Sa ne pregatim pentru GDPR in 12 pasi

Acest articol prezinta 12 pasi de urmat, asa incat organizatiile din care facem parte sa se poata alinia cu cerintele noului Regulament de Protectie a Datelor Personale (GDPR), care intra in vigoare la 25 mai 2018.
Multe dintre conceptele si principiile existente in Actul de Protectie a Datelor (DPA) in vigoare la acest moment, cu privire la protectia datelor, raman neschimbate, asa ca daca organizatia dumneavoastra urmareste in totalitate conformitatea cu aceasta lege, atunci abordarea pe care trebuie sa o urmati cand GDPR va intra in vigoare (25 mai 2018), va fi aceea prin care, conformitatea cu acest regulament se va face pornind de la legislatia existenta de pana la acel moment.

Este foarte important sa planificati cu atentie modul in care veti aborda alinierea la noul regulament si sa obtineti implicarea si aprobarea persoanelor “cheie” din organizatia dumneavoastra.
Va trebui, de exemplu, sa implementati noi proceduri care sa aiba in vedere transparenta si drepturile indivizilor a caror date personale sunt prelucrate. In organizatiile mari, implementarea noilor proceduri ar putea costa destul de mult, datorita implicatiilor in activitatile de HR, IT, comunicare, etc.
GDPR pune accent foarte mare pe documentatia pe care prelucratorii de date sunt obligati sa o pastreze pentru a-si demonstra caracterul responsabil si implicarea. Conformitatea in legatura cu toate ariile expuse in acest document vor obliga organizatiile sa isi revizuiasca abordarea in legatura cu guvernarea si cum este privita protectia datelor. Unul din aspecte priveste modul in care contractele si alte documente legale trebuie revizuite in ceea ce priveste distribuirea datelor catre alte organizatii.
Unele articole din regulament vor avea un impact mai mare asupra unor organizatii decat asupra altora (de exemplu, furnizarea informatiilor pentru activitatile de profiling sau furnizarea datelor cu privire la copii), asa ca este folositor sa se mapeze impactul asupra modelului de business si sa se acorde ariilor mai afectate (influentate intr-o masura mai mare) o importanta deosebita in faza de planificare.

Cei 12 pasi de urmat sunt:

1. Constientizarea

Este necesar sa va asigurati ca factorii de decizie si persoanele cheie din organizatie sunt constienti ca legile in vigoare cu privire la protectia datelor se modifica cu noul regulament

GDPR. Ei trebuie sa fie constienti de impactul pe care il va avea aceasta modificare si sa identifice ariile de activitate care pot creea probleme in cee ace priveste conformitatea cu noul regulament.
Este deosebit de util sa se ia in vedere registrul de riscuri al companiei, daca acesta exista, de asemenea implementarea GDPR, poate avea implicatii deosebite cu privire la resursele umane, in special in companiile mari si organizatiile mai complexe.
Actiunile ce trebuie luate pentru conformitatea cu GDPR necesita timp, ceea ce face ca, daca organizatiile se vor lasa pe ultima suta de metri, va fi foarte dificil ca implementarea sa fie una reusita.

2. Tipurile de informatii existente

Este necesar sa documentati ce informatii in legatura cu datele personale exista, de unde vin si cui sunt distribuite. Este poate nevoie sa organizezi un audit in organizatie sau in anumite zone de business.
Una din cerintele GDPR este sa mentii inregistrari ale activitatilor de prelucrare de date, de exemplu, daca ai cumva date personale inexacte si acestea au fost distribuite unei alte organizatii, va fi nevoie sa comunici aceasta situatie organizatiei respective, pentru ca aceasta sa isi corecteze informatia.
Nu vei putea face acest lucru daca nu vei stii ce fel de informatii detii, de cand le ai si catre cine au fost distribuite. Toate aceste informatii trebuie documentate astfel incat sa poti dovedi conformitatea cu cerintele din noul regulament tinand cont de principiul responsabilitatii, de exemplu prin crearea de politici si proceduri.

3. Comunicarea informatilor confidentiale

Esti obligat sa revizuiesti actualele notificari confidentiale si sa pui in aplicare masurile necesare pentru conformitatea cu GDPR.
Cand colectezi date personale, in momentul de fata, esti obligat sa dai persoanelor informatii cu privire la identitatea ta si cum intentionezi sa folosesti datele lor personale, acest lucru se face cu ajutorul notificarilor. Conform cu noul regulament, trebuie aduse la cunostiinta si alte cateva lucruri cum ar fi dreptul tau legal de a prelucra date cu caracter personal, perioada in care vei tine aceste date si ca persoanele au dreptul sa faca plangere la autoritatea de supraveghere daca considera ca exista o problema in modul in care tu le prelucrezi datele.
GDPR cere ca informatiile ce vor fi comunicate sa fie facute intr-un limbaj concis, usor de inteles si clar.

4. Drepturile persoanelor

Este nevoie sa verifici procedurile actuale pentru a te asigura ca acopera toate drepturile persoanelor, incluzand situatiile in care ar trebui sa stergi datele personale sau sa le furnizezi datele in format electronic si in format comun.
GDPR cuprinde urmatoarele drepturi ale persoanelor:

- Dreptul de a fi informat
- Dreptul la acces
- Dreptul la ratificari

- Dreptul la stergere
- Dreptul la restrictionarea procesarii
- Dreptul la portabilitatea datelor
- Dreptul de a obiecta si
- Dreptul de a nu fi subiectul unor campanii de tip profiling

In general, drepturile persoanelor sunt cam aceleasi cu cele din actualul regulament DPA dar cu ceva imbunatatiri. Este momentul sa verificati procedurile si masurile ce trebuie luate pentru implementarea noilor cerinte, cum ar fi cele referitoare la dreptul de a cere ca datele personale sa fie sterse, raspunzand la intrebarile: “cum vor fi localizate acele date? Cine ia decizia de stergere?”

Dreptul la portabilitatea datelor este noua, se aplica doar la datele personale care au fost furnizate catre unui operator, cand prelucrarea este acceptata de catre persoana si cand prelucrarea este automata, iar datele trebuie furnizate intr-un mod acceptabil si gratuit.

5. Cererile de acces ale subiectilor

Esti obligat sa revizuiesti procedurile si sa planifici cum cererile indivizilor ale caror date le detii vor fi manipulate, astfel ca trebuie sa tii cont de urmatoarele reguli:

- In cele mai multe cazuri nu vei putea sa oferi serviciul contra cost;
- Ai o luna sa te conformezi cererii, acum durata este de 40 de zile;
- Poti refuza sau sa oferi acest serviciu contra cost daca cererea este nefondata sau excesiva;
- Daca refuzi o astfel de cerere, trebuie sa comunici motivul deciziei tale si totodata ca acestia au treptul sa se planga autoritatii de supraveghere, in interval de o luna.

6. Dreptul legal de prelucrare a datelor personale

Trebuie sa identifici dreptul tau legal de a prelucra date personale, sa documentezi si sa revizuiesti notificarile cu privire la securitatea datelor personale. Aceste informatii vor trebui comunicate celor ale caror date personale se prelucreaza, atunci cand situatia o cere.

7. Consimtamantul

Trebuie sa revizuiesti modul in care cauti, inregistrezi si administrezi consimtamantul persoanelor ale caror date personale sunt prelucrate si daca este necesar sa efectuezi modificari, in cazul in care conformitatea cu noul regulament o cere.

Consimtamantul trebuie oferit in libertate, specific, informat si fara echivoc, acesta trebuie sa fie verificabil, nu trebuie sa fie declarat daca nu este primit un raspuns, sau prin lipsa de activitate.

Nu esti obligat sa ceri acordul din nou daca il ai deja, dar trebuie sa te asiguri ca acest acord este dat in mod specific pentru fiecate tip de informative de date personale prelucrata, clar, documentat, evident si usor de retras. Daca nu, mecanismele existente trebuie revizuite si trebuie obtinut un nou consimtamant.

8. Copiii

Trebuie sa te gandesti totodata daca este necesar sa implementezi sisteme sau moduri prin care sa verifici varsta persoanelor a caror date le procesezi si sa obtii acordul parintilor sau a tutorelui.
Pentru prima data, regulamentul va aduce o protectie speciala datelor personale ale copiilor, in special in cazul retelelor de socializare. Daca organizatia ofera servicii online copiilor, vei avea nevoie de consimtamantul parintelui sau tutorelui pentru procesarea datelor personale pentru cei cu varsta mai mica de 16 ani.

9. Incidente cu privire la date personale

Trebuie sa te asiguri ca ai implementat proceduri pentru a detecta, raporta si investiga incidentele referitoare la datele personale.
Organizatiile trebuie sa notifice autoritatii de supraveghere in cazul in care au detectat un incident referitor la securitatea datelor personale nu mai tarziu de 72 de ore. Daca incidentul afecteaza dreptul la libertate al persoanelor ale caror date personale au fost afectate, acestia trebuie si ei notificati. In cazul in care, incidentul nu este raportat, se poate ajunge la plata de penalitati.
Companiile mari trebuie sa puna in practica politici si proceduri pentru a fi capabili sa administreze incidentele cu privire la securitatea datelor personale.

10. Protectia datelor prin constructie si analiza de impact al protectiei datelor

Aceasta practica se refera la cazurile in care noi aplicatii sunt dezvoltate si ca protectia datelor personale sa fie luata in calcul in faza de constructie a acestora.
GDPR stabileste ca buna practica, adoptarea din constructie a unei bune practici referitor la protectia datelor personale si totodata sa va realiza analiza de impact a confidentialitatii datelor, parte a acestei practici.
Analiza de impact in legatura cu confidentialitatea datelor personale este obligatorie in unele cazuri, atunci cand o noua tehnologie este dezvoltata, cand o operatiune de profiling poate sa afecteze persoanele ale caror date personale sunt prelucrate sau cand prelucrarea pe scara larga se face in legatura cu categoriile de date speciale.
Daca analiza de impact indica ca prelucrarea datelor aduce un risc major si ca nu se pot diminua efectele acelor riscuri, se poate consulta autoritatea de supraveghere pentru a se obtine avizul asupra prelucrarii datelor.

11. Ofiterii pentru protectia datelor

Organizatia trebuie sa numeasca un DPO care sa aiba responsabilitatea pentru conformitatea cu noul regulament si sa se analizeze unde se incadreaza acest rol in structura organizatiei.
DPO este numit obligatoriu in cazul in care vorbim de o autoritate publica, o organizatie care prelucreaza date cu caracter personal in mod sistematic si regulat pe scara larga sau o

organizatie care prelucreaza date speciale cu caracter personal cum ar fi informatii despre starea de sanatate sau cele despre condamnari.

12. Internationalizarea

Daca organizatia opereaza in mai multe tari membre EU, va fi necesar sa se determine cu care din autoritatile de supraveghere va fi necesar sa se comunice si sa se documenteze aceasta decizie. Autoritatea de supravehere va fi probabil cea din tara in care organizatia are birourile principale, acolo unde se iau deciziile in legatura cu scopul si mijloacele de prelucrare a datelor.