SANS SECURITY AWARENESS

Buletinul informativ lunar de sensibilizare asupra securității pentru utilizatorii de calculatoare

Regulamentul General privind Protecția Datelor (RGPD)

Generalități

Veți fi auzit de noua lege denumită prescurtat „GDPR", sau Regulamentul General privind Protecția Datelor (RGPD, în limba română). Această lege a fost adoptată de Uniunea Europeană și devine direct aplicabilă începând cu 25 mai 2018. Se aplică oricărei organizații care prelucrează date personale ale cetățenilor rezidenți în Uniunea Europeană, indiferent de locul unde se află aceste organizații în lume. RGPD impune organizațiilor să asigure protecția și securitatea datelor personale ale oricărui rezident UE. Pentru a asigura conformitatea cu RGPD anumite principii de bază trebuie să fie înțelese și puse în practică.

Cetățenii au dreptul la protecția datelor cu caracter personal. Organizațiile trebuie să respecte acest drept prin limitarea colectării și procesării de date personale și protejarea acestor date. Aceste cerințe de protecție se aplică oricăror tipuri de informații, fie individual fie folosite corelat cu altele, ce ar putea permite identificarea persoanelor fizice rezidente în Uniunea Europeană. Aceste informații pot fi adresa, seria pașaportului, seria permisului de conducere, datele financiare, biometrice, apartenența la diverse organizații, istoricul medical, date despre localizare sau informații legate de orientarea sexuală, apartenența religioasă sau opțiunile politice. Regulamentul se referă la o „persoane fizică" adică indivizi în viață. Mai jos câteva dintre principiile de bază ale RGPD ce trebuie urmate:

Datele personale ale cetățenilor sunt prelucrate în mod legal, echitabil și transparent față de persoana vizată.

Persoanele vizate trebuie să fie informate despre informațiile care sunt colectate și scopul pentru care sunt colectate.

Datele personale trebuie să fie colectate pentru scopuri specifice, explicite și legitime. Acestea nu trebuie să fie folosite în alte scopuri care nu corespund acestor scopuri declarate.

Datele personale trebuie păstrate și procesate numai atât timp cât este necesar pentru scopul în care au fost colectate.

Datele personale păstrate trebuie să fie exacte și rectificate, dacă e cazul.

Persoanele vizate au dreptul să primească o copie a datelor personale colectate sau pot cere încetarea prelucrării sau, în anumite condiții, ștergerea acestora.

Organizațiile trebuie să ia măsuri adecvate de natură tehnică sau organizatorică pentru protejarea datelor personale față de accesul accidental sau fraudulos, distrugerea, pierderea sau modificarea lor.

În plus, organizațiile trebuie să se asigură că personalul care lucrează cu date personale a primit instruire adecvată privitor la securizarea și protejarea datelor cu caracter personal.

Măsurile de protecție ce sunt implementate pentru securizarea datelor cu caracter personal trebuie să asigure un nivel de protecție corespunzător caracterului sensibil al datelor. Deoarece riscurile asociate cu datele personale devin mai mari, eforturile și măsurile de protecție a acestora trebuie să crească în chip adecvat. Aceste măsuri de protecție trebuie revizuite periodic și actualizate corespunzător. Înregistrări bine documentate despre deciziile ce privesc măsurile de protecție și securitate a datelor personale demonstrează conformitatea cu cerințele legale. În plus, organizațiile sunt obligate prin lege să pună în practică măsuri adecvate, cum ar fi contracte și eforturi rezonabile necesare în negocieri, pentru protejarea datelor atunci când sunt transferate către parteneri externi și în particular când acești parteneri externi sunt în afara Uniunii Europene. În final, în cazul încălcării securității datelor cu caracter personal, organizațiile au obligația notificării în termen de cel mult 72 de ore de la data la care au luat cunoștință de aceasta. Companiile care încalcă dispozițiile RGPD pot primi amenzi administrative de până la 4 % din cifra de afaceri mondială totală anuală, ceea ce face RGPD una dintre cele mai costisitoare legi din lume.

Versiunea în limba română

Cegeka este un furnizor independent de servicii IT&C ce își ajută clienții din întreaga Europă în transformarea lor digitală, dezvoltarea de aplicații folosind metodologiile Agile, soluții de încredere de tip Cloud și managementul serviciilor 24/7. Cegeka este prezentă în Austria, Belgia, Republica Cehă, Franța, Germania, Italia, Olanda, Polonia, România și Republica Slovacă, având 3600 de angajați. Cegeka a realizat o cifră de afaceri de 368 milioane de euro în 2015. Pentru mai multe informații vizitați www.cegeka.com.

Editor invitat

Brian Honan *este CEO la BH Consulting, o firmă independentă de consultanță în securitatea cibernetică și protecția datelor cu sediul în Dublin, Irlanda. Brian a fost consilier special la Europol Cybercrime Centre (EC3), este fondatorul primului CERT din Irlanda și membru al consiliului consultativ din mai multe companii inovatoare în domeniul securității. Îl puteți găsi pe Brian la* www.linkedin.com/in/brianhonan sau pe Twitter la @brianhonan .

Resurse online

Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal:	http://www.dataprotection.ro/
Noul Regulament General de Protecția Datelor:	http://www.dataprotection.ro/?page=Regulamentul_nr_679_2016
Regulamentul General de Protecția Datelor în arhiva EUR-Lex:	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016R0679
Arhiva buletinelor informative OUCH!:	https://www.sans.org/u/D88