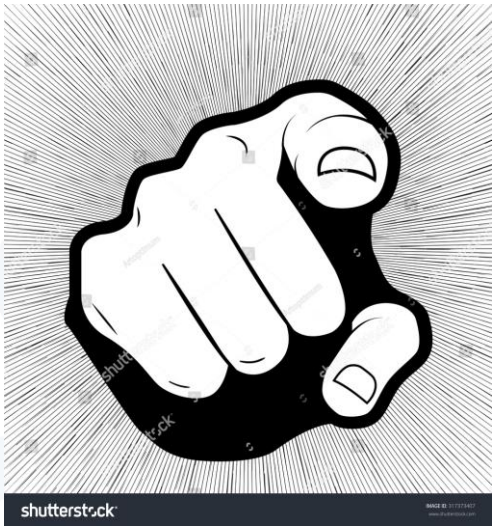
GHID
practic de implementare GDPR

Cerinte principale impuse de GDPR

- Temei juridic pentru controlul si prelucrarea datelor cu caracter personal
- Scop legitim pentru colectarea si prelucrarea datelor personale
- Documentarea tuturor activitatilor de prelucrare a datelor
- Evaluarea riscurilor asupra drepturilor si libertatilor persoanelor vizate
- Masuri organizatorice si tehnice pentru protejarea datelor
- Minimizarea cantitatii de date cu caracter personal prelucrate
- Sa fiti in masura sa probati conformitatea cu GDPR
- Notificarea autoritatii de supraveghere cu privire la incalcarea datelor
- Desemnarea unui responsabil cu protectia datelor (DPO)
- Actualizarea datelor personale inexacte
- Verificarea transferul datelor in afara UE

Determinati daca GDPR se aplica organizatiei dumneavoastra

- Mai mult ca sigur vi se aplica si dumneavoastra;
- Aveti in vedere aplicarea materiala si teritoriala.



MUȘAT & ASOCIAȚII
Attorneys at Law

Aplicare materiala

- Se aplica prelucrarilor de date cu caracter personal care fac parte sau care sunt destinate sa faca parte dintr-un sistem de evidenta a datelor;

- Nu se aplica prelucrarilor:

  - In cadrul activitatilor care nu intra sub incidenta dreptului Uniunii;
  - Efectuate de catre o persoana fizica in cadrul unei activitati exclusiv personale sau domestice;
  - Realizate de catre autoritati competente in scopul prevenirii, investigarii, depistarii sau urmaririi penale a infractiunilor, executarii pedepselor penale, protejarii impotriva amenintarilor la adresa sigurantei publice si prevenirii acestora.

Aplicare teritoriala

Regulamentul se aplica operatorilor sau persoanelor imputernicite de operator:

- avand un sediu aflat pe teritoriul Uniunii, pentru prelucrarile din cadrul activitatilor desfasurate la acest sediu (indiferent daca prelucrarea are loc sau nu pe teritoriul Uniunii);
- care nu sunt stabiliti pe teritoriul Uniunii, dar care prelucreaza date cu caracter personal ale unor persoane vizate care se afla in Uniune, cu privire la:
  - Oferirea de bunuri sau servicii unor astfel de persoane vizate in Uniune,
  - Monitorizarea comportamentului lor, daca acesta se manifesta in cadrul Uniunii;

Regulamentul se aplica si unui operator stabilit in afara Uniunii, intr-un loc in care dreptul intern (al Uniunii) se aplica in temeiul dreptului international public.

Cunoasterea conditiilor introduse de Regulament

- Educati administratorii si personalul cu privire la impactul prevederilor GDPR pentru compania dvs.

- Pe cine?
  - Directorul executiv
  - Echipa de conducere
  - Personalul care se ocupa de prelucrarea datelor personale
- Cum?
  - Desemnati un responsabil cu protectia datelor
  - Puneti in aplicare cerintele stipulate de Regulament
  - Crearea unui grup de lucru comun
- Instruiti personalul cu privire la protectia datelor

Exemple:

- Ce ar trebui sa faca angajatii
- Ce nu ar trebui sa faca angajatii
- Sarcini si responsabilitati in asigurarea protectiei datelor

MUȘAT & ASOCIAȚII
Attorneys at Law

Intelegeti cele doua niveluri de sanctiuni instituite pentru nerespectarea GDPR

❑ Comparati amenda pentru organizatia dvs. (2% si 4% din cifra de afaceri anuala globala pentru anul precedent) cu eventualele costuri pentru intrarea in conformitate (administrative).

❑ **Tineti cont:**
Pentru stabilirea unei amenzi Autoritatea de supraveghere va tine cont de masurile de protectie luate de organizatia dvs

❑ Evaluati optiunile de asigurare cibernetica

MUȘAT & ASOCIAȚII
Attorneys at Law

Incalcarile va costa

Agentia Spaniola pentru Protectia Datelor a impus o amenda de 1,08 milioane de euro pentru o companie de televiziune care, printre alte infractiuni, nu a reusit protejeze informatii personale apartinand 7.000 de concurenti de televiziune, permitandu-le hacker-ilor sa le acceseze.	**in urma unei incalcari a datelor din 2015 care afecteaza 150 000 de clienti, Biroul Comisarului pentru Informatii al Regatului Unit a amendat furnizorul de servicii de comunicatii TalkTalk cu £400,000**	**Grupo Financiero Banorte, a treia banca din Mexic, a suferit o incalcare a securitatii datelor la sfarsitul anului 2014 / inceputul anului 2015. La ancheta din 2015, autoritatile mexicane au amendat banca cu 32 de milioane de pesos (2 milioane dolari).**

MUȘAT & ASOCIAȚII
Attorneys at Law

Asigurarea protectiei datelor

- Evaluati sistemele detinute si modurile de prelucrare a datelor prin prisma principiului asigurarii protectiei datelor

- Includeti evaluarea:
  - sistemelor actuale care detin date personale (ale clientilor si ale angajatilor) prin prisma riscurilor pe care le creeaza pentru drepturile si libertatile persoanelor vizate;
  - site-urilor web, management-ului relatiilor cu clientii, marketing-ului, intranet-ului, profilurilor de angajati, sistemelor HR, aplicatiilor interne personalizate

Asigurarea protectiei datelor

- Verificati daca datele personale vor fi transferate in afara UE
  - Verificati ce masuri de protectie vor fi adoptate

- Optiuni :
  - Decizii privind caracterul adecvat al nivelului de protectie
  - Reguli corporative obligatorii
  - Clauze contractuale
  - Coduri de conduita si certificare

- Revizuiti acordurile de prelucrare a datelor cu alte organizatii (inclusiv furnizorii de servicii cloud) si evaluati conformitatea acestora cu prevederile GDPR
  - Includeti si revizuirea masurilor organizatorice si tehnice adoptate de terti pentru protejarea datelor cu caracter personal

- Adoptati mecanisme de certificare sau coduri de conduita pentru protectia datelor de catre organizatii terte

Asigurarea protectiei datelor

- Cautati asociatii si alte organisme similare care sa reprezinte tipul dvs. de afacere (lucrati impreuna la diferite mecanisme de respectare a GDPR)

- Evaluati standardele actuale si certificarile care ofera un cadru structurat pentru a va ghida in respectarea GDPR
  - Puteti folosi Certificari aprobate pentru a demonstra standardele de protectie adecvate

- Exemple:
  - **ISO 27001:** standard international de securitate a informatiilor care certifica respectarea initiala si continua a conformitatii cu GDPR. Nu garanteaza 100% conformitatea
  - **ISO 27018:** standard international pentru protejarea datelor cu caracter personal stocate in serviciile publice cloud

- Luati in considerare:
  - Contactarea din timp a autoritatii de supraveghere
  - Contactarea unor societati de avocati si/sau de consultanta specializate in respectarea conditiilor GDPR

MUȘAT & ASOCIAȚII
Attorneys at Law

Desfasurati un inventar de tip end-to-end si un audit

- Evaluati abilitatea dumneavoastra de a identifica, analiza si clasifica datele cu caracter personal
- Aplicati politici de remediere pentru diferite categorii de date si stergeti date care nu mai sunt necesare pentru a minimiza expunerea
- Limitati accesul la date
- Se vor avea in vedere:
  - Sistemele de date aflate sub controlul organizatiei dvs: sistemele de e-mail, bazele de date si aplicatiile, serverele, serviciile SharePoint, sistemele SharePoint, alte sisteme de colaborare si arhivele de e-mail
  - Datele stocate in surse autorizate
  - Datele stocate pe dispozitivele de tip endpoint
  - Fluxurile de date catre si din tarile din afara Uniunii Europene
- Asigurati-va ca persoanele imputernicite vor dispune de proceduri eficiente de audit si raportare (pentru a proteja datele si pentru a raspunde la timp)

Desfasurati un inventar de tip end-to-end si un audit

- Identificati sistemele de date aflate in afara controlului dvs. direct
- Exemple:
  - Servicii de stocare in cloud: Dropbox, Box, etc.
  - Sincronizarea datelor organizatiei cu serviciile cloud care sunt apoi sincronizate si accesate de la dispozitive personale (telefoane, computere)
- Identificati masurile organizatorice si tehnice care fac datele personale inaccesibile, pentru a proteja drepturile si libertatile persoanelor vizate
  - Limitarea accesului la datele personale
  - Criptare
  - Pseudonimizare

!! Mentineti o evidenta detaliata a masurilor organizatorice si tehnice evaluate si implementate

Desfasurati un inventar de tip end-to-end si un audit

- Clasificati in mod corespunzator datele curente pentru a determina categoriile specifice de date care vor face obiectul GDPR
- Determinati categoriile de date care ar declansa o notificare privind incalcarea securitatii datelor
  - Surse distribuite: baze de date, directoare, management-ul relatiilor cu clientii
  - Sursele de date locale: serverele de fisiere, site-urile SharePoint, e-mailurile
  - Medii de testare si dezvoltare care au copii ale sistemelor de productie (incluzand date personale)
  - Dispozitive de tip endpoint care au copii sincronizate ale datelor personale
- Stabiliti o baza legitima pentru fiecare prelucrare a datelor
  - Exemplu: consimtamantul persoanei vizate

Examinati si actualizati politicile pentru protectia datelor

- Politicile care au fost sau nu deja implementate trebuie sa fie actualizate astfel incat sa fie conforme cu prevederile GDPR
- Exemple:
  - Cum puteti proteja datele personale
  - Cum puteti limita accesul la datele personale
  - Cum va puteti asigura ca transferurile de date internationale sunt legitime
- **Tineti cont:**
  - Politicile trebuie sa fie adoptate impreuna cu masuri tehnice pentru a asigura conformitatea
- Puneti in aplicare mecanisme adecvate pentru stabilirea consimtamantului persoanelor vizate Actualizarea consimtamantului existent
  - Metoda de stocare a consimtamantului
  - Metoda de retragere a consimtamantului
- Puneti in aplicare mecanisme pentru respunsul la solicitarile persoanelor vizate incluzand
- Tipul de prelucrare si durata retinerii datelor
- Notificarea dreptului de a obiecta la procesare, dreptul de acces, rectificare si stergere

! Trebuie sa aveti consimtamant pentru fiecare prelucrare.

MUȘAT & ASOCIAȚII
Attorneys at Law

Examinati si actualizati politicile pentru protectia datelor

- Implementati politici si procese conform noilor cerinte din cadrul GDPR
  - Raspunsuri la dreptul de acces, rectificare si stergere in termenul stabilit si fara cerinte de procesare manuala costisitoare
  - Raspunsul la cererile de portabilitate a datelor, utilizand un format digital adecvat si, cand este necesar, transmiterea datelor solicitate direct noului furnizor

- Nerespectarea drepturilor persoanelor vizate reprezinta o infractiune de nivel 2,
  - Atrage o amenda posibila de 20 de milioane EUR sau 4% din cifra de afaceri anuala globala, oricare dintre acestea este mai mare

Examinati si actualizati politicile pentru protectia datelor

- Inregistrari exacte ale tuturor activitatilor de prelucrare
  - Netinerea unei evidente precise a activitatilor de prelucrare a datelor atrage o sanctiune de nivel 1 (amenda posibila este de 10 milioane EUR sau 2% din cifra de afaceri anuala globala, oricare dintre acestea este mai mare)
- Modificati sau anulati toate procesele care nu sunt in conformitate cu regulamentul si nu mai sunt necesare.
  - Utilizati pseudonimizarea sau anonimizarea
- Cand serviciile dvs. privesc copiii, stabiliti practici adecvate pentru verificarea varstei si obtinerea consimtamantului parintilor sau tutorelui
  - GDPR stabileste varsta copilului la mai putin de 16 ani, dar statele membre il pot reduce la 13

Examinati si actualizati politicile pentru protectia datelor

- Evaluarea impactului privind protectia datelor trebuie pusa in aplicare si dezvoltata in mod constant
  - Este recomandata consultarea prealabila cu autoritatea de supraveghere
  - Responsabilul cu protectia datelor trebuie implicat in evaluare
- Notificarea in caz de incalcare a securitatii datelor
  - Monitorizare continua a activitatilor suspecte
  - Notificarea nu este necesara daca nu exista niciun risc pentru drepturile si libertatile persoanelor vizate ca urmare a incalcarii
  - In cazul in care exista riscuri pentru drepturile si libertatile persoanelor vizate => notificarea autoritatii de supraveghere si a persoanelor vizate in anumite conditii
  - Acord permanent cu o firma de relatii publice, care va fi activat in cazul unei incalcari
  - Acord permanent cu un partener specializat (specialist in securitatea datelor) care sa poata raspunde la incidentele de specialitate (care sa fie activat in functie de necesitati)

Stabiliti rolul responsabilului cu protectia datelor

- Responsabilul cu protectia datelor
  - un rol intern pentru o organizatie
  - un rol comun in cadrul unui grup de organizatii

- Datele de contact ale Responsabilului cu protectia datelor trebuie sa fie accesibile de catre persoanele vizate
- Raporteaza direct administratorului sau echipei de conducere
- Are capacitatile profesionale necesare si cunostintele de specialitate in domeniul protectiei datelor

Masuri tehnice

- Instrumente automate pentru descoperirea, catalogarea si clasificarea datelor personale in intreaga organizatie
- Capabilitati de prevenire a pierderilor de date (DLP) pentru a examina fluxurile de date si a identifica datele cu caracter personal care nu fac obiectul garantiilor sau autorizatiilor adecvate. Instrumentele DLP pot bloca sau pune in carantina astfel de fluxuri de date, in asteptarea rectificarii adecvate
- Criptarea datelor
- Capacitatile de identificare, blocare si investigare a criminalitatii pentru identificarea rapida a tentativelor de acces neautorizat la date si alte amenintari.
- Capabilitati de export de date

Întrebări?

MUȘAT & ASOCIAȚII
Attorneys at Law

Vă mulțumesc!

MUȘAT & ASOCIAȚII
Attorneys at Law