Ghid

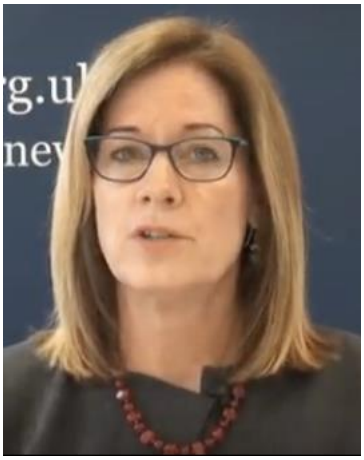
GDPR

pentru companiile

din **România**

STARTECH TEAM
CLASS IT SERVICES + SOLUTIONS

ÎNTR-O MISIUNE CONTINUĂ DE SUSȚINERE
A COMPANIILOR PRIN SOLUȚII ȘI SERVICII IT



Elizabeth Denham
Information Commissioner

"If your organization can't demonstrate that good data protection is a cornerstone of your business policy and practices, you're leaving your organization open to enforcement action that can damage both public reputation and bank balance.

But there's a carrot here as well as a stick: get data protection right, and you can see a real business benefit. Your customers will appreciate that you are taking a good care of their data."

"Comisia Europeană este ceea ce se poate numi "late în the game", din perspectiva datelor personale.

Europa și-a dat seama târziu că datele cetățenilor europeni sunt folosite fără nici un cadru legal și exploatate pentru profit, în special de către companiile de peste ocean, și încearcă în al 12-lea ceas să repare această problema.

Din păcate acest lucru creează costuri suplimentare, în special pentru companiile din Uniunea Europeană.

Bogdan Tudor
Startech Team

Lumea nu a început și nici nu se va termină odată cu GDPR așa cum încearcă majoritatea consultatilor să creeze impresia.

Pentru a te feri însă de neplăceri, este nevoie de o abordare structurată, organizată care să arate autorităților că în compania ta se ține cont și sunt respectate noile reglementări cu privire la protecția datelor personale."

Introducere in GDPR

GDPR în 10 pasi

Datele care intră sub incidența GDPR

GDPR se concentrează în exclusivitate asupra datelor personale deținute de companii.

Date personale sunt considerate următoarele:

Orice fișier care conține date specifice asociate persoanelor fizice, poate introduce o companie sub incidența GDPR.

1. **Informații de baza:** nume și prenume, adrese, numărul de telefon, adresa de email, dată de naștere, locul de naștere, numele de botez al mamei, detalii despre educație, numărul de buletin sau pașaport, CNP-ul.

2. **Date de identificare online** cum sunt adresele IP ale celor care accesează resursele online ale companiei, adresele MAC, locațiile GPS, nume de utilizator în diverse aplicații sau date care pot fi obținute prin cookie-urile din browser.

3. **Informații care pot identifica individual prin apartenența** la diverse asociații, opinii politice sau credințe religioase sau apartenența la sindicate.

4. **Informații biometrice**, de sănătate sau genetice.

5. **Înregistrări video, audio sau monitorizări ale activității la birou,** inclusiv monitorizarea accesului la Internet sau din punct de vedere al aplicațiilor folosite pe stațiile de lucru.

O reglementare europeană care stabilește modul în care sunt gestionate datele cu caracter personal ale indivizilor

Datele cu caracter personal, incluzând aici datele care pot identifica unic o anumită persoană, au fost tratate în general cu foarte multă lejeritate de către operatorii economici sau uneori chiar abuzate, conform analizelor realizate la cererea Comisiei Europene.

De la utilizarea în scopuri de marketing, direct intruziv prin email sau prin apelare telefonică, prin forme abuzive de analiză sau de procesare menite să identifice tipare în campaniile de vânzare, prin tranzitarea nereglementată a datelor de la un operator la altul sau prin stocarea neglijentă a acestora, toate aceste practici au fost identificate că reprezentând un risc ridicat pentru cetățenii parte a Uniunii Europene.

Noua reglementare stabilește drepturi specifice pentru cei care își oferă datele personale operatorilor economici, incluzând aici utilizarea acestora doar cu consimțământul personal, dreptul de a fi șterse oricând, la cerere, posibilitatea de a fi informați relativ la formă de procesare a acestora.

În noua reglementare, operatorii economici sunt obligați să trateze datele cu caracter personal ale indivizilor într-un mod sigur din punct de vedere al securității acestora, prevăzând reguli specifice de preluare, stocare, analiză și informare a celor care le oferă.

În practică, în realizarea activității proprii, majoritatea operatorilor economici utilizează și procesează date cu caracter personal, cel puțin prin datele de identificare ale angajaților proprii.

Tipuri de companii aflate sub incidența GDPR

În cazul în care datele sunt procesate sau trec prin sistemele unui terț, acesta trebuie la rândul lui să dovedească că respectă normele GDPR iar companiile client trebuie să se asigure de acest lucru

GDPR împarte companiile în două categorii mari:

1. Controlori de date,
2. Procesatori de date.

Un procesator este responsabil de prelucrarea datelor cu caracter personal în numele unui controlor. **Un controlor** stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal.

O altă diferențiere pe care GDPR o face este după numărul angajaților:

1. Sub 250 de angajați,
2. Peste 250 de angajați.

GDPR se așteaptă ca toate întreprinderile mici și mijlocii să respecte Regulamentul, dar regulamentul este mult mai strict pentru companiile cu peste 250 de angajați..

Astfel, se prevede că organizațiile cu mai mult de 250 de angajați sunt obligate să țină o evidență strictă a activităților de prelucrare aflate sub responsabilitatea lor.

Indiferent de tipul de companie reglementările trebuie să fie respectate

Companiile locale, din nou cele mai afectate

În cazul companiilor multinaționale, deși vor fi obligate să respecte obligațiile care reies din regulament în toate statele eueropene în care operează, acestea se vor înregistra și vor fi controlate de către autoritatea de supraveghere a statului în care au sediul principal.

Care sunt principalele responsabilități?

În esență, regulamentul solicită companiilor **să utilizeze sisteme și proceduri de securitate a informațiilor**, care permit profesioniștilor să creeze procese consecvente și repetate și să implementeze modalități stricte de control și protective a acestora.

În plus, companiile trebuie să ofere utilizatorilor care le oferă datele personale, informații complet transparente despre modul în care acestea sunt folosite și drepturi prin care aceștia pot cere oricând detalii despre modul în care sunt folosite datele lor.

În secolul informației datele personale au devenit o marfă care poate fi cumpărată, vândută și schimbată.

O oportunitate de a pune lucrurile în ordine

"Din punctul nostru de vedere, noul regulament este o oportunitate pentru companii de a organiza într-un mod temeinic și sigur datele și informațiile de care dispun. Este cel mai bun moment de a inventaria datele confidențiale – cu caracter personal și nu numai – de a securiza accesul acestor informații și de a crea procesele și procedurile pentru a asigura protecția acestora"

Bogdan Tudor, CEO Startech Team

Modul în care trebuie înțeleasă directiva la baza, este că datele sensibile trebuie protejate de companiile care le dețin.

Regulamentul reamintește de 21 de ori companiilor că sunt obligate să "implementeze măsuri tehnice și organizatorice relevante".

1. Inventariază datele personale

Documentați datele personale pe care le dețineți, de unde provin și cine are acces la acestea

Având în vedere definiția expansivă a datelor cu caracter personal a regulamentului, orice tip de monitorizare a sistemelor informatice, a dispozitivelor atașate la rețea sau a dispozitivelor mobile va implica date cu caracter personal.

Așa-numitele date "speciale" prezintă o altă provocare: regulamentul o definește foarte larg și include date genetice sau biometrice și informații privind sănătatea personală, cum ar fi un concediu medical și cauza acestuia.

O abordare recomandată pentru a trata acest lucru este descoperirea datelor care implică utilizarea atât a sistemului de scanare active, cât și a monitorizării rețelei pasive pentru a localiza date sensibile necriptate într-un ecosistem informatic al companiei. De acolo, membrii echipei IT pot determina dacă să elimine datele sau să aplice modalități de protecție a acestora

2. Informează-te și comunică în interior importanța respectării GDPR

Crește gradul de conștientizare a riscurilor pentru proprii angajați

Trebuie să te asiguri că factorii de decizie și persoanele cheie din companie sunt conștiente că legea se schimbă în direcția GDPR. Ei trebuie să aprecieze impactul pe care acest lucru îl are și să identifice domeniile care ar putea provoca probleme de conformitate în cadrul GDPR. Ar ajuta dacă ai începe cu registrul de informații confidențiale al companiei.

Implementarea GDPR ar putea avea implicații semnificative asupra resurselor disponibile, în special pentru organizațiile mici și mijlocii. Este posibil să întâmpi dificultăți în a aloca persoane care să se ocupe de acest lucru dacă lasi pregătirea pentru conformitate până în ultima clipă.

3. Implementează cadrul și procedurile interne

Articolul 32 din regulament mandatează controlorii și prelucratorii "să pună în aplicare măsuri tehnice și organizatorice adecvate pentru a asigura un nivel de securitate adecvat riscului".

Definește un set minimal de reguli pe care să le extinzi apoi pas cu pas.

Cadrele de securitate a informațiilor reprezintă o colecție de bune practici acumulate de profesioniști din diferite industrii de-a lungul timpului și oferă puncte de plecare ideale pentru elaborarea măsurilor adecvate. Cadre precum ISO / IEC 270017/270028 oferă standarde industriale acceptate pentru protecția datelor.

În timp ce UE nu prescrie un cadru special, aderarea unei companii la standardele stabilite în oricare dintre aceste cadre va face mult mai probabilă demonstrarea conformității cu articolul 32 în cazul unei încălcări.

4. Comunică regulile către cei care îți încredințează datele personale

Începe cu primul pas: colectarea datelor

Ar trebui să revizuiești notificările despre confidențialitatea datelor pe care le folosești în mod curent și să pui în aplicare un plan pentru a efectua modificările necesare în timp pentru implementarea GDPR.

Revizuiește notificările curente despre confidențialitatea datelor

Când colectezi date personale, trebuie să furnizezi în prezent anumite informații, precum identitatea ta și modul în care intenționezi să utilizezi informațiile. Acest lucru se face, de obicei, printr-o notificare privind confidențialitatea. Sub GDPR există câteva lucruri suplimentare pe care trebuie să le comunici utilizatorilor. De exemplu, va trebui să explici baza legală pentru prelucrarea datelor, perioadele de retenție a datelor și că persoanele au dreptul să se adreseze către autoritatea de supraveghere, dacă acestea consideră că există o problemă cu modul în care le gestionezi datele. GDPR cere că informațiile să fie furnizate în limbaj concis, ușor de înțeles și clar.

5. Cere acceptul de înregistrare și procesare a datelor

Revizuiește modul în care cauti, înregistrezi, gestionezi consimtamântul de procesare a datelor

Consimțământul trebuie să fie dat în mod liber, să fie specific, informat și lipsit de ambiguitate. Persoanele vizate ar trebui să înțeleagă asupra ceea ce consimt. Trebuie să existe un răspuns clar, consimțământul nu poate fi dedus din context, din campuri precompletate sau presupus. De asemenea, trebuie să fie separat de alți termeni și condiții și vor trebui să fie incluse modalități simple de retragere a acestuia.

Consimțământul trebuie să fie verificabil! Conform GDPR, indivizii au mai multe drepturi atunci cand vine vorba despre acceptul de a le procesa datele.

Dacă te bazezi pe acordul utilizatorilor, asigurați-vă că aceasta va respecta standardul GDPR de a fi specific, granular, clar, proeminent, documentat corespunzător și ușor de retras.

6. Stabilește cum vei gestiona cererile de operare asupra datelor

Actualizeaza procedurile și planifica modul în care vei rezolva cererile de operare a datelor

GDPR introduce noi drepturi ale utilizatorilor aspura datelor, precum: dreptul de a fi informat, dreptul de a avea acces la date, dreptul la rectificarea datelor, dreptul de ștergere a datelor (“dreptul de a fi uitat”), de restricționare a procesării, dreptul la portabilitatea datelor, de a obiecta și dreptul decizional privind prelucrarea automatizată sau profilarea datelor.

Luând în calcul toate cele de mai sus, ar trebui să te asiguri că ai proceduri implementate pentru a face față volumului mare de lucru generat de noile reguli.

În majoritatea cazurilor, nu vei putea percepe taxe pentru îndeplinirea cererilor. Vei avea la dispoziție o luna pentru a te conforma. Poți refuza sau taxa doar cererile care sunt nefondate sau excesive.

7. Implementează mecanisme de identificare și de raportare a accesului neautorizat sau a pierderilor de date

Conform art. 33, în cazul unei pierderi a datelor, operatorul trebuie să poată raporta autorităților de supraveghere competențe "fără întârzieri nejustificate" și, dacă este posibil, în termen de 72 de ore de la constatarea încălcării.

Realizeaza un plan de reacție la incidente!

GDPR introduce această obligație pentru toate organizațiile de a raporta încălcarea securității datelor către autoritatea de supraveghre și, în unele cazuri, chiar persoanelor fizice.

Notificările trebuie să conțină următoarele:

- natura și detaliile încălcării,
- informații de contact pentru responsabilul cu protecția datelor,
- consecințele probabile ale încălcării,
- ce măsuri au fost luate (sau sunt propuse) pentru remedierea nerespectării, inclusiv eforturile de atenuare a efectelor adverse.

Asigura-te că ai procedurile potrivite pentru a detecta, raporta și investiga o încălcare a datelor cu caracter personal

Trebuie notificată autoritatea de supraveghere, asupra unei breșe de securitate a datelor, în cazul în care există posibilitatea că pierderea de datel să ducă la un risc pentru drepturile și libertățile persoanelor - dacă, de exemplu, aceasta ar putea duce la discriminare, prejudiciu reputației, pierderi financiare, pierderea confidențialității sau orice alte dezavantaje economice sau sociale semnificative.

Organizațiile mai mari vor trebui să dezvolte politici și proceduri pentru gestionarea breșelor de securitate a datelor.

Eșecul în a raporta pierderile de date, atunci când se cere să o faceți, poate rezulta într-o amendă, de asemenea încălcarea în sine a prevederilor regulamentului poate duce la o amendă.

8. Asigură-te că sistemele tale IT respectă standardele de protecție a datelor

Deși articolul 32 oferă exemple de măsuri de securitate, acesta nu oferă o listă completă a măsurilor ce trebuie implementate, acestea trebuie să fie stabilite în detaliu de către fiecare companie.

E simplu: "pază bună trece primejdia rea"

Printre tehnologiile la care face referire sunt:

1) Criptarea si pseudonimizarea datelor stocate,
2) Criptarea conexiunilor,
3) Realizarea salvărilor de siguranță a datelor,
4) Asigurarea integrității datelor în uz, în tranzit și în staționare,
5) Testarea măsurilor organizaționale,
6) Testarea sistemelor folosite, evaluarea eficacității controalelor tehnice de procesare a datelor.

În cazul unui eveniment neprevăzut lipsa oricărei măsuri de protecție sau inițiative de securizare a datelor va expune compania.

Asigurarea integrității datelor în uz, în tranzit și în staționare presupune proceduri și procese solide de oferire a accesului la date, de schimbare a datelor confidențiale de acces, de folosire de tehnologii de validare suplimentară a autorizării și de stocare sigură a acestora.

În plus, două situații specifice - echipamente necunoscute aflate în rețea, sisteme neactualizate și tehnologii IT învechite - au potențialul de a crea probleme majore de securitate și de a invită autoritatea de supraveghere în control, în eventualitatea unei încălcări sau a utilizării abuzive a datelor cu caracter personal.

Un proces pus la punct, cel puțin la nivel minimal arată bună intenție a companiei.

Atenție la furnizorii de servicii cloud, pentru că oferă o expunere extraordinară persoanelor malițioase; acele bunuri sau servicii nu beneficiază de regulile de securitate a informațiilor ale companiei, pot avea vulnerabilități neprotejate sau pot fi pur și simplu improprii pentru stocarea acestor date. Odată compromise, autoritatea de supraveghere va întreba compania de ce nu a avut un program de combatere a acestor fenomene

Un laptop pierdut care conține date confidențiale reprezintă un incident de securitate care trebuie raportat in 72 de ore

Totodată companiile trebuie să aibă la dispoziție măsuri și sisteme care să le permită să identifice o potențială breșă de securitate și să informeze autoritatea în maximum 72 de ore de la producerea acesteia.

Acest lucru presupune urmărirea continuă și corelarea informațiilor de acces produse de echipamente (Log Analysis), instalare de capcane (Honeypots) și supervizarea 24/7 a acestora.

Datele trebuie protejate si in cazul avariei majore a locației principale

Nu în ultimul rând, Art. 32 este principala dispoziție care impune măsuri tehnice de protecție a datelor. Alineatul (1) litera (c) prevede, ca măsură de securitate, "capacitatea de a restabili în timp util disponibilitatea și accesul la date cu caracter personal în cazul unui incident fizic sau tehnic."

Profesioniștii ar trebui să revizuiască atât propriile planuri de continuitate a afacerii, cât și planurile de redresare în caz de catastrofe, de asemenea vor verifica și angajamentele de restaurare a serviciilor în cadrul contractelor cu furnizorii de servicii, asta pentru a determina dacă trebuie să se facă modificări în lumina regulamentului.

Așadar, asigură-te că ai pus la punct și validat planul de continuitate a afacerii tale și de recuperare în caz de evenimente neprevăzute care pot afecta datele stocate.

9. Asigură-te că furnizorii tăi respectă GDPR

Furnizorii tai trebuie sa respecte GDPR

Conform regulamentului ești obligat să te asiguri că furnizorii cu care lucrezi sunt conformi cu reglementările GDPR.

Având în vedere datele la care au acces, este cu atât mai critic ca furnizorii de aplicații, de servicii și soluții IT să se asigure că respectă în detaliu noul regulament și că operează cu maxim de responsabilitate asupra datelor la care au acces.

Un furnizor IT va trebui să va poată dovedi următoarele:

Responsabilul cu protecția datelor (DPO – Data Protection Officer)

1. Să aibă un **responsabil pentru protecția datelor**:

Rolul acestui responsabil poate fi alocat unui angajat intern, deja existent, atât timp cât îndatoririle sale profesionale sunt compatibile și nu se produce un conflict de interese. Responsabilul raportează direct managementului și este obligat să păstreze secretul sau confidențialitatea în ceea ce privește îndeplinirea sarcinilor sale.

Evaluarea impactului privind protecția datelor (DPIA – Data Protection Impact Assessment)

2. Să fi făcut o evaluare de impact privind protecția datelor, această fiind obligatorie atunci când prelucrarea datelor duce la un risc ridicat pentru persoanele fizice, de exemplu:

- când o nouă tehnologie este implementată,
- în cazul în care o operațiune de profilare a datelor poate afecta persoanele,
- acolo unde se procesează pe scară largă date cu caracter special.

Evaluarea impactului ajută organizațiile să identifice cea mai eficientă modalitate de a-și respectă obligațiile de protecție a datelor și de a satisface nevoile de confidențialitate.

Informații de Identificare Personală (PII – Personally Identifiable Information)

3. Să fi pregătit personalul propriu, relativ la PII

Toate datele despre PII pot fi considerate date cu caracter personal, dar nu toate datele personale sunt informații cu caracter personal.

10. Stabilește un plan de acțiune și apucă-te de treabă

Acum ai la dispoziție cadrul general și majoritatea informațiilor relevante despre noua reglementare europeană cu privire la procesarea datelor cu caracter personal (GDPR).

Mai jos ai câțiva pași pe care ar trebui să îi iei în considerare pentru implementare, pe măsură ce îți începi călătoria pentru a deveni conform cu GDPR:

1. **Stabilește modalitatea în care vei aborda procesul**
   Vei asigna o persoană din interiorul companiei care să realizeze acest proces sau vei selecta un furnizor extern. În cazul în care vei aloca o persoană din interior pe site-ul nostru sunt disponibile mai multe informații, documente și modele de procese și proceduri.

2. **Validați împreună cu serviciul IT care sunt datele care intră sub incidența GDPR și puneți la punct modalitățile de protectie**
   În cazul în care folosești un furnizor extern, cere dovezile care să arate respectarea de către acesta a noilor reglementări. Stabilește măsurile tehnice de protecție a datelor.

3. **Stabilește un plan de lucru și termene concrete**

4. **Cere să fii informat relativ la progres până la finalizarea procesului**
   Lucrați în intervale de o săptămâna în care să validați progresul.

5. **Validează la final cu un expert**
   În special dacă ai lucrat in-house, cere un review final sau o a două părere unui expert. Acesta trebuie să aibă experiență profesională și o înțelegere profundă a Regulamentului UE privind protecția datelor.

"Noul regulament este o oportunitate pentru companii de a organiza într-un mod temeinic și sigur datele și informațiile de care dispun. Este cel mai bun moment de a inventaria datele confidențiale – cu caracter personal și nu numai – de a securiza accesul la acestea și de a crea procesele și procedurile pentru a asigura protecția lor."

Bogdan Tudor, CEO Startech Team

O abordare informată asupra procesului și un set minimal de acțiuni specifice

1. Inventariază datele personale din companie ☐
2. Informează-te și comunică în interior importanța respectării GDPR ☐
3. Implementează cadrul și procedurile interne ☐
4. Comunică regulile către cei care îți încredințează datele personale ☐
5. Cere acceptul de înregistrare și procesare ☐
6. Stabilește cum vei gestiona cererile de operare asupra date ☐
7. Implementează mecanismele de identificare și de raportare ☐
8. Asigura-te că sistemele IT respectă standardele de protecție a datelor ☐
9. Asigura-te că furnizorii tăi respectă GDPR ☐
10. Stabilește un plan de acțiune și apucă-te de treaba ☐

Mai multe resurse și modele de documente sunt disponibile online la:

https://www.startechteam.ro/gdpr

STARTECH TEAM
CLASS IT SERVICES + SOLUTIONS