

ES BENDRASIS DUOMENŲ APSAUGOS REGLAMENTAS (GDPR)

Viskas, ką turite žinoti, viename puslapyje

Kas yra GDPR?

Angl. *General Data Protection Regulation – GDPR*.

Naujas teisės aktas, kuris nuo 2018 m. gegužės 25 d. numato, kaip rinkti, naudoti ir saugoti informaciją apie žmones Europos Sąjungoje.

Ar man svarbus GDPR?

Taip, jeigu Jūsų bendrovė ar įstaiga renka, naudoja ar saugo bet kokią informaciją apie klientus, darbuotojus, tarnautojus, piliečius, reklamos adresatus, interneto puslapio lankytojus, interesus, pacientus, studentus, kitus žmones ar naudoja vaizdo kameras.

Kokia rizika nesilaikant GDPR?

Baudos iki 20 milijonų eurų arba 4% metinės pasaulinės apyvartos.

Ką reiškia laikytis GDPR?

- Vadovautis duomenų naudojimo principais (apibrėžti, kodėl naudojate duomenis, naudoti kuo mažiau duomenų, saugoti duomenis kuo trumpiau, turėti teisinį pagrindą duomenimis, užtikrinti, kad duomenys būtų saugūs iš techninės pusės, kt.) – už tai atsakingi visi Jūsų darbuotojai
- Laikytis procedūrų (nagrinėti žmonių prašymus dėl jų duomenų, duomenų saugumo pažeidimus, kam atskleidžiate duomenis, teikti žmonėms informaciją apie tai, kaip naudojate jų duomenis, atlikti poveikio duomenų apsaugai vertinimus, kt.) – tai duomenų apsaugos pareigūno ar kt. specialisto atsakomybė

Kas naujo GDPR?

- **Duomenų apsaugos pareigūnas:** dauguma bendrovių ir įstaigų turi paskirti darbuotoją ar pasisamdyti išorės ekspertą, kurie padėtų laikytis GDPR
- **Pranešimai apie duomenų saugumo pažeidimus:** nutekėjus duomenims ar įvykus incidentui, turite skubiai informuoti priežiūros instituciją ir nukentėjusius žmones.
- **Poveikio duomenų apsaugai vertinimas:** diegdami IT sistemas ar planuodami naują veiklą, turite patikrinti, ar ta sistema ar veikla atitinka GDPR reikalavimus.
- **Griežtesni reikalavimai sutikimams:** nebegalite imti iš žmonių sutikimų dėl jų duomenų naudojimo, jeigu tie žmonės negali laisvai pasirinkti, ar sutikimą duoti.
- **Griežtesni reikalavimai paslaugų teikėjams:** turite griežčiau kontroliuoti, kaip su jūsų duomenimis elgiasi IT, apskaitos, rinkodaros, finansinių ir kitus paslaugų teikėjus, sudaryti su jais griežtas sutartis.
- **Duomenų perkeliamumas:** jei gausite tokį prašymą, turėsite iš savo sistemų žmonėms patogiu formatu išeksportuoti žmonėms informaciją, kurią gavote iš jų.
- **Duomenų tvarkymo veiklos įrašai:** turite vesti jūsų naudojamų ir saugomų duomenų registrą ir jame aprašyti, kokius ir kaip duomenis naudojate.
- **Išankstinės konsultacijos su priežiūros institucija:** jei matysite, kad jūsų diegiamos IT sistemos arba procesai kelia riziką duomenims, turėsite kreiptis į Valstybinę duomenų apsaugos inspekciją patarimo.
- **Vieno langelio priežiūra:** tarptautinės bendrovių grupės paprastai gali bendrauti su priežiūros institucija tik vienoje Europos Sąjungos narėje.
- **GDPR turi laikytis ir ne Europos Sąjungos bendrovės:** tais atvejais, kai pardavinėja prekes ir paslaugas Europos Sąjungoje esantiems žmonėms arba juos seka.

Kaip galiu įgyvendinti GDPR?

- Atlikti auditą, kaip Jūsų įmonė ar įstaiga atitinka GDPR reikalavimus
- Pasitvirtinti procedūras bei dokumentus, reikalingus pagal GDPR
- Paskirti duomenų apsaugos pareigūną ar kt. specialistą
- Apmokyti personalą apie tai, kaip laikytis GDPR

Kas gali padėti įgyvendinti GDPR?

DATAISTIC – atitiktis GDPR paslaugų bendrovė.