**CHESTIONAR AUDIT INIȚIAL CONFORMITATE GDPR**

Denumire companie:

Sediu/punct de lucru:

Activitate/activități:

|  |
| --- |
| **Capitolul A: Persoanele vizate și datele lor personale** |

1. Compania procesează date personale ale persoanelor fizice? Aceasta pot fi atat angajați, personal contractat, dar și clienții și alte persoane ale căror date personale ajung în posesia dumneavoastră.

* Da/Nu

2. Persoanele ale căror date personale le procesați, sunt localizate pe teritoriul UE?

* Da/Nu

3. Compania procesează date personale în numele și/sau pentru altă companie?

* Da/Nu

4. În ce scop sau scopuri sunt folosite datele personale colectate pentru propria companie? Enumerați-le pe toate.

* ………...
* ……….

5. În ce scop sau scopuri sunt folosite datele personale prelucrate în numele sau pentru altă companie? Enumerați-le pe toate.

* ………….

6. Prin ce modalități se colectează datele personale? (ex: convorbire directă, telefonică, prin e-mail, formular online mail, formular web etc.) Enumerați-le pe toate.

* …………..

7. Care este sursa/sursele informației prin care sunt colectate date personale? (ex: direct de la persoană, terți persoane fizice, terți companii) Enumerați-le pe toate.

|  |
| --- |
| **Capitolul B. Responsabilitatea în cadrul companiei** |

1. Managementul companiei conștientizează responsabilitatea pe care o are cu privire la protecția datelor personale? Bifați din lista de mai jos ceea ce există acum la nivelul companiei.

* Politici generale privind protecția datelor personale
* Obiective generale privind protecția datelor personale
* Responsabilități delegate prin fișa postului către persoanele care procesează date personale
* Audit de evaluare cu privire la riscurile privind procesarea datelor personale
* Proceduri de urmărire și securizare a fluxului de date personale
* Altele:
* Nimic din cele de mai sus

2. Compania are o persoană desemnată ca responsabil cu protecția datelor, identificată ca punct de contact pentru Autoritatea Națională de Supraveghere?

* Da
* Nu

3. Dacă da, cui este subordonat responsabilul pentru protecția datelor?

* …………….

4.Dacă în prezent nu aveți un Responsabil cu Protecția Datelor, aveți în vedere numirea unei persoane/companii care să îndeplinească un astfel de rol?

* Da
* Nu

|  |
| --- |
| **Capitolul C. Vedere generală asupra activităților de prelucrare** |

1. Activitățile de procesare a datelor personale din cadrul companiei sunt înregistrate în conformitate cu GDPR?

* Da. Este documentat acest lucru?
* Nu

2. Există o evidență a activităților de prelucrare, în care sunt identificate principiile de prelucrare a datelor personale?

* Da. Este documentat acest lucru?
* Nu

3. Principiile de protecție a datelor sunt luate în considerare la inițierea sau modificarea fiecărei activități/proceduri care presupune prelucrarea datelor personale (Privacy by Design)?

* Da. Este documentat acest lucru?
* Nu

4. Există în cadrul companiei o politică de confidențialitate adusă la cunoștința tuturor persoanelor ce prelucrează date personale?

* Da. Este documentat acest lucru?
* Nu

5. Dacă da, a fost actualizată în conformitate cu prevederile G.D.P.R?

* Da. Este documentat acest lucru?
* Nu

6. Cunoasteți care sunt temeiurile juridice ale colectării și prelucrării datelor personale?

* Da. Este documentat acest lucru?
* Nu

7. În cazul în care prelucrarea se bazează pe consimțământ, există suficientă claritate pentru ca individul să poată înțelege exact la ce va consimți?

* Da. Este documentat acest lucru?
* Nu

|  |
| --- |
| **Capitolul D. Prelucrarea datelor personale de către terți** |

1. Exista companii terțe, instituții sau persoane fizice autorizate care prelucrează date personale pentru companie?

* Da
* Nu

2. Aveți o imagine de ansamblu asupra operațiunilor întreprinse în acest sens de aceștia?

* Da
* Nu

3. Sunt încheiate contracte/acorduri scrise între părți, în cadrul cărora sunt identificate cu claritate aceste activități și sunt definite drepturile și obligațiile cu privire la prelucarea datelor personale?

* Da
* Nu

4. Aceste contracte/acorduri sunt revizuite și conțin clauze care le fac conforme cu GDPR?

* Da
* Nu

5. Acești terți folosesc la rândul lor o altă organizație care efectuează efectiv acest serviciu în numele lor?

* Da
* Nu
* Nu știu

|  |
| --- |
| **Capitolul E. Drepturile persoanelor vizate. Transparență, informare și asigurare.** |

1. Ați adaptat notificările companiei ce furnizează informații privind protecția datelor pentru persoanele vizate în cursul colectării de date în conformitate cu cerințele GDPR?

* Da
* Nu

2. În cazul în care nu le obțineți direct de la persoana vizată, din ce sursă provin datele personale pe care le prelucrați? Enumerați-le pe toate.

* ………….

3. Prin modalitatea de obținere a consimțământului, persoanele vizate sunt informate cu privire la obligațiile pe care le aveți, respectiv drepturile pe care le au?

* Da
* Nu

4. Aveți stabilită o procedură de răspuns prompt la cererile formulate de persoanele vizate cu privire la datele lor personale în conformitate cu GDPR?

* Da
* Nu

5. Sunt persoanele vizate informate că datele lor personale pot fi dezvăluite ca răspuns la o cerere ad-hoc a unei terțe părți?

* Da
* Nu

6. Există decizii cu privire la datele personale ale indivizilor, care se iau exclusiv prin mijloace pur automatizate, adică prin intermediul unui computer fără intervenție umană?

* Da
* Nu

7. Procedurile actuale ale companiei permit ca persoanele vizate să-și modifice / șteargă în mod direct datele lor personale?

* Da
* Nu

|  |
| --- |
| **Capitolul F. Responsabilitate, managementul riscului** |

1. Fiecare activitate de prelucrare de date personale este bine documentată prin informații scrise care arată baza legală a procesării, categoriile de date personale prelucrate, scopul etc?

* Da
* Nu

2. Ați efectuat o minimă evaluare a impactului protecției datelor?

* Da
* Nu

3. Ați stabilit o metodă adecvată de analiză a riscului în cadrul unei evaluări a impactului privind protecția datelor?

* Da
* Nu

4. Aveți stabilită o procedură pentru evaluarea impactului privind protecția datelor?

* Da
* Nu

5. Descrieți sumar traseul tuturor datelor personale prelucrate în companie, identificând tipul de date, departamentele care pot avea acces și numărul de persoane din fiecare departament la care acestea pot ajunge, conform exemplului de mai jos.

- date pers. clienți – secretariat (1), marketing (2), management (1), juridic (2), contabilitate (1)…

- date pers. Angajați – ….…

- date pers. Colaboratori – ….....

|  |
| --- |
| **Capitolul G. Breșe de date** |

1. Ați elaborat politici și proceduri pentru trasabilitatea fluxurilor de date, detectarea și tratarea breșelor de date? Dacă da, care sunt acestea?

* Da
* Nu

2. Sunteți siguri că notificarea privind o breșă de date poate fi transmisă către autoritatea națională de supraveghere în termen de 72 de ore conform GDPR?

* Da
* Nu

3. Ați determinat o modalitate adecvată în companie pentru a identifica și clasifica o prelucrare de date cu risc sau cu risc ridicat?

* Da
* Nu

4. Modul de gestionare a breșelor de date pe plan intern este stabilit printr-o procedură clară adusă la cunoștința tuturor persoanelor implicate?

* Da
* Nu

5. Ați desemnat o persoană în cadrul companiei care comunică cu autoritatea de supraveghere? Această persoană știe ce, când și cum trebuie să comunice?

* Da
* Nu

6. Știți exact care angajați au acces la informațiile personale din cadrul organizației / în afara organizației?

* Da
* Nu

|  |
| --- |
| **Capitolul H. Alte informații** |

Firma Dumneavoastra are website ? - Raspuns:

Aveti implementat sistem de chat online? - Raspuns:

Firma Dumneavoastra are pagina de Facebook ? - Raspuns:

Aveti implementat sistem de plata online? - Raspuns:

Aveti implementat sistem de plata POS? - Raspuns:

Aveti implementat sistem de newsletter catre clienti? - Raspuns:

Aveti implementat sistem de fidelizare cu carduri ? - Raspuns:

Aveti implementat sistem de direct mailing catre clienti? - Raspuns:

Aveti implementat sistem de monitorizare video in sediu? - Raspuns:

Aveti implementat sistem de monitorizare auto - GPS? - Raspuns:

Aveti externalizat serviciul de contabilitate? - Raspuns:

Aveti externalizate servicii de asistenta / consultanta / intretinere IT ? - Raspuns:

Aveti externalizat serviciul de marketing ? - Raspuns:

Stocati date in baze de date in format electronic ? - Raspuns:

Stocati date in baze de date in format fizic ( hartie)? - Raspuns:

Aveti implementat sistem de securitatea datelor? - Raspuns:

Aveti implementat sistem de garantare a calitatii serviciilor? (ISO/RBPF)? - Raspuns:

Aveti implementat un sistem de arhivare a documentelor ? - Raspuns:

Aveti implementat sistem de programare a clientilor / pacientilor ? - Raspuns:

Efectuati transmiteri de rapoarte catre terti ( Ex. Raportare ANAF, CNAS) ? - Raspuns:

Aveti formulare de obtinere a consimtamantului clientului ? - Raspuns:

Incheiati contracte cu persoane fizice ? - Raspuns:

Utilizati semnaturi electronice ? - Raspuns:

Sunteti operator care prelucreaza pe scara larga unele categorii speciale de date (origine etnica, orientare politica/religioasa, date genetice/biometrice, privind sanatate sau referitoare la infracțiuni) ? - Raspuns:

**Estimati va rog urmatoarele valori**

Numarul persoanelor vizate pentru care procesati date intr-o luna: - Raspuns:

Nr. de angajati: - Raspuns: