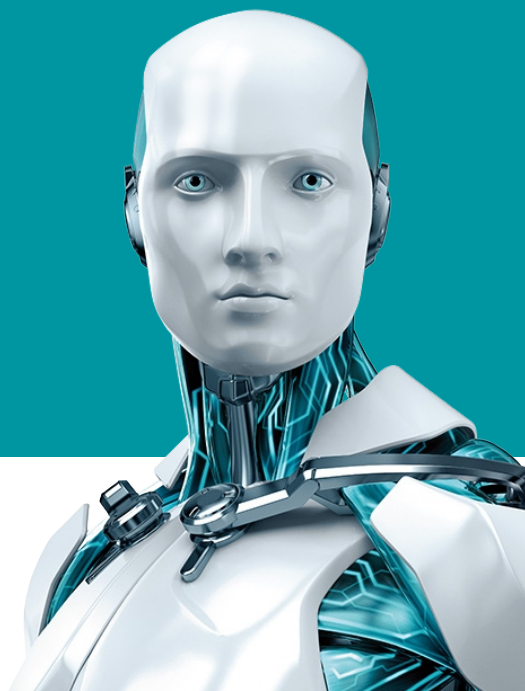
GDPR

Ghid Rapid privind Regulamentul General al UE pentru Protecția Datelor



ENJOY SAFER TECHNOLOGY™

Regulamentul General privind Protecția Datelor (GDPR) înlocuiește Directiva 95/46/CE a UE din 1995 privind Protecția Datelor. GDPR a fost dezvoltat pentru a consolida și unifica drepturile de confidențialitate online și protecția datelor pentru persoanele fizice în cadrul Uniunii Europene (UE), eficientizând în același timp obligațiile de protecție a datelor ce vizează companiile care deservesc cetățenii UE, printr-un regulament unic în locul a 28 de legi naționale diferite.

În data de 8 aprilie 2016, Consiliul a adoptat GDPR și o directivă asociată. Pe 14 aprilie 2016 Regulamentul și Directiva au fost adoptate de Parlamentul European.

Pe 4 mai 2016, textele oficiale ale Regulamentului și ale Directivei au fost publicate în Jurnalul Oficial al Uniunii Europene. Regulamentul se va aplica începând cu 25 mai 2018.

Cele 28 de state membre ale UE au pus în aplicare în 1995 normele în mod diferit, fiind dificil și costisitor pentru companiile din UE să opereze dincolo de frontierele interne, din cauza acestor diferențe considerabile în ceea ce privește normele de aplicare. Se estimează că eliminarea acestei fragmentări va conduce la economii pentru companii de aproximativ 2,3 miliarde € pe an în spațiul Uniunii Europene.

Care sunt schimbările?

Modificările cheie ale reformei includ[1]:

- Dreptul de a ști când datele cuiva au fost piratate: Companiile și organizațiile trebuie să notifice Autoritatea Națională de Supraveghere a Prelucrării Datelor despre încălcările securității datelor care supun persoanele unor riscuri și să comunice persoanelor afectate toate încălcările de mare risc cât mai curând posibil, astfel încât utilizatorii să poată lua măsurile corespunzătoare.
- O aplicare mai strictă a regulilor: autoritățile de protecție a datelor vor fi în măsură să amendeze companiile care nu respectă normele UE cu până la 4% din cifra de afaceri globală anuală a acestora. Amenzile administrative nu sunt obligatorii, dar dacă se impune aplicarea lor, valoarea acestora trebuie să se decidă, în fiecare caz în parte și trebuie să fie eficace, proporționale și să aibă un efect de descurajare.
- Un continent, o singură lege: o lege unică europeană pentru protecția datelor, care să înlocuiască actualul mozaic de legi naționale. Companiile se vor ocupa de o singură lege, nu de 28. Beneficiile reducerilor de costuri sunt estimate la 2,3 miliarde € pe an.
- Organizațiile trebuie să notifice autoritatea națională când au de-a face cu încălcări grave ale datelor, cât mai curând posibil (dacă este posibil, în termen de 24 de ore).
- Normele UE trebuie să se aplice în cazul în care datele personale sunt prelucrate în străinătate de către companiile care activează pe piața UE, oferind bunurile și serviciile lor (inclusiv bunuri și servicii gratuite) pentru cetățenii UE sau în cazul în care aceste organizații monitorizează comportamentul indivizilor în UE.
- Protecția datelor prin concepție sau implicit: "protecția datelor prin concepție" și "protecția datelor în mod implicit" sunt acum elemente

1 Rezumatul comunicatului de presă: http://europa.eu/rapid/press-release_MEMO-15-6385_en.htm

esențiale în normele UE privind protecția datelor. Norma va fi ca măsurile de protecție a datelor să fie încorporate în produse și servicii din etapa inițială de dezvoltare, iar setările de confidențialitate să fie prestabilite.

Prin consolidarea protecției datelor în UE, devine obligatoriu pentru companii să protejeze în mod adecvat datele personale sensibile, definite ca fiind:

> *"orice informație referitoare la o persoană fizică identificată sau identificabilă, denumită în continuare «persoană vizată»; o persoană identificabilă este o persoană care poate fi identificată, în mod direct sau indirect, în special prin referire la un număr de identificare sau la unul sau mai mulți factori specifici identității sale fizice, fiziologice, psihice, economice, culturale sau sociale;"*[2]

Această definiție largă a datelor cu caracter personal acoperă cu ușurință cele mai simple înregistrări care se referă, chiar și indirect, la utilizatori, clienți, angajați, elevi și orice alte înregistrări referitoare la un individ.

Ce spune Regulamentul despre protejarea datelor?

Articolul 32, Securitatea proceselor afirmă[3]:

> 1. *Având în vedere stadiul actual al tehnicii, costurile de punere în aplicare și natura domeniului de aplicare, contextul și scopul prelucrării, precum și riscul variabil de probabilitate și severitate ce vizează drepturile și libertățile persoanelor fizice, operatorul și procesatorul trebuie să pună în aplicare măsuri tehnice și organizatorice adecvate pentru a asigura un nivel de securitate corespunzător riscului, în care se includ, printre altele, după caz:*
>
> *a) anonimizarea sau criptarea datelor cu caracter personal;*
> *b) capacitatea de a asigura continuu confidențialitatea, integritatea, disponibilitatea și capacitatea de rezistență a sistemelor și serviciilor de prelucrare;*
> *c) capacitatea de a restabili disponibilitatea și accesul la datele cu caracter personal în timp util, în cazul unui incident fizic sau tehnic;*
> *d) un proces constant de testare, evaluare și apreciere a eficienței măsurilor tehnice și organizatorice pentru asigurarea securității prelucrării.*

Criptarea este cel mai simplu și sigur mod de a asigura securitatea datelor, în conformitate cu articolul 32 din GDPR. Tehnologia este un mijloc stabilit de protejare a informațiilor, care sunt vulnerabile la furt sau pierdere. GDPR reprezintă, de asemenea, cazul pentru planuri eficiente de recuperare în caz de dezastru, de recuperare a parolei și a sistemelor de gestionare a cheilor.

Articolul 30 din Regulament impune ca înregistrările să fie păstrate, inclusiv o descriere generală a măsurilor tehnice și organizatorice de securitate adoptate, după cum se prevede în articolul 32, ceea ce înseamnă că organizațiile au nevoie de înregistrări și de dovezi că sistemele sunt sigure și că datele criptate sunt recuperabile după un incident tehnic.

2 REGULAMENT (EC) No 45/2001: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2001.008.01.0001.01.ENG

3 Textul Regulamentului: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN

Care sunt regulile de notificare în cazul unei breșe de date?

Articolul 33[3] prevede notificarea unei încălcări a securității datelor personale către autoritatea de supraveghere și precizează că, în cazul unei încălcări a datelor cu caracter personal, autoritatea de supraveghere trebuie să fie notificată, dacă este posibil, nu mai târziu de 72 de ore după ce organizația în cauză devine conștientă de încălcare. Orice notificare dincolo de 72 de ore trebuie să fie însoțită de o justificare motivată a întârzierii.

Articolul 34 se referă la comunicarea unei încălcări a securității datelor cu caracter personal către persoana vizată și prevede că:

> 1. *Atunci când încălcarea securității datelor cu caracter personal poate conduce la un risc ridicat la nivelul drepturilor și libertăților persoanelor fizice, operatorul comunică încălcarea datelor cu caracter personal către persoana vizată, fără întârzieri nejustificate.*

Cu toate acestea, articolul continuă să afirme că:

> 3. *Nu este necesară comunicarea către persoana vizată, după cum se face referire la alineatul 1, dacă oricare dintre următoarele condiții sunt îndeplinite:*
>
> *a) compania a pus în aplicare măsuri tehnice de protecție și de organizare adecvate, iar aceste măsuri au fost aplicate datelor personale afectate de încălcarea securității datelor cu caracter personal, în special măsuri care fac ca datele personale să fie neinteligibile oricărei persoane care nu este autorizată să le acceseze, cum ar fi criptarea;*
>
> *b) compania a luat măsuri ulterioare care să garanteze că riscul ridicat al drepturilor și libertăților persoanelor vizate, prevăzut la alineatul 1, nu mai este posibil să se materializeze;*
>
> *c) ar implica un efort disproporționat. Într-un astfel de caz, trebuie să existe în schimb o comunicare publică sau o măsură similară prin care persoanele vizate sunt informate într-un mod la fel de eficient.*

Criptarea este fără dubiu considerată o garanție suficientă pentru a exclude aceste riscuri și consecințele pentru reputația corporativă.

Cum descurajează Regulamentul infractorii?

Articolul 83, Condiții generale de aplicare a unor amenzi administrative - punctul 4[4]:

> *4. Încălcările următoarelor dispoziții, în conformitate cu alineatul 2, sunt supuse unor amenzi administrative de până la 10 000 000 EUR sau, în cazul unei companii, de până la 2% din cifra de afaceri anuală totală, la nivel mondial, al exercițiului financiar precedent (alegându-se cea cu valoare mai mare):*
>
> *a) obligațiile operatorului și procesatorului în temeiul Articolelor 8, 11, 25 până la 39, 42 și 43; astfel, acoperind articolelor referitoare la normele de notificare a încălcării - articolul 33 și articolul 34, precum și punctul cinci din articolul 83 prevede în continuare:*
>
> *5. Încălcările următoarelor dispoziții, în conformitate cu alineatul 2, sunt supuse unor amenzi administrative de până la 20 000 000 de euro sau, în cazul unei companii, de până la 4% din cifra de afaceri anuală totală, la nivel mondial, al exercițiului financiar precedent, (alegându-se cea cu valoare mai mare):*
>
> *a) principiile de bază pentru prelucrare, inclusiv condițiile de autorizare, în conformitate cu articolele 5, 6, 7 și 9;*

4 Textul Regulamentului: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN

În cazul articolului 5, Principii referitoare la prelucrarea datelor cu caracter personal prevăd:

1. Datele cu caracter personal sunt:

f) prelucrate într-o manieră care să asigure securitatea adecvată a datelor cu caracter personal, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii accidentale, distrugerii sau deteriorării, prin măsuri tehnice sau organizatorice adecvate ("integritate și confidențialitate").

Această explicație clară care penalizează și descurajează companiile care nesocotesc regulile de confidențialitate intră în vigoare în acest an, așa că e timpul să acționăm acum.

Unele țări au început deja să lucreze în acest sens; Senatul olandez a adoptat un proiect de lege în mai 2015 pentru modificarea Legii privind protecția datelor în anticiparea și pre-aderarea la GDPR, transformând Olanda din țara care avea unul dintre cele mai slabe regimuri de aplicare din Europa într-una cu unul din cele mai puternice. Regulamentul va fi aplicat în toate cele 28 de state membre, din mai 2018.

Ce măsuri ar trebui luate acum?

Regulamentul cere organizațiilor de toate mărimile să adopte un set nou de procese și de politici menite să ofere un control sporit persoanelor fizice asupra înregistrărilor personale. O mare parte din această prevedere va implica scrierea de noi procese și manuale, pregătirea personalului și a sistemelor de actualizare pentru a se adapta acestor noi proceduri. Alți pași implică măsuri practice, cum ar fi folosirea criptării în cazul în care există date expuse riscului.

Un laptop sau stick USB pierdut sau furat nu trebuie să conducă la o penalizare în cazul în care a fost criptat cu un produs validat. Software-ul DESlock a ajutat cu succes organizațiile de toate dimensiunile să își cripteze laptop-urile, mediile de stocare mass-media, e-mailurile sau fișierele, vreme de mai mulți ani. Produsele noastre acoperă toate platformele Windows de la XP la Windows 10 și iOS de la versiunea 7 în sus. Software-ul nostru este construit pe un subsistem criptografic FIPS 140-2 nivelul 1 validat, iar sistemul de gestionare a cheilor și serverul de management unic fac obiectul unor patente la nivel mondial.

Contactați ESET România sau un reseller ESET pentru mai multe informații și pentru a vă prezenta un produs demo sau software trial.

Unul dintre principiile cheie ale GDPR, după cum este prevăzut la articolul 5, este asigurarea securității corespunzătoare a datelor cu caracter personal. Și, după cum se menționează în articolul 32 - denumit Securitatea prelucrării- criptarea este o măsură tehnică adecvată pentru a realiza acest lucru. În cazul în care criptarea este utilizată ca o măsură tehnică, ea trebuie să ofere posibilitatea restabilirii datelor imediat după un incident, iar înregistrările trebuie să fie păstrate pentru a dovedi că sistemele sunt sigure și recuperabile.

DESlock Encryption de la ESET este proiectat pentru a face față acestor cerințe într-un mod simplu și eficient.

Obiective	DESlock Encryption - ESET
Siguranța datelor, păstrate în cadrul organizației	Toate versiunile comerciale ale DESlock Encryption includ posibilitatea de criptare a fișierelor, folderelor și mediilor de stocare mobile în mod standard, pentru a asigura securitatea datelor la nivel de endpoint.
Date sigure în tranzit	DESlock + Pro include opțiunea de criptare completă a discurilor și a mediilor de stocare mobile, stickuri USB și suporturi optice, pentru a asigura securitatea datelor în mișcare.
Securizează datele mobile în cazul practicilor de muncă de la domiciliu	Licențele comerciale DESlock Encryption se extind pentru a permite a doua instalare pe un PC deținut privat. Pe lângă aceasta, DESlock + Go adaugă criptare portabilă la orice dispozitiv de stocare USB.
Securizează tranferul datelor între locații	Toate versiunile DESLock Encryption includ un plug-in Outlook, criptare clipboard ce este compatibilă cu toți clienții de mail, inclusiv webmail, precum și criptarea la nivel de atașament pentru orice sistem. Criptarea sistemelor media optice permite transferul în condiții de siguranță a datelor stocate pe CD sau pe DVD.
Blochează/limitează accesul la anumite date	Tehnologia unică, patentată de key-sharing face simplă implementarea și gestionarea în cazul echipelor și grupurilor de lucru complexe.
Permite accesul la datele securizate atunci când este cazul	DESlock + Enterprise Server este proiectat pentru management de la distanță pentru utilizatori, printr-o conexiune la internet securizată. Cheile pot fi distribuite la nivel central și retrase rapid.
Stocarea în condiții de siguranță a datelor cu caracter personal	DESlock Encryption este validat FIPS-140-2 și folosește standarde de criptare, algoritmi și metode impuse de industrie, de încredere, aprobate și securizate.
Distrugerea securizată a datelor redundante	Instrumentul DESlock + Desktop Shredder șterge datele în mod securizat la standardul DoD-5220.22-M, asigurându-se că acestea sunt complet nerecuperabile.

Informații suplimentare:

Cum vă poate ajuta ESET privind GDPR

https://encryption.eset.com/ro/

Reforma UE privind regulile de protecție a datelor

http://ec.europa.eu/justice/data-protection/reform/

Regulamentul (EU) 2016/679 al Parlamentului European și al Consiliului

http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

ÎNCERCAȚI CRIPTAREA ESET GRATUIT

Aflați mai multe detalii accesând
encryption.eset.com/ro

eset ENJOY SAFER TECHNOLOGY™

ESET, spol. s r.o.
Aupark Tower, 16th Floor
Einsteinova 24, 851 01 Bratislava
Slovak Republic