Anexa 1. Instrucțiunea nr. .....

Regulamentul General privind Protectia Datelor (GDPR) nr. 679/2016

Legislatia romaneasca privind datele cu caracter personal

Trecut

Directiva 95/46/CE privind ptotecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date

Legea 677/2001 privind protecția datelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date

Legislatia romaneasca privind datele cu caracter personal

Prezent

Regulamentul 2016/679/UE 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

Legea nr. 190/2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului 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 abtrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor);

Ce este GDPR-UL?

- GDPR- ul este un **Regulament**, nu Directiva!!!!
- Reprezinta o singura lege ce se aplica unitar in toata Uniunea Europeana.
- Nu se armonizeaza cu legislatia nationala ci se preia cu totul de catre aceasta.
- O interpretare unitara a Regulamentului de catre toate autoritatile de supraveghere din tarile membre ale UE cat si de catre statele terte.
- Crearea Bordului European pentru Protectia Datelor (EDPB) – organismul european insarcinat cu aplicarea GDPR-ului

De ce vorbim despre GDPR?

Autoritatea Nationala de Supraveghere a Prelucrării Datelor cu Caracter Personal poate:

- ✓ Să emită avertizări
- ✓ Să dea dispoziții
- ✓ Să oblige Operatorul să informeze persoana vizată cu privire la încălcarea protecției datelor
- ✓ Să limiteze sau să interzică prelucrarea datelor
- ✓ Să dispună rectificarea sau ștergerea datelor
- ✓ **Să amendeze Operatorul pentru prelucrarea incorectă a datelor cu caracter personal.**

Activitatea ANSPDCP – iulie 2019?

Prima amendă data de ANSPDCP 27.06.2019,

- ANSPDCP a finalizat o investigație la operatorul UNICREDIT BANK S.A. și a constatat că acesta a încălcat prevederile art. 25 alin. (1) din Regulamentul (UE) 2016/679

- Operatorul a fost sancționat contravențional cu amendă în cuantum de **613.912 lei**, echivalentul în euro al sumei de **130.000 euro**.

Motivarea sancționării:

- Sancțiunea a fost aplicată UNICREDIT BANK S.A. ca urmare a neaplicării măsurilor tehnice şi organizatorice adecvate, atât în momentul stabilirii mijloacelor de prelucrare, cât şi în cel al prelucrării în sine, destinate să pună în aplicare în mod eficient principiile de protecție a datelor, precum reducerea la minimum a datelor, şi să integreze garanțiile necesare în cadrul prelucrării, pentru a îndeplini cerințele RGPD şi a proteja drepturile persoanelor vizate.

Activitatea ANSPDCP – iulie 2019?

Prima amendă data de ANSPDCP 27.06.2019

Sesizarea ANSPDCP:

- Sancțiunea a fost aplicată ca urmare a unei sesizări a Autorității Naţionale de Supraveghere din data de 22.11.2018 prin care se semnala faptul că datele privind CNP-ul și adresa persoanelor care efectuau plăți la UNICREDIT BANK S.A., prin intermediul tranzacțiilor on-line, erau dezvăluite către beneficiarul tranzacției, prin formularele de extras de cont/detalii.

Justificarea amenzii:

- Potrivit art. 5 alin. 1 lit. c) din RGPD (”Principii legate de prelucrarea datelor cu caracter personal”), operatorul avea obligația de a prelucra date limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate datele.

Activitatea ANSPDCP – iulie 2019?

Prima amendă data de ANSPDCP 27.06.2019,

- În același timp, considerentul (78) din Regulament precizează: ”*Protecția drepturilor și libertăților persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal necesită adoptarea de măsuri tehnice și organizatorice corespunzătoare pentru a se asigura îndeplinirea cerințelor din prezentul regulament. Pentru a fi în măsură să demonstreze conformitatea cu prezentul regulament, operatorul ar trebui să adopte politici interne și să pună în aplicare măsuri care să respecte în special principiul protecției datelor începând cu momentul conceperii și cel al protecției implicite a datelor. Astfel de măsuri ar putea consta, printre altele, în reducerea la minimum a prelucrării datelor cu caracter personal, pseudonimizarea acestor date cât mai curând posibil, transparența în ceea ce privește funcțiile și prelucrarea datelor cu caracter personal, abilitarea persoanei vizate să monitorizeze prelucrarea datelor, abilitarea operatorului să creeze elemente de siguranță și să le îmbunătățească. Atunci când elaborează, proiectează, selectează și utilizează aplicații, servicii și produse care se bazează pe prelucrarea datelor cu caracter personal sau care prelucrează date cu caracter personal pentru a-și îndeplini rolul, producătorii acestor produse și furnizorii acestor servicii și aplicații ar trebui să fie încurajați să aibă în vedere dreptul la protecția datelor la momentul elaborării și proiectării unor astfel de produse, servicii și aplicații și, ținând cont de stadiul actual al dezvoltării, să se asigure că operatorii și persoanele împuternicite de operatori sunt în măsură să își îndeplinească obligațiile referitoare la protecția datelor. Principiul protecției datelor începând cu momentul conceperii și cel al protecției implicite a datelor ar trebui să fie luate în considerare și în contextul licitațiilor publice.*”

Activitatea ANSPDCP – iulie 2019?

A doua amendă data de ANSPDCP 02.07.201

- ANSPDCP a finalizat o investigație la operatorul WORLD TRADE CENTER BUCHAREST S.A. și a constatat că acesta a încălcat prevederile art. 32 alin. (4) raportat la art. 32 alin. (1) și alin. (2) din Regulamentul General privind Protecția Datelor, referitoare la securitatea prelucrării.

- Operatorul WORLD TRADE CENTER BUCHAREST S.A. a fost sancționat contravențional cu amendă în cuantum de 71.028 lei, echivalentul sumei de 15.000 euro.

- Încălcarea securității datelor cu caracter personal a constat în faptul că o listă printată pe suport de hârtie, utilizată pentru verificarea clienților care serveau micul dejun și care conținea date cu caracter personal ale unui număr de 46 de clienți, cazați la unitatea hotelieră aparținând WORLD TRADE CENTER BUCHAREST S.A., a fost fotografiată de către persoane neautorizate din afara societății, ceea ce a condus la dezvăluirea în mediul on-line a datelor cu caracter personal ale unor clienți, prin publicare.

,

Activitatea ANSPDCP – iulie 2019?

A doua amendă data de ANSPDCP 02.07.201

Motivul sancționării:

- Operatorul WORLD TRADE CENTER BUCHAREST S.A. a fost sancționat deoarece nu a luat măsuri pentru a se asigura că angajații săi care au acces la date cu caracter personal nu le prelucrează decât la cererea sa, potrivit legii.

- De asemenea, operatorul nu a implementat măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător riscului prelucrării generat în special, în mod accidental sau ilegal, de divulgarea neautorizată sau accesul neautorizat la datele cu caracter personal. Aceasta a condus la accesul neautorizat la datele cu caracter personal ale unui număr de 46 de clienți ai WORLD TRADE CENTER BUCHAREST S.A și divulgarea neautorizată a acestor date, în mediul on-line, ceea ce a condus la afectarea drepturilor la viață privată și la protecția datelor cu caracter personal, garantate de art. 7 și art. 8 din Carta Drepturilor Fundamentale a Uniunii Europene și de art. 16 din Tratatul privind Funcționarea Uniunii Europene.

Activitatea ANSPDCP – iulie 2019?

A doua amendă data de ANSPDCP 02.07.201

Sesizarea ANSPDCP:

- Autoritatea Națională de Supraveghere a efectuat investigația ca urmare a transmiterii de către WORLD TRADE CENTER BUCHAREST S.A. a unei notificări privind încălcarea securității datelor cu caracter personal prin completarea formularului privind încălcarea securității datelor cu caracter personal, prevăzută de art. 33 din RGPD.

Justificarea amenzii:

- Regulamentul General privind Protecția Datelor instituie, prin art. 24, principiul responsabilității operatorului, potrivit căruia: ”*Ținând seama de natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și de riscurile cu grade diferite de probabilitate și gravitate pentru drepturile și libertățile persoanelor fizice, operatorul pune în aplicare măsuri tehnice și organizatorice adecvate pentru a garanta și a fi în măsură să demonstreze că prelucrarea se efectuează în conformitate cu prezentul regulament. Respectivele măsuri se revizuiesc și se actualizează dacă este necesar.*”
- Totodată, considerentul (75) din RGPD

Activitatea ANSPDCP – iulie 2019?

A treia amendă data de ANSPDCP 05.07.201

- ANSPDCP a finalizato investigație la operatorul LEGAL COMPANY & TAX HUB SRL și a constatat că acesta a încălcat prevederile art. 32 alin. (1) și alin. (2) din Regulamentul (UE) 2016/679

- Operatorul LEGAL COMPANY & TAX HUB SRL a fost sancționat contravențional cu amendă în cuantum de **14.173,50 lei**, echivalentul sumei de **3.000 euro**.

Motivarea sancționării:

- Sancțiunea a fost aplicată operatorului întrucât nu a implementat măsuri tehnice și organizatorice adecvate, în vederea asigurării unui nivel de securitate corespunzător riscului prelucrării. Aceasta a condus la divulgarea neautorizată și accesul neautorizat la datele cu caracter personal ale persoanelor care au efectuat tranzacții recepționate de site-ul avocatoo.ro (nume, prenume, adresa de corespondență, email, telefon, loc de muncă, detalii tranzacții efectuate), documente accesibile public, în perioada 10 decembrie 2018 – 1 februarie 2019.

Activitatea ANSPDCP – iulie 2019?

A treia amendă data de ANSPDCP 05.07.201

Sesizarea ANSPDCP:

- Autoritatea Națională de Supraveghere a aplicat sancțiunea ca urmare a unei sesizări din data de 10.12.2018 prin care se semnala faptul că un set de fișiere cu privire la detaliile tranzacțiilor recepționate de site-ul avocatoo.ro, ce conținea nume, prenume, adresa de corespondență, email, telefon, loc de muncă și detalii tranzacții efectuate, era accesibil public prin intermediul a două link-uri.

Justificarea amenzii:

- Conform 5 alin. 1 lit. f) din RGPD, operatorul avea obligația de a prelucra date într-un mod care asigură securitatea adecvată a datelor cu caracter personal, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luarea de măsuri tehnice sau organizatorice corespunzătoare (”integritate și confidențialitate”).

Activitatea ANSPDCP – iulie 2019?

A treia amendă data de ANSPDCP 05.07.201

Justificarea amenzii:

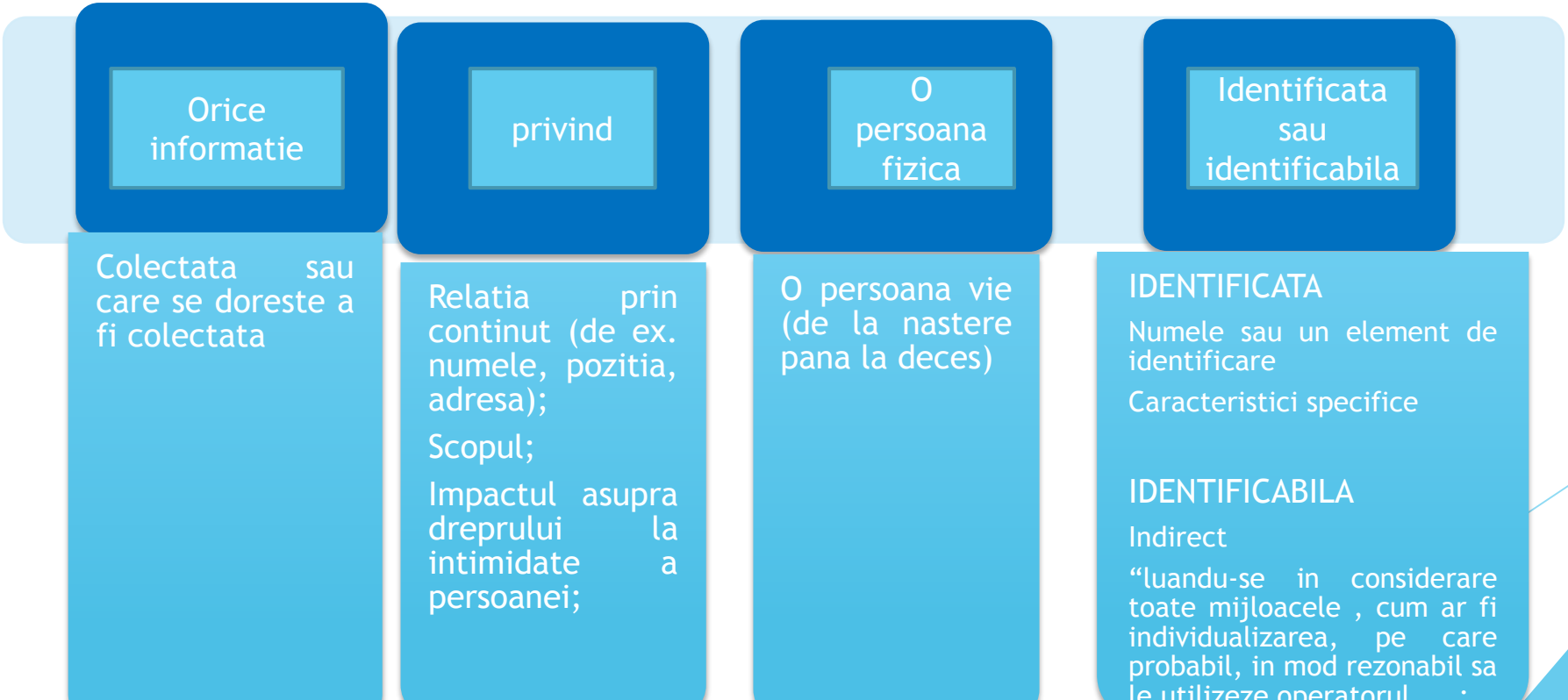
- De asemenea, Regulamentul General privind Protecţia Datelor prevede, în art. 32 că:

”(1) Având în vedere stadiul actual al dezvoltării, costurile implementării și natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și riscul cu diferite grade de probabilitate și gravitate pentru drepturile și libertățile persoanelor fizice, operatorul și persoana împuternicită de acesta implementează măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător acestui risc, incluzând printre altele, după caz:
a) pseudonimizarea și criptarea datelor cu caracter personal;
b) capacitatea de a asigura confidențialitatea, integritatea, disponibilitatea și rezistența continue ale sistemelor și serviciilor de prelucrare;c) capacitatea de a restabili disponibilitatea datelor cu caracter personal și accesul la acestea în timp util în cazul în care are loc un incident de natură fizică sau tehnică;
d) un proces pentru testarea, evaluarea și aprecierea periodice ale eficacității măsurilor tehnice și organizatorice pentru a garanta securitatea prelucrării.

(2) La evaluarea nivelului adecvat de securitate, se ține seama în special de riscurile prezentate de prelucrare, generate în special, în mod accidental sau ilegal, de distrugerea, pierderea, modificarea, divulgarea neautorizată sau accesul neautorizat la datele cu caracter personal transmise, stocate sau prelucrate într-un alt mod.”

Ce intelegem prin data personala?

"Orice informatie privind o persoana fizica identificata sau identificabila ("persoana vizata") *" art.4.1 din GDPR*



Conform Cartei Fundamentale a Drepturilor Omului

Intimitatea

- Respect pentru ……
  - Viata privata
  - Viata de familie
  - Casa
  - Comunicatii

Protectia datelor

- Protectia datelor personale
- Procesarea corecta a acestora
- Scopuri precise
- Consimtamant sau legitimitate
- Acces si rectificare

Extinderea acestor termeni conform GDPR

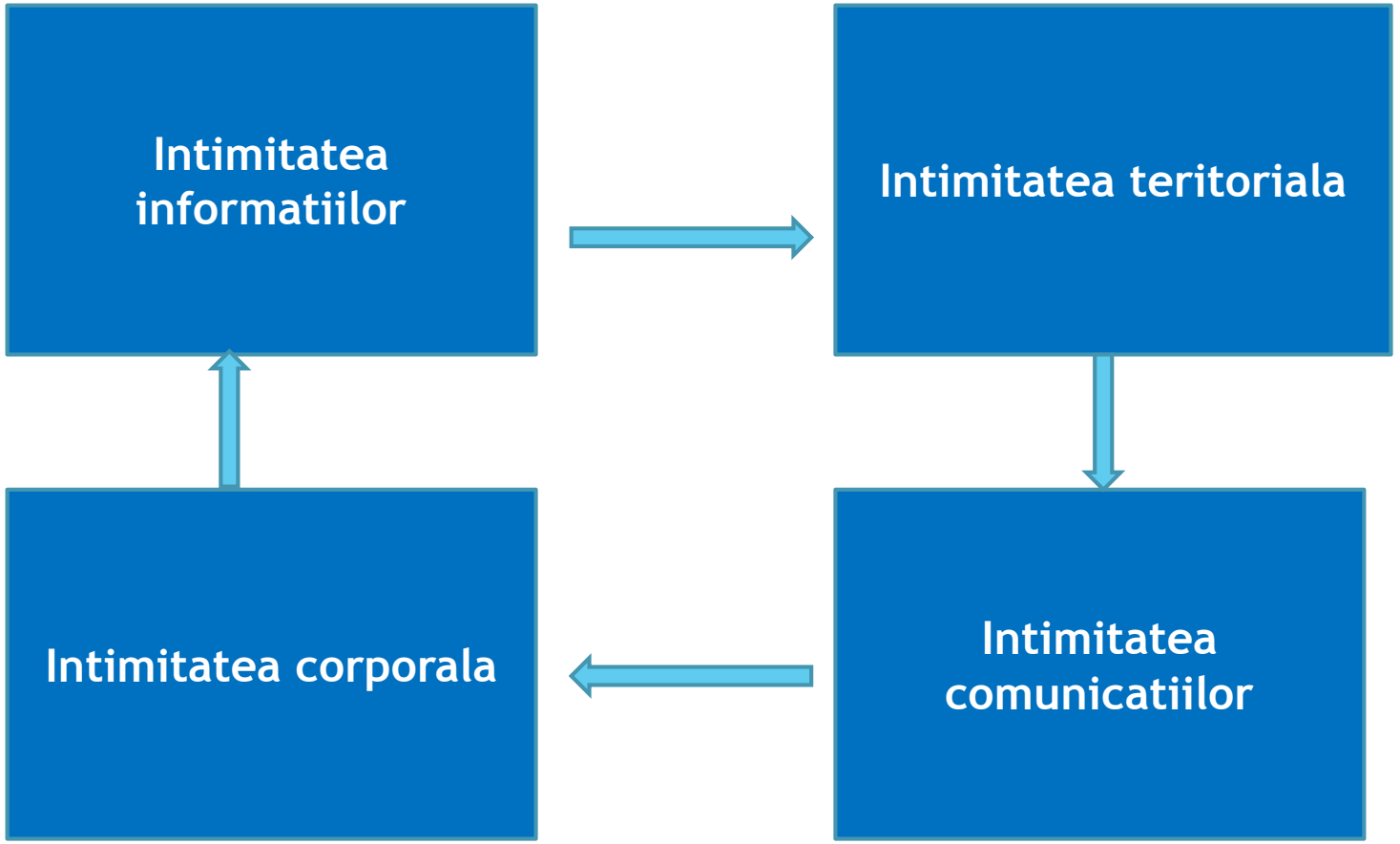
Intimitatea

- Intimitatea informatiilor
- Intimitatea teritoriala
- Intimitatea corporala
- Intimitatea comunicatiilor

Protectia datelor

- Transparenta
- Baza legala pentru procesare
- Proportionalitate
- Exactitatea datelor si actualitatea lor
- Dreptul de corectare si de a obiecta
- Securitate
- Portabilitatea restrictiilor

Tipurile de intimitate?



Tipurile de intimitate?

- **Intimitatea informatiilor:** privind stabilirea regulilor care reglementeaza colectarea si prelucrarea datelor cu caracter personal.
  - date financiare, date medicale, inregistrari privind activitatile unei persoane pe internet
- **Intimitatea teritoriala:** referitoare la plasarea limitelor privind patrunderea in spatiul personal al individului.
  - prin spatiu personal se poate intelege: acasa, la birou sau chiar in public
  - Invadarea acestuia poate avea loc prin supraveghere video, verificarea ID-urilor, instalarea GPS-ului pe masina, etc

Tipurile de intimitate?

- **Intimitatea corporala:** se concetreaza pe existenta fizica a persoanei si a intruziunilor asupra acesteia.
  - testare genetica, testare dopaj, explorarea anumitor cavitati ale corpului, masuri profilactice, informatii referitoare la avorturi, adoptie
- **Intimitatea comunicatiilor:** se refera la protectia mijloacelor de comunicatie.
  - Continul: e-mail-urilor, al conversatiilor telefonice, sau al oricarui alt mijloc de comunicare

Exemple de date personale

Generale

- Nume
- Gen
- Varsta si data nasterii
- Stare civila
- Cetatenie
- Limbi vorbite
- Statutul de veteran
- Statutul de handicapat
- IP-ul

Organizationale

- Adresa personala / a locului de munca
- Numarul de telefon personal / de la birou
- Adresa de email personala / de la locul de munca
- Numerele interne de identificare (ex. nr de telefon interior)
- Numerele de identificare emise conform legislatiei (ex. CNP, marca angajatului)
- Informatii privind verificarea identitatii

Categorii speciale de date personale

Conform art. 9.1 din GDPR – “Date sensibile”:

- Date personale ce dezvaluie:
  - Rasa si etnie
  - Opinii politice
  - Religie si alte credinte filosofice
  - Apartenenta la un sindicat

Categorii speciale de date personale

Conform art. 4.14 din GDPR – “Date biometrice”

- Date ce ajuta la identificarea unicitatii unei persoane fizice:
  - Imagini faciale
  - Datele dactiloscopice

- Date referitoare la:
  - Sănatate (preambulul 35 si art 4.15 din GDPR)
  - Viața sexuală
  - Orientarea sexuală

Cui se aplica RGDP-ul?

Se aplică atat entităților cu mai puțin de 250 angajați cât și celor ce depășesc acest plafon, dacă prelucrarea datelor este susceptibilă să genereze un risc pentru drepturile persoanelor vizate sau include categorii speciale de date

Se aplica ca proces de operare a datelor cu caracter personal si pentru persoane fizice, cat si pentru mediul de afaceri.

Procesarea datelor personale

“Orice operatiune sau set de operatiuni operata efectuata asupra datelor cu caracter personal, sau asupra seturilor de dare cu caracter personal, cu sau fara utilizarea de mijloace automatizate.” art 4.2 din GDPR.

Prin procesarea datelor se intelege absolut orice actiune asupra datei cu caracter personal din momentul din care aceasta intra in companie.

Simpla utilizare a unei informatii reprezinta o procesare a datei.

Datele se proceseaza conform principiilor:

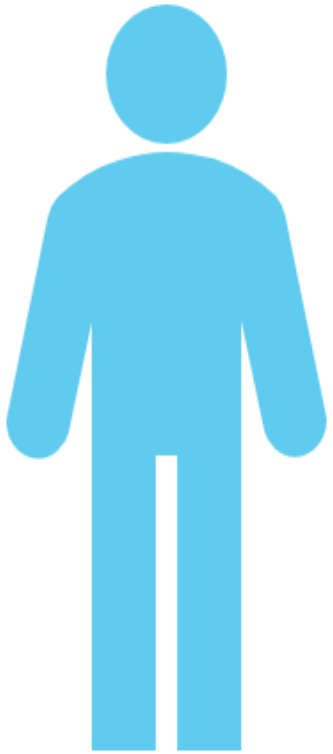
- Minimalizarea datelor
- Proporționalitate

Procesarea datelor personale

Prin procesare se intelege:

- **Colectarea**
- Inregistrarea
- Organizarea
- Structurarea
- **Stocarea**
- Adaptarea sau modificarea
- Extragerea
- Consultarea
- **Utilizarea**
- Divulgarea prin transmitere
- Diseminarea sau punerea la dispozitie in orice alt mod
- Alinierea sau combinarea
- Restrictionarea
- Stergerea sau distrugerea

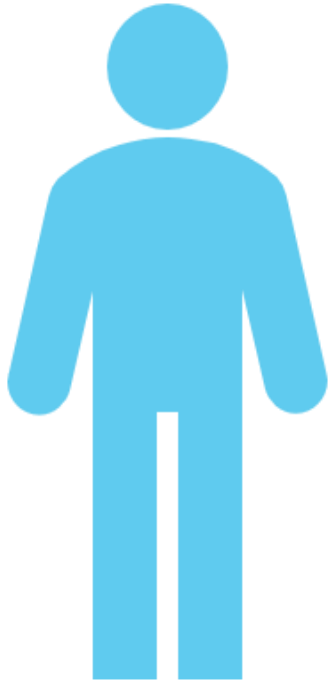
Procesarea datelor personale – Principiile procesarii



- **Limitarea colectarii:**
  - Daca nu iti este necesara, nu o colecta
  - Odata ce ai obtinut-o protejeaz-o
  - Consimtamant sau informare

- **Calitatea datelor:**
  - Trebuie sa fie relevante pentru scopul colectarii
  - Trebuie sa fie corecte, complete si bine pastrate

Procesarea datelor personale – Principiile procesarii



- Intotdeauna inainte de colectarea datelor trebuie facut un “Test Balance” referitor la:
  - ✓ Sunt necesare aceste date?
  - ✓ Pot sa le obtin prin alte metode?
  - ✓ Afecteaza drepturile persoanei?
- Trebuie demonstrat “ interesul legitim’ conform caruia interesul tau business este mai important si nu interfereaza cu dreptul persoanei de a avea o viata privata.

Procesarea datelor - Drepturile persoanelor

Operatorul are 2 mari obligatii:

- De a furniza informatii (art 13 – 14)
- De a comunica persoanei vizate despre drepturile sale.

Drepturile persoanelor

- ✓ Transparenta art. 12 si dreptul la informare – art. 13 – 14
- ✓ Dreptul la acces – art. 15
- ✓ Dreptul la rectificare – art. 16
- ✓ Dreptul la stergerea datelor (dreptul de a fi uitat) – art. 17
- ✓ Dreptul la restrictionarea prelucrarii – art. 18
- ✓ Dreptul la portabilitatea datelor – art. 20
- ✓ Dreptul la opozitie – art. 20
- ✓ Dreptul de a nu face obiectul unei decizii bazate exclusive pe prelucrarea automata, inclusiv crearea de profiluri – art. 21
- ✓ Restrictionarea exercitiului drepturilor. Informarea cu privire la incidentele de securitate – art. 34

Procesarea datelor – Consimtamantul

Pentru orice activitate realizata asupra datelor personale este nevoie de consimtamantul persoanei vizate – art. 7 din RGPD.

- Consimtamantul poate fi luat in considerare, doar cand cele doua parti care sunt considerate egale.

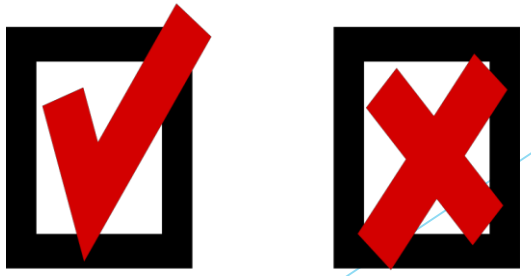
Consimtamantul NU poate fi aplicat in relatia angajator - angajat deoarece se considera ca cele doua entitati nu sunt egale, deci angajatorul trebuie sa gaseasca alte mijloace prin care isi notifica angajatul privind procesarea datelor acestuia cu caracter privat – de ex. prin actualizarea fișelor de post, proceduri interne, politica instituției privind confidentialitatea datelor.

Procesarea datelor - Consimtamantul

Orice manifestare de voință liberă, specifică, informată și lipsită de ambiguitate a persoanei vizate prin care aceasta acceptă, printr-o declaratie sau actiune fără echivoc ca datele cu caracter personal care o privesc să fie prelucrate.

Procesarea datelor - Consimtamantul

- Declarație/acord scris
- Prin bifarea unei opțiuni pe site
- Pentru prelucrarea în scopuri multiple trebuie să existe consimțământ pentru toate activitățile de prelucrare a datelor (fiind precizat fiecare scop în parte)



Procesarea datelor - Consimtamantul

- ✓ Operatorul trebuie să demonstreze existența consimțământului.
- ✓ Solicitarea acordului să fie în formă inteligibilă și ușor accesibilă, limbaj clar lipsit de ambiguitate.
- ✓ Consimțământul poate fi retras în orice moment și va afecta doar prelucrările ulterioare.
- ✓ Retragerea consimțământului trebuie să fie la fel de simplă și ușoară ca si acordarea acestuia
- ✓ Nu este admis consimțământul condiționat. (ex. In baza consimtamantului tau vei primi o reducere de 5%).
- ✓ Atunci când nu este nevoie de Consimțământ, va fi nevoie de **Informarea** persoanei vizate (art. 13 din RGPD)

Procesarea datelor – Consimtamantul / Informarea persoanei vizate

Persoana vizată trebuie să fie informată referitor la:

- ✓ Identitatea și datele de contact ale Operatorului
- ✓ Scopurile în care sunt prelucrate datele și temeiul juridic al prelucrării
- ✓ Destinatarii și/sau categoriile de destinatari ai datelor
- ✓ Perioada pentru care vor fi stocate sau criteriile utilizate pentru a stabili această perioadă.

Procesarea datelor – Consimtamantul – Informarea persoanei vizate

Persoana vizată trebuie să fie informată referitor la:

- ✓ Faptul că persoana vizată are dreptul de acces la date și de a le porta, dreptul de rectificare, dreptul de ștergere, de restricționare, de a se opune prelucrării, de a-și retrage consimțământul, după caz.
- ✓ Datele de contact ale DPO - ului
- ✓ Dreptul de a formula plângere unei autorități de supraveghere.
- ✓ Dacă furnizarea de date reprezintă o obligație legală, contractuală sau necesară încheierii unui contract și care pot fi consecințele nerespectării obligației.

Procesarea datelor – Consimtamantul – Informarea persoanei vizate

- ✓ **În situația în care consimțământul este obținut și în numele unor terți, informarea prealabilă trebuie să includă identitatea terților!** (ex. Firma imputernicita care gestioneaza site-ul).

- ✓ **Nu este acceptată doar simpla indicare a unei categorii!**

DPO (Data Protection Officer)

este obligatorie desemnarea unui Responsabil protecția datelor cu caracter personal

Este subordonat direct Ministrului

Este independent

Nu este in conflict de interese prin indeplinirea altor sarcini

Comunica cu intreg personalul

Are acces in celelalte departamente, pentru informații privind personalul și operațiunile de prelucrare a datelor ale acestora

Trebuie sa i se aloce resursele necesare financiare, infrastructurale si umane, pt realizarea sarcinilor

Nu raspunde personal pentru nerespectarea GDPR-ului de către instituție

Va benefica de formare continua

Nu poate fi concediat pentru indeplinirea sarcinilor

DPO (Data Protection Officer)

este obligatorie desemnarea unui Responsabil protecția datelor cu caracter personal

Are rol consultativ referitor la obligațiile specifice RGDP

Monitorizeaza realizarea DPIA

Elaborează Registrul de Evidență a prelucrării datelor cu caracter personal

Gestioneaza riscurile

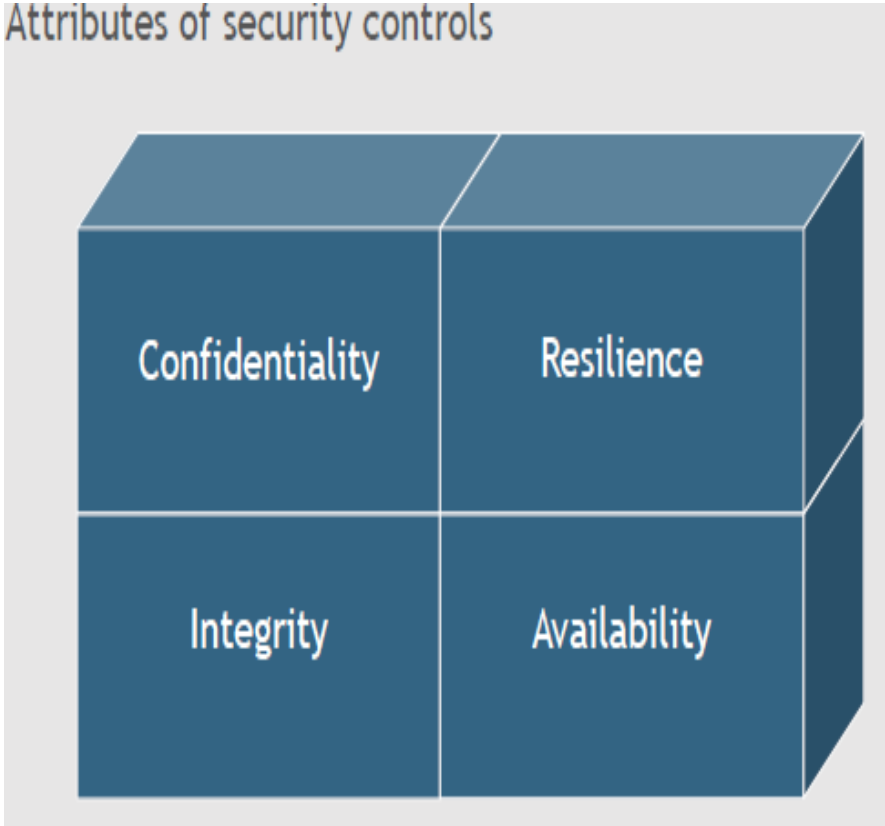
Monitorizeaza respectarea RGDP-ului

Răspunde la solicitarile primite

Exercita secretul profesional

Cooperează cu ANSPDCP

Securitatea datelor



- **Confidentialitate** – Sistem care sa permita accesul pe principiul ”need to know basis”
- **Integritatea** - sunt stabilite controale care sa stabileasca acuratetea si integritatea datelor.
- **Disponibilitatea** – datele sunt disponibile oricand, pentru activitatiile de business.
- **Rezilienta** – datele pot sa fie in siguranta si sa fie recuperate dupa o amenintare.

Securitatea datelor

Cum se realizeaza securizarea datelor?

- Mijloace administrative
- Solutii tehnice

Masuri de securitate privind prelucrarea datelor personale

Prin ANONIMIZARE

Preambulul 26

- Nu se refera la o persoana identificata sau identificabila
- Data transformata in neidentificabila
- Odata anonimizata, conform GDPR-ului nu se considera data cu caracter personal

Prin PSEUDOMIZARE

Preambulul 26, 28, 29

Art. 4.5, 6.4.e, 25.1, 32.1.a

- Nu este anonima in totalitate – cu intermediul unei chei poti ajunge inapoi la identificarea persoanei
- Un proces care separa datele atribuite unei anume personae, pentru a face proteja identitatea acestuia
- Reprezinta o masura de securizare a datelor
- Este o prelucrare ce intra sub incidenta GDPR-ului

Impactul **GDPR asupra organizațiilor**

Legalitate si conformitate

RGDP introduce noi cerințe și provocări pentru legalitate și funcționalitate. Se estimează că este necesară formarea a peste 2.800.000 de DPO numai în Europa. Nivelul amenzilor este cel mai ridicat în istoria UE. Se pune un accent deosebit pe responsabilitatea organizațională care necesită un management proactiv și robust al confidențialității datelor. Obligă organizațiile să analizeze serios modul în care elaborează politici de protecție a datelor private

Tehnologie

GDPR presupune modificări ale modului în care sunt proiectate și gestionate tehnologiile de prelucrare a datelor. Se solicită evaluări de riscuri privind confidențialitatea pentru a proiecta și implementa sisteme și tehnologii. Este avută în vedere mai accentuat mascarea datelor, pseudo-anonimizarea și criptarea.

Impactul **GDPR asupra organizațiilor**

Sancțiuni

Sancțiuni și amenzi cu sume nemaiîntânite până acum. Respectarea GDPR se va extinde și la țări din afara UE, cel puțin pentru organizațiile non-UE care prelucrează date ale cetățenilor europeni.

Funcții noi

Organizațiile care prelucrează pe scară largă date personale sau au peste 250 angajați trebuie să aibă desemnat un DPO cu experiența, cunoștințe și abilități adecvate. DPO trebuie să aibă o poziție specifică în organizație pentru a impune măsurile de securitate.

Responsabilitate

Cerința actuală de a furniza anual autorităților informații despre activitatea de prelucrare a datelor este înlocuită cu cerințe noi referitoare la audit și evaluare și trasabilitatea datelor. Accentul se pune pe o atitudine proactivă a organizațiilor și capabilă de a demonstra conformitatea cu cerințele GDPR. O responsabilitate mărită a organizațiilor în ceea ce privește protejarea datelor private, managementul riscurilor și acțiuni de răspuns la incidente de securitate.

Impactul **GDPR asupra organizațiilor**

Măsuri criptografice

GDPR recunoaște în mod oficial beneficiile criptării datelor. Organizațiile trebuie să identifice măsuri și controale criptografice adecvate, fiind răspunzătoare în cazul producerii de incidente datorate utilizării unor mecanisme slabe sau vulnerabile de criptare.

Privacy-by-Design

Organizațiile trebuie să stabilească un set de reguli bine concepute în sensul protecției datelor private încă din faza de proiectare a sistemelor de prelucrare a datelor sau în situația dezvoltării și implementării de noi soluții și tehnologii. Unul din mecanismele utilizate în acest sens trebuie să fie DPIA (Data Protection Impact Assessment) care este acum cerut în cazul prelucrării datelor cu risc ridicat.

Inventarul informațiilor

Organizațiile trebuie să demonstreze că știu ce date dețin, unde sunt stocate, cum și cu cine sunt procesate și transmise prin crearea și întreținerea unui “inventar” al activităților de prelucrare a datelor. Trebuie implementat un sistem de gestionare a înregistrărilor referitoare la date personale și activități de procesare.

Impactul **GDPR asupra organizațiilor**

Dreptul la portabilitate

Presupune furnizarea datelor cu caracter personal într-un format lizibil și standardizat pentru a fi accesibile persoanelor vizate. Poate fi o provocare majoră pentru unele organizații.

Date pseudo-anonimizarea

GDPR recunoaște și extinde conceptul de date pseudo-anonime punând un accent mai mare pe clasificarea datelor.

Privacy by Design / Default

Privacy by Design

Activitățile de procesare trebuie planificate și proiectate ținând cont de cerințele de securitate a datelor cu caracter personal

Privacy by Default

Implicit, doar datele necesare pentru fiecare scop specific vor fi culese și procesate.
Implicit, datele personale nu vor fi accesibile terților în mod automat și/sau fără intervenție umană.

Privacy by Design / Default

- Nu vor fi colectate mai multe informații decât strict cele necesare scopului prelucrării.
- Nu vor fi stocate mai multe informații sau pe termen mai lung decât cel strict necesare scopului prelucrării
- Nu vor fi procesate mai multe informații decât strict cele necesare scopului prelucrării
- Nu vor fi vândute date personale
- Nu vor fi stocate/transmise date personale decât în formă criptată

Etapele implementarii

1. Stabilirea si inventarierea categoriilor de date personale
2. Stabilirea și inventarierea proceselor de prelucrare (stocare, procesare, transmitere) a datelor personale
3. Stabilirea si inventarierea echipamentelor și platformelor, aplicațiilor implicate (asset inventory)
4. Identificarea și evaluarea vulnerabilităților și amenințărilor asociate (vulnerabilities scan, pen test)

   Identificarea, analiza, evaluarea riscurilor și impactului
5. Stabilirea opțiunilor de tratare a riscurilor Implementarea măsurilor

   de tratare a riscurilor
6. Elaborarea și implementarea politicilor și procedurilor
7. Instruirea, conștientizarea personalului și colaboratorilor Elaborarea și testarea
8. planurilor de continuitate, de recuperare și
   revenire după incidente majore
9. Monitorizarea, analiza și auditarea performanțelor