškai

Visoje Europos Sąjungoje yra šimtai Europe Direct informacijos centrų. Artimiausio centro adresą rasite svetainėje https://europa.eu/european-union/contact_lt

Telefonu arba el. paštu

Europe Direct tarnyba atsakys į jūsų klausimus apie Europos Sąjungą. Su šia tarnyba galite susisiekti:

- nemokamu numeriu: 00 800 6 7 8 9 10 11 (kai kurie operatoriai už šiuos skambučius gali imti mokestį),
- šiuo standartiniu numeriu: +32 22999696 arba
- elektroniniu paštu svetainėje https://europa.eu/european-union/contact_lt

Kaip rasti informacijos apie ES

Internetas

Informacijos apie Europos Sąjungą visomis oficialiosiomis ES kalbomis galima rasti svetainėje Europa (https://europa.eu/european-union/index_lt)

ES leidiniai

Nemokamų ir mokamų ES leidinių galite atsisiųsti arba užsisakyti svetainėje EU Bookshop (<https://publications.europa.eu/bookshop>). Jeigu jums reikia daugiau nemokamų leidinių egzempliorių, kreipkitės į Europe Direct arba į vietos informacijos centrą (žr. https://europa.eu/european-union/contact_lt)

ES teisė ir susiję dokumentai

Norėdami susipažinti su ES teisine informacija, įskaitant visus ES teisės aktus nuo 1952 m. visomis oficialiosiomis kalbomis, apsilankykite svetainėje EUR-Lex (<http://eur-lex.europa.eu>)

ES atvirieji duomenys

ES atvirųjų duomenų portale (<http://data.europa.eu/euodp/lt>) galima susipažinti su ES duomenų rinkiniais. Duomenis galima nemokamai parsisiųsti ir pakartotinai naudoti tiek komerciniais, tiek nekomerciniais tikslais.

Bendrujų duomenų apsaugos reglamentu (BDAR) reglamentuojama, kaip įmonės tvarko ir valdo asmens duomenis. Dabar jūsų įmonei reikia laikytis tik vieno Europos duomenų apsaugos teisės akto, jeigu siūlote prekes ar paslaugas bet kurioje ES šalyje.

BDAR yra supaprastinama įmonių reguliavimo aplinka, todėl jūsų įmonei suteikiama nauja galimybė pagerinti asmens duomenų valdymą ir taip padidinti vartotojų pasitikėjimą savo verslu.

Šioje brošiūroje pabrėžiamos jūsų įmonės prievolės pagal BDAR.

europa.eu/dataprotection/lt

