# EVALUAREA RISCURILOR DIN PUNCT DE VEDERE GDPR

**Nume Organizație: _____ Judet: _____**

**Domeniul de activitate: _____**

**Chestionarul completat se trimite prin email la adresa secretariat@ascpd.ro pana la 01.12.2018.**

**Fiecare organizatie care va transmite completat acest formular va primi in mod GRATUIT un raport de analiza a riscurilor si recomandari privind implementarea principiilor GDPR din partea Safetech Innovation si a Centrului pentru Protecția Datelor din cadrul UMFST, Asociatiei Specialistilor in Confidentialitate si Protectia Datelor.**

Prevederile Regulamentului (UE) 2016/679 sunt direct aplicabile in toate statele membre ale Uniunii Europene, incepand cu data de 25 mai 2018 si impun un set unic de reguli in ceea ce priveste protectia datelor cu caracter personal. Operatorii, indiferent de numarul de angajati sau de domeniul de activitate, au ca obligatie conform Regulamentului *"implementarea de masuri adecvate" care presupun prelucrarea datelor intr-un mod care asigura "securitatea datelor cu caracter personal, inclusiv protectia impotriva prelucrarii neautorizate sau ilegale si impotriva pierderii, a distrugerii sau a deteriorarii accidentale, prin luarea de masuri tehnice sau organizatorice corespunzatoare"*

Ca prim efect al impunerii Regulamentului, se observa clar, in piata, tentinta companiilor de a-si concentra atentia pe aspectul juridic al conformitatii, in detrimentul factorului tehnic. In fond, Regulamentul este despre a crea un nivel de securitate acceptabil din punct de vedere al riscului si despre uniformizarea nivelului de Securitate cibernetica in toata Uniunea Europeana. Ca DPO, este imperios necesar sa luati in considerare si sa urmariti implementarea ambelor tipuri de masuri: cele de natura juridica, dar si cele din domeniul securitatii informatiei.

**Înainte de completarea Chestionarului, vă rugăm să aveți în vedere următoarele definiții:**

1. "date cu caracter personal" înseamnă orice informaţii privind o persoană fizică identificată sau identificabilă ("persoana vizată"); o persoană fizică identificabilă este o persoană care poate fi identificată, direct sau indirect, în special prin referire la un element de identificare, cum ar fi un nume, un număr de identificare, date de localizare, un identificator online, sau la unul sau mai multe elemente specifice, proprii identităţii sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale;
2. "prelucrare" înseamnă orice operaţiune sau set de operaţiuni efectuate asupra datelor cu caracter personal sau asupra seturilor de date cu caracter personal, cu sau fără utilizarea de mijloace automatizate, cum ar fi colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, divulgarea prin transmitere, diseminarea sau punerea la dispoziţie în orice alt mod, alinierea sau combinarea, restricţionarea, ştergerea sau distrugerea;
3. "creare de profiluri" înseamnă orice formă de prelucrare automată a datelor cu caracter personal care constă în utilizarea datelor cu caracter personal pentru a evalua anumite aspecte personale referitoare la o persoană fizică, în special pentru a analiza sau prevedea aspecte privind performanţa la locul de muncă, situaţia economică, sănătatea, preferinţele personale, interesele, fiabilitatea, comportamentul, locul în care se află persoana fizică respectivă sau deplasările acesteia;

**Va rugam detaliati raspunsul Dumneavoastra pentru a a creste acuratetea raportului privind analiza riscurilor si recomandarile privind implementarea principiilor GDPR.**

| Nr Crt | Întrebare | Răspuns |
|---|---|---|
| **A. Structura organizatorică** | | |
| 1. | Numărul de posturi de conducere și numărul total de angajați cu contract individual de muncă și cu contract de colaborare pe durată determinată/nedeterminată | |
| 2. | Care este numărul aproximativ de clienți persoane fizice/ pacienți pe an | |
| 3. | Estimați extinderea geografică a prelucrării (local, regional, național) | |
| 4. | Transferați datele personale în state terțe? | |
| 5. | Există o persoană responsabilă cu politica de confidențialitate în cadrul companiei? | |
| 6. | Există un set de linii directoare interne pentru a proteja confidențialitatea datelor cu caracter personal? În caz afirmativ, acestea sunt puse la dispoziția angajaților și terților? | |
| **B. Date personale și prelucrarea acestora** | | |
| 1. | Ce date personale prelucrați pentru angajații dvs.? (nume, prenume, CNP, adresă, date biometrice, date privind starea de sănătate, cazier etc.) | |
| 2. | Ajungeți în posesia acestor date direct de la persoana vizată? | |
| 3. | Ce date personale prelucrați de la clienți persoane fizice/pacienți (nume, prenume, CNP, date privind starea de sănătate, date privind veniturile, numărul de copii etc.)? | |
| 4. | Ajungeți în posesia acestor date direct de la persoana vizată? | |
| 5. | Realizați o profilare a clienților/pacienților? (Prin intermediul unei prelucrări automate a datelor evaluați anumite aspecte personale) | |
| 6. | Aveți încheiate contracte cu persoane fizice? (altele decât cele ce privesc personalul) În caz afirmativ, care este obiectul acestora? | |
| 7. | Dețineți informații referitoare la fiecare activitate de prelucrare pentru dovada legalității prelucrării: (de exemplu, cu privire la scopurile, categoriile de date cu caracter personal, destinatari și/sau perioadele de păstrare a informațiilor)? | |
| 8. | Efectuați o prelucrare automatizată sau manuală a datelor cu caracter personal sau atât manuală cât și automatizată, după caz? | |

| | | |
|---|---|---|
| **9.** | **Aveți servicii subcontractate? Care sunt acestea? (pagina web, monitorizare video etc)** | |
| **10.** | **Aveți un sistem de supraveghere video instalat în cadrul companiei?** | |
| **11.** | **Personalul este supravegheat video în timpul orelor de muncă?** | |
| **12.** | **Utilizați un sistem GPS?** | |
| **13.** | **Distribuiți comunicări de marketing sau alte comunicări de business către clienți persoane fizice?** | |
| **14.** | **Folosiţi serviciile de Call Center?** | |
| **15.** | **Organizația deține website?** | |
| **16.** | **Aveți implementat sistem de chat online pe website?** | |
| **17.** | **Organizatia are pagină de Facebook?** | |
| **18.** | **Aveți implementat sistem de plată online?** | |
| **19.** | **Aveți implementat sistem de plată POS?** | |
| **20.** | **Aveți implementat sistem de fidelizare cu carduri ?** | |
| **21.** | **Ați adaptat consimțământul pentru clienți și potențiali viitori clienți conform cerințelor Art. 7 și Art. 13 din RGPD (în special: obligațiile de informare extinsă, inclusiv în ceea ce privește dreptul de retragere al consimțământului în orice moment)?** | |
| **22.** | **Aveți implementat un sistem de arhivare? (atât fizic, cât și electronic)** | |
| **23.** | **Există o procedură specifică pentru modul de acces la datele cu caracter personal atât ale angajaților, cât și ale clienților?** | |
| **24.** | **Aveți implementată o procedură privind soluționarea cererilor pentru exercitarea drepturilor ce privesc datele cu caracter personal?** | |
| **25.** | **Există o procedură specifică în cazul retragerii consimțământului persoanei vizate cu privire la prelucrarea datelor sale cu caracter personal?** | |
| **26.** | **Ați avut vreo reclamație pe protecția datelor sau aveți litigii pe rol între angajat și angajator indiferent de natura litigiului?** | |
| **C. Securitatea informațiilor** | | |
| **1.** | **Aveți stabilit un sistem de management al securității informațiilor? Dacă da, prin ce standarde ?(ex. ISO 27000 sau 27001)** | |

| | | |
|---|---|---|
| **2.** | **Au fost implementate politici/proceduri de securitate?** | |
| **3.** | **S-a realizat o instruire a angajaților cu privire la problematica protecției datelor cu caracter personal?** | |
| **4.** | **V-ați confruntat cu incidente de securitate?** | |
| **5.** | **Ați implementat un Plan de reacție la incidente de securitate?** | |
| **6.** | **Folositi aplicații livrate din cloud (ex: HRM in cloud, CRM in cloud, ERP in cloud, Dropbox, WhatsApp, email etc).** | |
| **7.** | **Utilizati adrese de email personal (@yahoo.com, @gmail.com) in interes profesional** | |
| **8.** | **Toate spatiile in care isi desfasoara activitatea organizatia Dumneavoastra sunt in proprietate sau exista contracte de detinere legala a acestora ?** | |
| **9.** | **Va rog deschieri procedura de arhivare si stocare a documentelor ( atat fizic cat si electronic)** | |
| **10.** | **Echipamentele de pe care personalul isi desfasoara actvitatea ( unde sun procesate date) sunt in proprietatea Organizatiei Dumneavoastra ? ( laptop, telefon)** | |
| **11.** | **Toate echipamentele dispun de software licentiat ?** | |
| **12.** | **Aveti implementate sisteme tehnice de protectie informatica ( antivirus, antimalware etc) ?** | |

Acest document a fost realizat cu contribuția

- Centrului pentru Protecția Datelor din cadrul UMFST,
- Asociatiei Specialistilor in Confidentialitate si Protectia Datelor
- Safetech Innovations, care își mențin drepturile de autor.

**Rezultatele vor fi prelucrate in scop statistic pentru a realiza un proiect de cercetare privind masurile adoptate in cadrul unitatilor sanitare din Romania in vederea implementarii principiilor GDPR, fara a disemina numele organizatiilor sau alte informatii care pot duce la identificarea acestora.**