SANS SECURITY AWARENESS

Mesečni bilten za podizanje svesti o bezbednosti informacija

GDPR - Opšta uredba o zaštiti podataka o ličnosti

Pregled uredbe

Možda ste već čuli za novu regulativu pod nazivom GDPR ili Opšta uredba o zaštiti podataka o ličnosti (eng. General Data Protection Regulation). Ovaj zakon je izradila i usvojila Evropska unija i on počinje da se primenjuje 25. maja 2018. godine. GDPR se primenjuje na svaku organizaciju koja obrađuje podatke o ličnosti bilo kog stanovnika (rezidenta) u Evropskoj uniji (EU), bez obzira na to gde u svetu je sedište te organizacije. GDPR zahteva da organizacije čuvaju privatnost i bezbednost podatka o ličnosti svakog stanovnika EU. Da bi se osigurala usklađenost sa GDPR-om, treba razumeti i primeniti osnovne principe ove uredbe.

Ljudi imaju pravo na privatnost. Organizacije moraju da poštuju njihovu privatnost ograničavanjem podataka koje o njima prikupljaju i obrađuju i tako što štite ove podatke. Obaveze vezano za privatnost odnose se na bilo koju informaciju na osnovu koje može da se identifikuje pojedinac koji živi u Evropskoj uniji, bilo da se to može učiniti samo pomoću ove informacije ili njenim korišćenjem u kombinaciji sa nekom drugom informacijom. Ove informacije mogu biti adrese, brojevi pasoša, brojevi vozačke dozvole, finansijski podaci, biometrijski podaci, članstvo u sindikatu, podaci o lokaciji, o zdravstvenom stanju, kao i informacije koje se odnose na seksualnu, versku ili političku orjentaciju osobe. Uredba se odnosi na „fizička lica“, što znači pojedince. U nastavku je pregled glavnih principa kojih se treba pridržavati kada je GDPR u pitanju:

Podaci o ličnosti moraju da se obrađuju zakonito, pravično i na transparentan način.

Licima čiji se podaci obrađuju se mora saopštiti koji se njihovi podaci prikupljaju i u koju svrhu.

Podaci o ličnosti se moraju prikupljati u određene, jasno definisane i legitimne svrhe. Prikupljeni podaci se ne mogu koristiti ni za jedan drugi razlog koji nije u skladu sa ovim svrhama.

Podaci o ličnosti moraju da se čuvaju i obrađuju samo dok je to potrebno za tu svrhu i ne duže od toga.

Podaci o ličnosti moraju biti ažurni i tačni.

Lica čiji se podaci obrađuju imaju pravo da dobiju kopiju svojih podataka ili mogu zatražiti da se njihovi lični podaci više ne koriste, odnosno u nekim slučajevima da budu potpuno izbrisani.

Organizacije moraju da primene odgovarajuće bezbednosne mere radi zaštite podataka o ličnosti od slučajnog ili namernog uništenja, gubitka, promene ili otkrivanja.

Pored toga, organizacije moraju da osiguraju da svi zaposleni koji rade sa podacima o ličnosti budu odgovarajuće obučeni kako da obezbede i zaštite te podatke.

Primenjene mere za zaštitu podataka o ličnosti moraju da pružaju nivo bezbednosti koji odgovara osetljivosti ovih podataka. Kako rizik povezan sa ovim podacima postaje veći, tako i napori i ulaganja u mere zaštite ovih podataka treba da budu veće. Ove mere treba da se redovno preispituju i po potrebi ažuriraju. Odluke i mere za zaštitu privatnosti i bezbednosti treba da budu dokumentovane kako bi pomogle organizacijama da demonstriraju usklađenost sa zahtevima uredbe. Pored toga, organizacije su u zakonskoj obavezi da primenjuju mere, kao što su definisanje ugovornih obaveza i provera trećih strana, kako bi zaštitile podatke o ličnosti prilikom prenosa trećim stranama, a naročito subjektima koji su izvan Evropske unije. Konačno, u slučaju povrede bezbednosti podataka o ličnosti, organizacija mora da prijavi ovu povredu u roku od 72 sata nakon što je postane svesna. Neuspeh organizacije da zadovolji zahteve GDPR može da rezultira novčanim kaznama koje iznose do 4% njenog globalnog prihoda, što GDPR čini jednim od najskupljih propisa na svetu.

Verzija na srpskom

Telekom Srbija kao društveno odgovorna telekomunikaciona kompanija pomaže prevođenje i distribuciju ovog biltena kako bi se unapredila svest korisnika informaciono-komunikacionih tehnologija o bezbednosti informacija.

Gost urednik

Brajan Honan *je direktor kompanije BH Consulting, nezavisne konsultantske kuće iz Dablina specijalizovane za sajber bezbednost i zaštitu podataka. Brajan je obavljao poslove specijalnog savetnika Europol-ovog centra za sajber kriminal (EC3), osnivač je prvog irskog CERT-a i član je savetodavnih odbora u nekoliko inovativnih kompanija koje se bave sajber bezbednošću. Brajana možete pronaći na* www.linkedin.com/in/brianhonan *ili Tviteru* (@brianhonan).

Dodatne informacije

Pregled GDPR-a za pojedince i organizacije:	http://gdprandyou.ie
Tekst GDPR uredbe:	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016R0679
OUCH! prevodi i arhive:	https://www.sans.org/u/D88