Conformitatea cu GDPR.
DE UNDE ÎNCEPEM?

certSIGN

Ce?

Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului Uniunii Europene din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) – GDPR (General Data Protection Regulation) nu se poate compara cu prea multe din regulamentele emise, până în prezent, de Uniunea Europeană, având în vedere impactul și amplitudinea măsurilor pe care le stipulează.

Prevederile acestui regulament nu sunt opționale și vizează toate activitățile din orice sector și domeniu, indiferent de dimensiunea business-ului, pentru că măsurile prevăzute aduc atingere tuturor activităților care implică informații - GDPR are informația ca punct central de interes - mai precis, tot ceea ce ține de prelucrarea informațiilor, adică de colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, divulgarea prin transmitere, diseminarea sau punerea la dispoziție în orice alt mod, alinierea sau combinarea, restricționarea, ștergerea sau distrugerea informațiilor.

Când?

25 mai 2018 este data de la care Regulamentul începe să producă efecte.

Cui se aplică regulamentul?

Tuturor persoanelor fizice sau juridice, autorități publice, agenții sau alte organisme care procesează sau au acces la date cu caracter personal – ORICE informații privind o persoană fizică identificată sau identificabilă („persoana vizată”), direct sau indirect.

Așadar, respectând proporțiile, Regulamentul vizează **ORICE ENTITATE** indiferent de obiectul său de activitate.

Cine evaluează?

În România, Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal - ANSPDCP va efectua verificările și va aplica sancțiuni în numele UE.

Cum se aplică?

Noul Regulament nu este o Directivă, deci se aplică în mod direct tuturor entităților vizate, fără a fi necesară adoptarea la nivelul legislației naționale. Aceasta înlocuiește Legea nr. 677/ 2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulaţie a acestor date.

Se impune implementarea de măsuri de securitate tehnice și organizatorice prin intermediul cărora să se pună în aplicare în mod eficient principiile de protecție a datelor. De asemenea, este necesară reducerea la minimum a datelor prelucrate și integrarea garanțiilor necesare, în cadrul prelucrării, pentru a îndeplini cerințele regulamentului și a proteja drepturile persoanelor vizate.

DOMENIUL DE APLICARE MATERIAL

• **Toate** datele care fac parte dintr-un sistem de evidență a datelor sau care sunt destinate să facă parte dintr-un sistem de evidență a datelor:

- Prelucrarea datelor efectuată total sau parțial prin mijloace automatizate
- Prelucrarea datelor prin alte mijloace decât cele automatizate

DOMENIUL DE APLICARE TERITORIAL

• **Operatori înregistrați în UE:** Toate activitățile unui operator sau ale unei persoane împuternicite de un operator înregistrat pe teritoriul Uniunii, indiferent dacă prelucrarea are loc sau nu pe teritoriul Uniunii
• **Persoane aflate în UE:** Prelucrarea datelor cu caracter personal ce aparțin unor persoane vizate care se află în Uniune, de către un operator sau o persoană împuternicită de operator care nu este stabilit(ă) în Uniune, atunci când activitățile de prelucrare sunt legate de:

- oferirea de bunuri sau servicii unor astfel de persoane vizate în Uniune, indiferent dacă se solicită sau nu efectuarea unei plăți de către persoana vizată
- monitorizarea comportamentului lor dacă acesta se manifestă în cadrul Uniunii

Noțiuni de bază

Regulamentul conține o multitudine de prevederi aplicabile în funcție de profilul organizației și introduce, de asemenea, o serie de cerințe ce TREBUIE respectate indiferent de tipul entității. Consimțământ explicit, breșe de securitate, responsabil cu protecția datelor personale, drepturile copiilor, protecția implicită a datelor, protecția datelor prin design, transferul internațional al datelor sunt conceptele cheie pe care le tratează Regulamentul GDPR.

Câteva dintre cele mai importante noțiuni care trebuie avute în vedere:

PERSOANA VIZATĂ (direct sau indirect) persoană identificată sau identificabilă prin intermediul unui element de identificare, cum ar fi un nume, un număr de identificare, date de localizare, un identificator online, sau unul sau mai multe elemente specifice, proprii identității sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale, indiferent de sursa de proveniență a datelor (echipamente mobile, aplicații informatice, adrese IP, cookies, etichete RFID etc).

PRELUCRARE a datelor cu caracter personal înseamnă orice operațiuni, fizice sau electronice, sau asupra unui set de date sau seturi de date cu caracter personal, cum ar fi: colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, divulgarea prin transmitere, diseminarea sau punerea la dispoziție în orice alt mod, alinierea sau combinarea, restricționarea, ștergerea sau distrugerea acestora.

OPERATOR DATE înseamnă persoana fizică sau juridică, autoritate publică, agenție sau alt organism care, singur sau împreună cu alte persoane, stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal.

PERSOANĂ ÎMPUTERNICITĂ DE OPERATOR (processor) înseamnă persoana fizică sau juridică, autoritate publică, agenție sau alt organism care prelucrează datele cu caracter personal în numele operatorului.

PSEUDONIMIZARE înseamnă prelucrarea datelor cu caracter personal într-un asemenea mod încât acestea să nu mai poată fi atribuite unei anume persoane vizate fără a se utiliza informații suplimentare, cu condiția ca aceste informații suplimentare să fie stocate separat și să facă obiectul unor măsuri de natură tehnică și organizatorică care să asigure neatribuirea respectivelor date cu caracter personal unei persoane fizice identificate sau identificabile.

CRIPTARE înseamnă măsură tehnică de protecţie prin care se asigură că datele cu caracter personal devin neinteligibile oricărei persoane care nu este autorizată să le acceseze.

GDPR
certSIGN

Drepturi și obligații

Persoana vizată are următoarele drepturi:

• Dreptul de informare și acces la date
• Rectificarea sau ștergerea datelor (dreptul de a fi uitat)
• Restricționarea prelucrării
• Dreptul de a se opune prelucrării
• Dreptul portabilității datelor
• Dreptul de nu fi supus unei decizii individuale
• Dreptul de opoziție

Operatorul/procesatorul datelor trebuie să asigure:

• Mijloacele pentru obținerea consimțământului explicit
• Disponibilitatea și rezistența sistemelor și a serviciilor de prelucrare
• Siguranța accesului la date și transferului acestora
• Testarea și evaluarea periodice
• Integritatea și confidențialitatea datelor
• Pseudonimizarea și/ sau criptarea datelor
• Evidența prelucrării
• Transmiterea notificărilor de atac în maxim 72 ore
• Restaurarea datelor și a accesului la acestea în caz de incidente

Provocări

Principala provocare pe care o va aduce implementarea Regulamentului este, în esență, reformarea întregului flux de lucru din cadrul fiecărei organizații astfel încât, la momentul T0, respectiv 25 mai 2018, să poată fi declarată conformitatea. O abordare riguroasă va avea în vedere ambele dimensiuni ale fluxului de date dintr-o organizație și anume:

• informațiile tranzacționate în fluxurile de lucru interne, inclusiv pe cele ale departamentelor precum resurse umane, financiar/contabilitate etc.
• informațiile tranzacționate ca urmare a desfășurării obiectului de activitate al organizației.

Ce tip de date referitoare la angajați, clienți, colaboratori colectează/accesează organizația?
Cine are aceste informații?
Către cine sunt distribuite informațiile?
Care este sursa informațiilor?
Cum se pot controla fluxurile de informații?
Cum pot fi gestionate breșele de securitate?

Răspunsul la fiecare dintre aceste întrebări va aduce organizația cu un pas mai aproape de conformitatea cu GDPR, indiferent de fluxul de lucru vizat.

O altă provocare este păstrarea rezultatelor obținute ca urmare a implementării măsurilor prevăzute de regulament, respectiv menținerea conformității atât la nivelul proceselor interne de lucru, cât și în ceea ce privește fluxurile de lucru cu terți, clienți sau furnizori. Cu toate acestea, și în ciuda provocărilor, implementarea măsurilor GDPR ar trebui văzută ca o oportunitate de a înțelege, organiza și optimiza tranzacțiile informaționale din organizație, așa cum proiectele Y2K au adus, în esență, o îmbunătățire a sistemelor informatice.

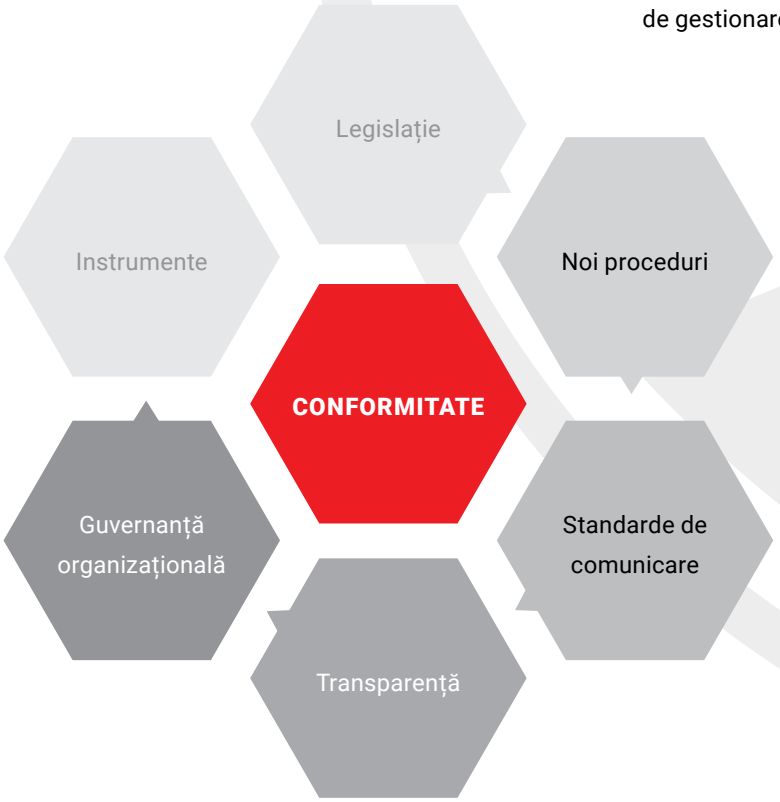
Conformitate cu GDPR.
De unde începem?

Pentru început ar trebui subliniat că implementarea acestui Regulament nu va afecta un singur departament al organizației din care faceți parte, ci, mai degrabă, vizează întreaga activitate. De aceea, pentru asigurarea unei implementări cât mai riguroase este necesară implicarea unei echipe multidisciplinare care va putea include, în funcție de tipul activității, managerul, departamentul juridic, departamentul resurse umane, responsabilii de clienți, auditorul etc. De asemenea, e important de menționat că stabilirea conformității nu se realizează doar prin implicarea unei echipe de proiect, impunerea de noi proceduri organizaționale, implicarea juriștilor în proces sau utilizarea instrumentelor IT, ci, în egală măsură, și prin utilizarea unor proceduri și instrumente complementare.

În primul rând, pentru ca o organizație să își poată atinge obiectivul impus de Regulamentul GDPR, respectiv obținerea conformității, este necesară o înțelegere cât mai bună a acestuia și, mai ales, este necesară identificarea acelor prevederi ale Regulamentului care se aplică organizației.

În paralel, cunoașterea datelor pe care le are organizația și a modului în care sunt gestionate în prezent reprezintă un alt aspect foarte important care trebuie să fie cunoscut. Deși poate părea complicat și anevoios, aceste două acțiuni (un inventar riguros al datelor și structurarea informațiilor conținute de Regulament cu privire la măsurile ce afectează organizația) vor reprezenta baza pentru un plan de activități ce va trebui întocmit pentru a avea o privire de ansamblu asupra a ceea ce va urma. Desigur, un număr cât mai mare de detalii legate de situația curentă va spori precizia cu care se va întocmi planul de lucru. Cunoașterea unor aspecte precum: modul în care se obține consimțământul în prezent, locul în care sunt stocate datele, cine le stochează, cine le accesează etc. va fi foarte utilă și pentru identificarea vulnerabilităților curente ale organizației din punctul de vedere al GDPR, dar și pentru identificarea de măsuri pentru eliminarea acestora.

Pentru a concluziona, considerăm că punctul de plecare în demersul de aliniere cu prevederile GDPR este reprezentat de momentul în care se inițiază colectarea de informații despre persoane și modul de gestionare al acestora în organizație.



GDPR

certSIGN

ANALIZEAZĂ

- Guvernanța organizației
- Infrastructura existentă
- Fluxul actual al datelor
- Riscurile actuale asociate prelucrărilor datelor
- Prevederile GDPR cu impact asupra organizație

PLANIFICĂ

- Proceduri de lucru în conformitate cu prevederile GDPR
- Măsuri tehnice și organizatorice de asigurare a prevederilor GDPR
- Transferul datelor, inclusiv transferul internațional

ACȚIONEAZĂ

- Implementarea noilor proceduri de lucru
- Implementarea măsurilor tehnice și organizatorice adecvate
- Informarea permanentă a stakeholderilor
- Numirea unui Responsabil cu protecția datelor (DPO - data protection officer), dacă e necesar

MENȚINERE

- Evaluarea periodică a măsurilor pentru a garanta securitatea prelucrărilor
- Plan de acțiune în caz de incident

CONFORMITATE GDPR

ANALIZEAZĂ

ETAPA	CE PRESUPUNE?	CUM OBȚINEM REZULTATUL?
Guvernanța organizației	Realizarea unei radiografii a organizației, din punct de vedere al personalului, pentru identificarea părților interesate (stakeholders) și responsabile cu respectarea politicilor și procedurilor care guvernează prelucrarea datelor cu caracter personal. În funcție de tipul organizației, va fi identificat și Responsabilul pentru Protecția Datelor (DPO - Data Protection Officer)	Resurse interne și/sau consultanță
Infrastructura existentă	Cuantificarea resurselor materiale existente și a celor utilizate pentru gestionarea datelor va oferi o imagine de ansamblu asupra nivelului de concordanță tehnică cu obiective GDPR	Resurse interne și/sau consultanță
Inventarul datelor si fluxul actual al acestora	Documentarea cât mai riguroasă cu privire la activitățile de procesare a datelor și realizarea unui inventar având la bază întrebările: cine, ce, unde, când, de ce, cum? Trebuie identificate și detaliile legate de transferurile internaționale de date atât pe teritoriul EU, cât și în afara lui.	Resurse interne și/sau consultanță
Prevederile GDPR cu impact asupra organizației	Descrierea detaliată a modului actual în care se asigură protecția datelor, cu scopul de a evalua ce trebuie să fie actualizat sau nou introdus pentru respectarea cerințelor GDPR	Resurse interne și/sau consultanță

GDPR

certSIGN

PLANIFICĂ

ETAPA	CE PRESUPUNE?	CUM OBȚINEM REZULTATUL?
Proceduri de lucru în conformitate cu prevederile GDPR	Actualizarea procedurilor de lucru existente, dar și definirea unor noi măsuri pentru a asigura conformitatea cu GDPR. Este recomandată elaborarea unui cod de conduită intern care să includă mecanisme cu ajutorul cărora se poate demonstra conformitatea cu GDPR sau aderarea la coduri de conduită aprobate. Principalele avantaje pe care îl oferă un cod de conduită: • creșterea transparenței și a responsabilității • oferirea de mijloace de soluționare a situațiilor de criză • stabilirea de bune practici cu privire la GDPR	Resurse interne și/sau consultanță
Măsuri tehnice de asigurare a prevederilor GDPR	Stabilirea mijloacelor ce urmează a fi implementate pentru a: • Obține consimțământul explicit • Asigură disponibilitatea și reziliența sistemelor și a serviciilor de prelucrare • Asigură siguranța accesului la date și transferului acestora • Asigură integritatea și confidențialitatea datelor • Asigură pseudonimizare și criptare • Asigură urmărirea duratei de viață și a ștergerii datelor • Asigură portabilitatea • Menține evidența prelucrării • Șterger a datelor	Resurse interne și/sau consultanță
Transferul datelor, inclusiv transferul internațional	Stabilirea măsurilor necesare pentru a putea desfășura în legalitate transferurile internaționale de date atât pe teritoriul EU, cât și în afara lui.	Resurse interne și/sau consultanță

ACȚIONEAZĂ

ETAPA	CE PRESUPUNE?	CUM OBȚINEM REZULTATUL?
Implementarea noilor proceduri de lucru	Odată definit cadrul de conformitate și măsurile necesare pentru a asigura conformitatea, vor fi făcuți pași concreți pentru aplicarea prevederilor GDPR.	Resurse interne și/sau consultanță
Implementarea /configurarea mijloacelor tehnice pentru protecția datelor	Implementarea/configurarea mijloacelor tehnice ce permit gestionarea datelor cu caracter personal în conformitate cu prevederile GDPR, ținând cont de volumul de date colectate, gradul de prelucrare a acestora, perioada de stocare și accesibilitatea acestora. Aceste mijloace trebuie să asigure cel puțin: • Obținerea consimțământului explicit • Disponibilitatea, integritatea și confidențialitatea datelor • Reziliența sistemelor și a serviciilor de prelucrare • Siguranța accesului la date și transferului acestora • Restricționarea prelucrării datelor • Pseudonimizarea și criptarea datelor • Urmărirea duratei de viață și ștergerea datelor • Portabilitatea datelor • Menținerea evidenței prelucrării datelor	Resurse interne Instrumente informatice pentru protecția datelor și/sau Consultanță tehnică
Modificarea infrastructurii	Modificarea infrastructurii poate lua forme foarte variate și, de cele mai multe ori, proporțional cu dimensiunea organizației. Modificarea poate însemna: îmbunătățirea componentelor existente, adăugarea de noi componente sau chiar înlocuirea unor componente. Integrarea de produse de securitate în infrastructura existentă este cea mai uzuală măsură ce se recomandă a fi adoptată.	Resurse interne și/sau consultanță

ACȚIONEAZĂ

GDPR
certSIGN

ETAPA	CE PRESUPUNE?	CUM OBȚINEM REZULTATUL?
Informarea permanentă a stakeholderilor	Un principiu cheie al GDPR este cel al responsabilității, fapt ce poate fi sinonim cu o conformitate demonstrabilă. Responsabilizarea se poate face prin informarea permanentă a factorilor de decizie din organizație, dar și a personalului cu privire la măsurile ce trebuie respectate și pașii ce trebuie urmați. O detaliere eficient structurată a GDPR ar trebui comunicată atât conducerii, cât și personalului întregii organizații, prin intermediul campaniilor interne de conștientizare care vor ajuta la educarea persoanelor și la sensibilizarea cu privire la schimbările iminente ale politicilor și procedurilor organizației. Informațiile relevante și documente de conformitate ale organizației trebuie structurate într-un pachet pentru a putea asigura accesibilitatea, menținerea și controlul cât mai facil al programul de conformitate. Informarea se poate referi la: • Politici, proceduri și instrumente • Măsuri de securitate • Inventarul de prelucrare a datelor • Alte părți interesate și informații de contact	Resurse interne și/sau consultanță
Numirea unui Responsabil cu protecția datelor (DPO - data protection officer), dacă e necesar	Responsabilul de protecție a datelor (DPO) are rolul de a supraveghea datele gestionate de organizație, strategia de protecție a acestora și punerea în aplicare a măsurilor necesare pentru a asigura conformitatea cu cerințele GDPR. În trei cazuri este ogligatorie numirea unui DPO: • Dacă prelucrarea datelor este efectuată de o autoritate publică (cu excepția instanțelor) • Dacă activitatea de bază a companiei private este reprezentată de operațiuni de prelucrare care implică monitorizare regulată și sistematică a persoanelor vizate pe scară largă • Dacă procesarea datelor sensibile implică și prelucrarea pe scară largă a unor categorii speciale de date sau informații referitoare la condamnări penale și/ sau infracțiuni DPO poate fi o persoană sau o organizație.	Resurse interne și/sau consultanță

MENȚINERE

ETAPA	CE PRESUPUNE?	CUM OBȚINEM REZULTATUL?
Audit	Testarea și evaluarea periodică a eficienței măsurilor de asigurare a securității datelor atât din punct de vedere tehnic, cât și din punct de vedere al procedurilor de lucru implementate în organizație.	Resurse interne Instrumente informatice pentru protecția datelor Consultanță tehnică
Plan de acțiune în caz de incident	În conformitate cu principiile GDPR, organizația ar trebui să dețină procedurile și procesele interne de notificare a unei situații de risc pentru drepturile și libertățile unei persoane, în maxim 72 de ore. Planul de acțiune în caz de incident include: • Măsuri de atenuare a efectelor adverse ale incidentelor • Măsuri de prevenire a incidentelor • Proceduri pentru restaurarea datelor și a accesului la ele • Proceduri pentru asigurarea rezilienței sistemelor și a serviciilor de prelucrare • Proceduri pentru raportare De asemenea, pentru a avea un plan eficient, în unele organizații se poate dovedi necesară implementarea unor instrumente și mijloace cu ajutorul cărora să se asigure: restaurarea datelor și a accesului la ele, dar și reziliența sistemelor și a serviciilor de prelucrare.	Resurse interne Instrumente informatice pentru restaurarea datelor și păstrarea rezilienței Consultanță tehnică

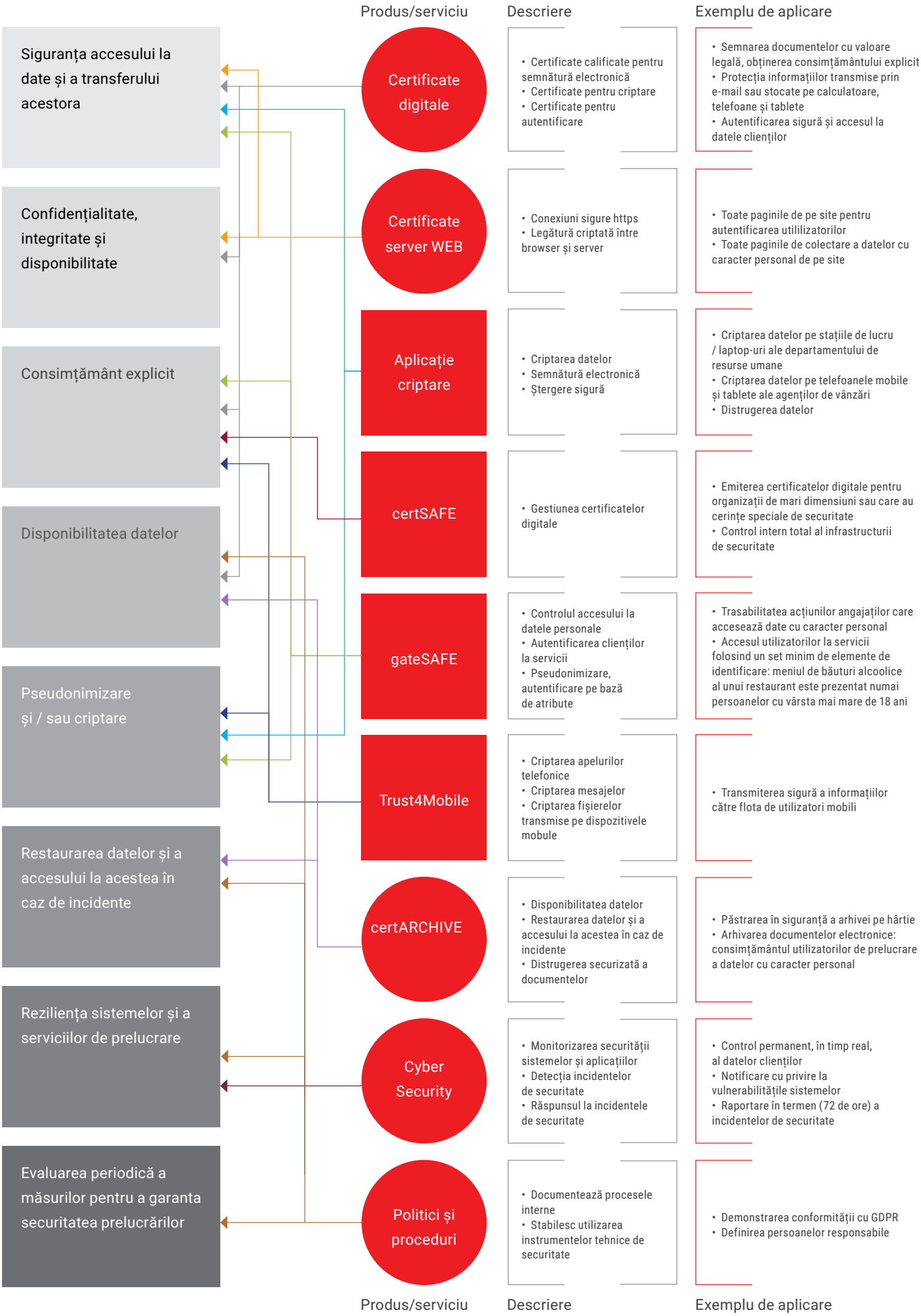
Cum verificăm conformitatea?

În prezent nu există, la nivel internațional și nici la nivel național, un standard sau un set de norme standardizate pentru a putea verifica conformitatea, ci există cerințe minime (bune practici) ce trebuie respectate. Prin textul Regulamentului sunt încurajate demersurile pentru:

• Realizarea de **Coduri de conduită** ce reprezintă norme de implementare a GDPR elaborate de asociații organizaționale sau alte organisme care reprezintă categorii de operatori sau de persoane împuternicite de operatori

• Instituirea de **Mecanisme de certificare** în domeniul protecției datelor, precum și de sigilii și mărci în acest domeniu, care să permită demonstrarea faptului că operațiunile de prelucrare efectuate de operatori și de persoanele împuternicite de operatori respectă Regulamentul

CONFORMITATE GDPR


Produs/serviciu
Descriere
Exemplu de aplicare
Siguranța accesului la date și a transferului acestora
Confidențialitate, integritate și disponibilitate
Consimțământ explicit
Disponibilitatea datelor
Pseudonimizare și / sau criptare
Restaurarea datelor și a accesului la acestea în caz de incidente
Rezilienta sistemelor și a serviciilor de prelucrare
Evaluarea periodică a măsurilor pentru a garanta securitatea prelucrărilor
Certificate digitale
• Certificate calificate pentru semnătură electronică
• Certificate pentru criptare
• Certificate pentru autentificare
• Semnarea documentelor cu valoare legală, obținerea consimțământului explicit
• Protecția informațiilor transmise prin e-mail sau stocate pe calculatoare, telefoane și tablete
• Autentificarea sigură și accesul la datele clienților
Certificate server WEB
• Conexiuni sigure https
• Legătură criptată între browser și server
• Toate paginile de pe site pentru autentificarea utililizatorilor
• Toate paginile de colectare a datelor cu caracter personal de pe site
Aplicație criptare
• Criptarea datelor
• Semnătură electronică
• Ștergere sigură
• Criptarea datelor pe stațiile de lucru / laptop-uri ale departamentului de resurse umane
• Criptarea datelor pe telefoanele mobile și tablete ale agenților de vânzări
• Distrugerea datelor
certSAFE
• Gestiunea certificatelor digitale
• Emiterea certificatelor digitale pentru organizații de mari dimensiuni sau care au cerințe speciale de securitate
• Control intern total al infrastructurii de securitate
gateSAFE
• Controlul accesului la datele personale
• Autentificarea clienților la servicii
• Pseudonimizare, autentificare pe bază de atribute
• Trasabilitatea acțiunilor angajaților care accesează date cu caracter personal
• Accesul utilizatorilor la servicii folosind un set minim de elemente de identificare: meniul de băuturi alcoolice al unui restaurant este prezentat numai persoanelor cu vârsta mai mare de 18 ani
Trust4Mobile
• Criptarea apelurilor telefonice
• Criptarea mesajelor
• Criptarea fișierelor transmise pe dispozitivele mobule
• Transmiterea sigură a informațiilor către flota de utilizatori mobili
certARCHIVE
• Disponibilitatea datelor
• Restaurarea datelor și a accesului la acestea în caz de incidente
• Distrugerea securizată a documentelor
• Păstrarea în siguranță a arhivei pe hârtie
• Arhivarea documentelor electronice: consimțământul utilizatorilor de prelucrare a datelor cu caracter personal
Cyber Security
• Monitorizarea securității sistemelor și aplicațiilor
• Detecția incidentelor de securitate
• Răspunsul la incidentele de securitate
• Control permanent, în timp real, al datelor clienților
• Notificare cu privire la vulnerabilitățile sistemelor
• Raportare în termen (72 de ore) a incidentelor de securitate
Politici și proceduri
• Documentează procesele interne
• Stabilesc utilizarea instrumentelor tehnice de securitate
• Demonstrarea conformității cu GDPR
• Definirea persoanelor responsabile
Produs/serviciu
Descriere
Exemplu de aplicare

De ce certSIGN?

Deși poate oferi instrumente care pot soluționa punctual una sau mai multe din prevederile GDPR, certSIGN propune clienților o abordare de ansamblu a acestor prevederi, având ca scop final menținerea permanentă a conformității cu regulamentul.

INSTRUMENTE TEHNICE

Produse

• **certSAFE** – confidențialitate, integritate
• **shellSAFE** – criptare, confidențialitate, integritate, consimțământ explicit
• **gateSAFE** – integritate, disponibilitate și reziliență a sistemelor și a serviciilor de prelucrare, siguranța accesului la date și a transferului acestora
• **Trust4Mobile** – confidențialitate, criptare

Servicii tehnice de securitate

Cybersecurity – evaluarea periodică a măsurilor pentru a garanta securitatea prelucrărilor; garantarea siguranței accesului la date și transferului acestora

SERVICII

Consultanță pentru:

• Analiza proceselor de lucru existente
• Inventarul datelor private existente și clasificarea acestora
• Inventarul fluxurilor de date actual, inclusiv al schimbului de date cu alți prelucrători
• Analiza modalității de gestionare a datelor pe întreaga lor durată de viață
• Evaluarea modului actual de prelucrare a datelor
• Audit al infrastructurii existente pentru evidențierea riscurilor actuale și pentru identificarea modalităților de corecție
• Audit pentru evaluarea periodică a măsurilor implementate (tehnice și organizatorice) pentru a garanta securitatea prelucrărilor

PROIECTE DE CERCETARE

• Dezvoltarea de mecanisme inovative de asigurare a conformității cu GDPR – ReCRED (www.recred.eu)

Resurse

Texul integral al Regulamentului: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC

Întrebări, răspunsuri, exemple: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations_en

Autoritatea Nationala de Supraveghere a Prelucrării Datelor cu Caracter Personal
http://www.dataprotection.ro/

Instrumente și mod de abordare a GDPR
https://www.certsign.ro/GDPR

Conformitatea cu GDPR.
DE UNDE ÎNCEPEM?

certSIGN