Mėnesinis informacinio saugumo naujienlaiškis kompiuterių naudotojams

BDAR

Apžvalga

Tikriausiai esate ką nors girdėję apie naują įstatymą, dar vadinamą trumpiniu BDAR, kuris reiškia „Bendrasis duomenų apsaugos reglamentas“. Tai Europos Sąjungos įstatymas, kuris įsigalios 2018 m. gegužės 25 d. Jis galios bet kuriai organizacijai, tvarkančiai bet kurio Europos Sąjungoje (ES) gyvenančio fizinio asmens duomenis, nepriklausomai nuo to, kurioje pasaulio vietoje ta organizacija bebūtų. BDAR reikalauja, kad organizacijos išlaikytų bet kurio ES gyvenančio fizinio asmens duomenų privatumą ir saugumą. Siekiant užtikrinti BDAR laikymąsi, reikia suprasti ir įgyvendinti pagrindinius principus.

Žmonės turi teisę į privatumą. Organizacijos turi gerbti jų privatumą, apribodamos renkamus ir tvarkomus jų asmens duomenis bei užtikrindamos tų duomenų apsaugą. Įsipareigojimai saugoti privatumą galioja bet kokiai informacijai, tiek naudojamai atskirai, tiek su kita informacija, pagal kurią būtų galima nustatyti Europos Sąjungoje gyvenančio atskiro asmens tapatybę. Tai gali būti tokia informacija kaip adresai, pasų numeriai, vairuotojo pažymėjimų numeriai, finansiniai duomenys, biometriniai duomenys, narystės Sąjungoje, sveikatos istorija, vietos nustatymo duomenys arba informacija, susijusi su asmens seksualine, religine arba politine orientacija. Reglamentas yra taikomas „fiziniam asmeniui“, kuris reiškia gyvą asmenį. Štai keletas pagrindinių BDAR principų, kuriais reikėtų vadovautis:

Fizinių asmenų duomenys turėtų būti tvarkomi teisėtu, sąžiningu ir skaidriu būdu.

Žmonės turėtų būti informuojami, kokia informacija yra renkama ir kokiais tikslais.

Asmens duomenys turi būti renkami nustatytais, aiškiai apibrėžtais bei teisėtais tikslais. Jie neturėtų būti naudojami dėl jokių kitų priežasčių, kurios prieštarauja šiems tikslams.

Asmens duomenys turi būti laikomi ir tvarkomi ne ilgiau, nei tai yra būtina tais tikslais.

Asmens duomenys privalo būti atnaujinami ir tikslūs.

Žmonės turi teisę gauti savo duomenų kopiją arba gali reikalauti, kad jų asmens duomenys daugiau nebebūtų naudojami, arba kai kuriais atvejais būtų visiškai ištrinti.

Organizacijos privalo įgyvendinti tinkamas saugumo priemones, skirtas apsaugoti, kad asmens duomenys nebūtų netyčia ar neteisėtai sunaikinti arba netyčia prarasti, pakeisti ar neleistinai atskleisti.

Be to, organizacijos turi užtikrinti, kad visi asmens duomenis tvarkantys darbuotojai būtų tinkamai išmokyti, kaip tokius duomenis saugoti ir apsaugoti.

Apsaugos priemonėmis, kuriomis siekiama apsaugoti asmens duomenis, privaloma užtikrinti duomenų slaptumo pobūdį atitinkantį apsaugos lygį. Didėjant su duomenimis susijusiai rizikai, turėtų būti didinamos ir duomenų apsaugai dedamos pastangos bei skiriamos išlaidos. Šias priemones reikėtų nuolat peržiūrėti ir atitinkamai atnaujinti. Tinkamai dokumentuoti įrašai apie privatumo ir saugumo sprendimus bei priemones padeda įrodyti, jog šių reikalavimų yra laikomasi. Be to, organizacijos yra teisiškai įpareigotos naudoti tokias priemones, kaip sutartys ir deramo patikrinimo peržiūros, skirtos apsaugoti asmens duomenis, kai jie yra perduodami išorinėms trečiosioms šalims, o ypač šalims, kurios nepriklauso Europos Sąjungai. Galiausiai, pažeidus asmens duomenis, organizacijos turi apie pažeidimą pranešti per 72 valandos nuo jo sužinojimo. Organizacijoms, nesilaikančioms BDAR, gali būti taikomos baudos, siekiančios iki 4 % jų pasaulinės apyvartos, todėl BDAR yra laikomas vienas iš finansiškai brangiausių pasaulio reglamentų.

Kviestinė redaktorė

Brian Honan *yra Dubline (Airija) įkurtos nepriklausomos konsultacinės kibernetinio saugumo ir duomenų apsaugos firmos „BH Consulting“ generalinis direktorius. Brian yra dirbęs Europolo kibernetinio nusikalstamumo centro (EC3) specialiuoju patarėju, yra Airijos pirmosios kompiuterinių incidentų tyrimų tarnybos (CERT) įkūrėjas bei keletą metų dalyvauja keleto novatoriškų saugumo bendrovių patariamosios valdybos veikloje.“Brian veiklą galite stebėti adresu* www.linkedin.com/in/brianhonan arba „Twitter“ paskyroje @brianhonan.

Šaltiniai

BDAR apžvalga fiziniams asmenims ir organizacijoms: http://gdprandyou.ie

BDAR reglamentas: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016R0679

OUCH! vertimai ir archyvai: https://www.sans.org/u/D88