SANS SECURITY AWARENESS

Ikmēneša informācijas drošības biļetens ikvienam

Vispārīgā datu aizsardzības regula (GDPR)

Ievads

Iespējams esat dzirdējuši par jauno regulējumu – vispārīgo datu aizsardzības regulu (GDPR). To ir sagatavojusi Eiropas Savienība un tas stājas spēkā 2018.gada 25.maijā. GDPR ir piemērojama visām organizācijām, kas apstrādā Eiropas savienības iedzīvotāja personas datus, neatkarīgi no tā, kur atrodas organizācija. GDPR paredz, ka organizācija aizsargā ES iedzīvotāju personas datu privātumu un drošību. Lai nodrošinātu regulas prasības, nepieciešams izprast un ieviest pamatprincipus.

Cilvēkiem ir tiesības uz privātumu. Organizācijām jārespektē personas privātums, ierobežojot to, kādus personas datus tās ievāc un apstrādā, kā arī jānodrošina to pienācīga aizsardzība. Privātuma prasības attiecas uz jebkādu informāciju, kas pati par sevi vai kopā ar citu informāciju ļautu identificēt individuālu personu, kas dzīvo Eiropas Savienībā – piemēram, adreses, pases numuri, vadītāja apliecību numuri, finanšu informācija, biometrija, arodbiedrību dalība, medicīniskā vēsture, atrašanās vietas dati vai informācija par personas seksuālo, reliģisko vai politisko orientāciju. Regula attiecas uz fizisku personu - dzīvu indivīdu. Te ir daži galvenie GDPR aspekti, ko būtu jāievēro:

Personas dati jāapstrādā likumīgi, godīgi un caurspīdīgā veidā.

Cilvēkiem ir jāzina, kādi dati tiek ievākti un kādam mērķim.

Personas dati ir jāievāc specifiskiem, noteiktiem un likumīgiem mērķiem. Tos nedrīkst izmantot veidos, kas neatbilst šiem mērķiem.

Personas datus jāuzglabā un jāapstrādā tik ilgi, cik nepieciešams šim mērķim, un ne ilgāk.

Personas dati ir jāuztur precīzi un aktuāli.

Cilvēkiem ir tiesības saņemt viņu datu kopiju vai pieprasīt, lai datus turpmāk neizmanto, vai atsevišķos gadījumos, lai tos izdzēš.

Organizācijām jāievieš atbilstoši drošības risinājumi, lai aizsargātu datus pret nelikumīgu vai nejaušu iznīcināšanu, pazaudēšanu, izmainīšanu vai noplūdi.

Papildus orgnaizācijām ir jānodrošina atbilstoša personāla apmācība, lai darbnieki, kas apstrādā datus, zinātu, kā tos pareizi apstrādāt un aizsargāt.

Aizsardzības pasākumiem jāatbilst datu sensitivitātes pakāpei. Palielinoties ar datiem saistītajam riskam, attiecīgi jāpalielina arī pūles un izdevumi datu atbilstošai aizsardzībai. Aizsardzības pasākumus regulāri jāpārskata un jāatjauno. Pietiekami dokumentēti pieraksti par privātuma un drošības lēmumiem var palīdzēt pierādīt atbilstību regulas prasībām. Papildu organizācijām ir juridisks pienākums īstenot pasākumus, piemēram, līgumus un auditus, lai aizsargātu datus gadījumos, kad tie tiek nodoti trešajām pusēm vai īpaši organizācijām ārpus Eiropas Savienības. Visbeidzot gadījumā, ja notiek incidents saistībā ar personas datiem, organizācijai par to jāziņo ne vēlāk kā 72 stundu laikā pēc tam, kad tā par incidentu ir uzzinājusi. GDPR prasību pārkāpums var tikt sodīts ar soda naudu līdz par 4% apmērā no organizācijas globālajiem ienākumiem, tādejādi GDPR ir potenciāli finansiāli visdārgākais globālais regulējums.

CERT.LV ir Latvijas Republikas Informācijas tehnoloģiju drošības incidentu novēršanas institūcija. CERT.LV misija ir veicināt informācijas tehnoloģiju drošību Latvijā. Uzziniet vairāk https://www.cert.lv vai sekojiet mums Twiterī @certlv.

Viesredaktors

Brian Honan *ir BH Consulting izpilddirektors, BH Consulting ir Dublinā bāzēta kiberdrošības un datu aizsardzības konsultāciju firma. Brian ir konsultējis Eiropas Kibernoziedzības Centru, ir Īrijas pirmā CERTa dibinātājs un darbojas vairāku drošības kompāniju padomēs. "Brian var atrast* www.linkedin.com/in/brianhonan vai Twitter @brianhonan .

Resursi

GDPR Idivīdiem un organizācijām:	http://gdprandyou.ie
GDPR regulējums:	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016R0679
OUCH! Tulkojumi un arhīvs:	https://www.sans.org/u/D88

Redakcija: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley | Tulkojums: Edgars Tauriņš