smart alliance

Smart Business Technology Series

Episode 3

Regulamentul General privind Protecția Datelor (GDPR)

24 Mai – Hotel Epoque

Prezentarea cerințelor tehnice și a unor soluții practice pentru obținerea conformității cu noul GDPR

Cosmin Măcăneață
Managing Partner, OMEGA Trust

Regulamentul General privind Protecția Datelor (GDPR)

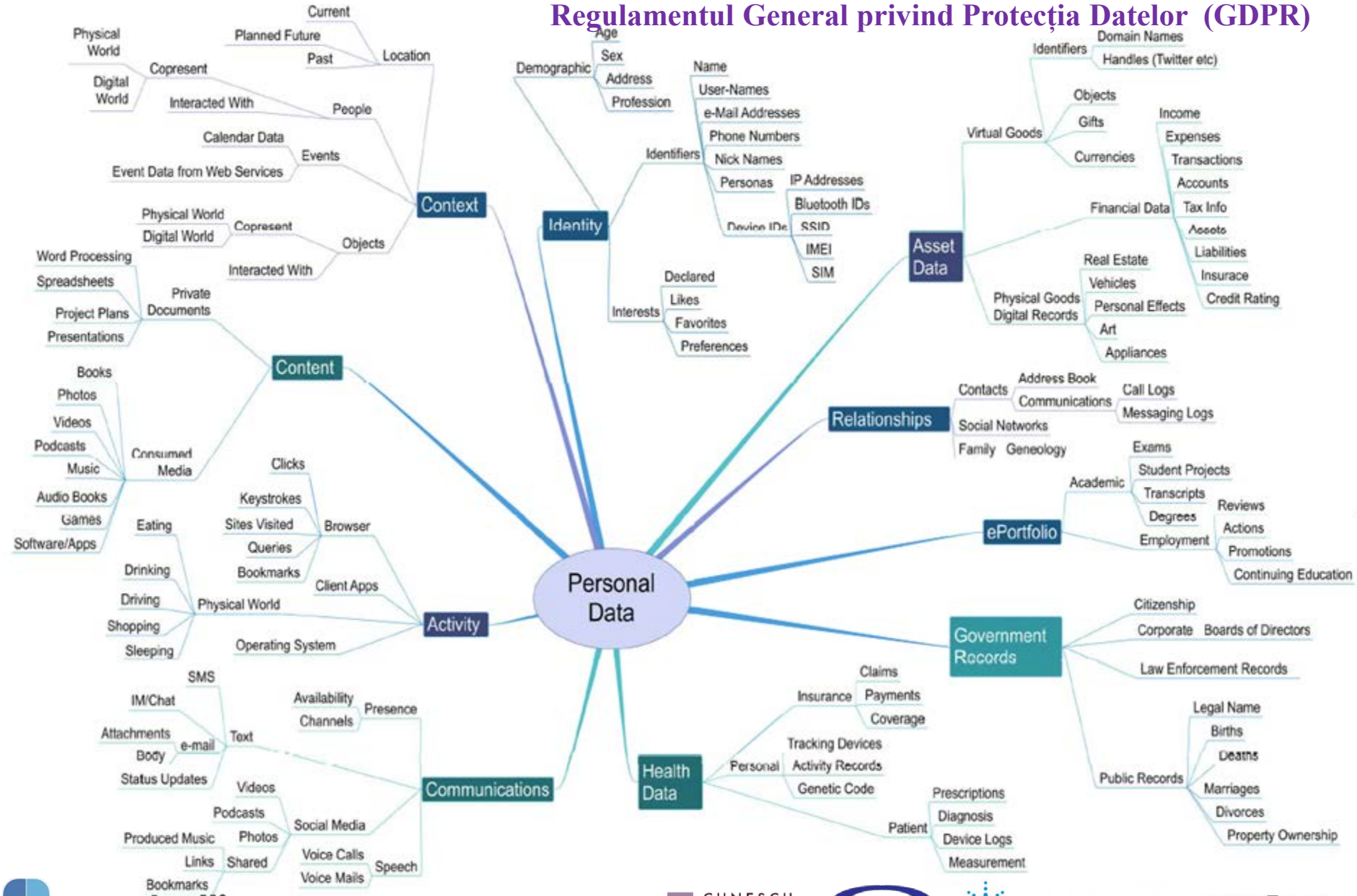
http://www.nasul.tv/spionii-din-casa-ta-gigantii-it-colecteaza- | Iată cum ne spionează televizo... | Spionii din casa ta | Giganții...

Televizoarele inteligente pot inregistra toate conversatiile care au loc in jurul lor, insa nu sunt singurele obiecte din casa care se pot transforma in spioni.

In aceasta saptamana, presa a relatat ca producatorul sud-coreean Samsung si-a avertizat clientii asupra unui aspect foarte important, arata Daily Mail.

Televizoarele sale sunt dotate cu o functie de recunoastere vocala. In principal, ar trebui sa

Regulamentul General privind Protecția Datelor (GDPR)



Introducere

- Regulamentul European privind Protecția Datelor este **prima reglementare completă cu privire la protecția datelor** emisă în ultimii 20 de ani.

- **Înlocuiește fosta Directivă 95/46/EC**

- GDPR este direct aplicabil în toate statele UE **și va înlocui orice legislație națională aferentă Directivei 95/46/EC**

Cui se aplică?

Regulamentul se aplică prelucrării datelor în cadrul activităților aferente unui sediu al unui operator de pe teritoriul UE, indiferent dacă prelucrarea are loc sau nu pe teritoriul Uniunii Europene.

Regulamentul se aplică entităților care sunt situate în afara teritoriului UE, dacă aceștia prelucrează date ale persoanlor care se afla pe teritoriul UE, in cazul in care:

- le ofera bunuri/servicii
- monitorizeaza comportamentul lor daca acesta se manifesta in Uniune

Definiții

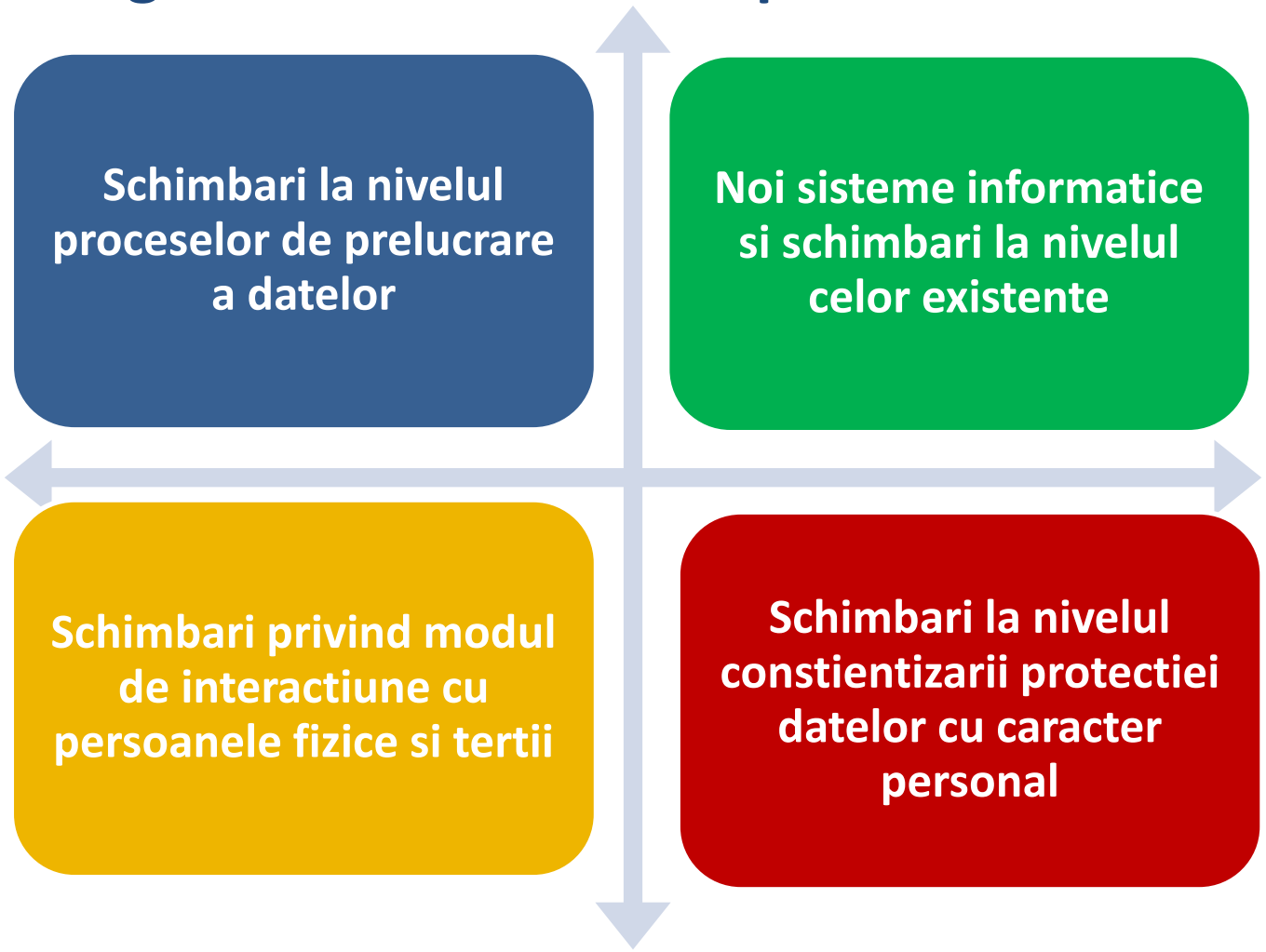
Date cu caracter personal - orice informații privind o persoană fizică care poate fi identificată, direct sau indirect, în special prin referire la un element de identificare (nume, un număr de identificare, un identificator online, etc.) sau elemente specifice, proprii identității fizice, fiziologice, genetice, etc.

Operator - persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal.

Prelucrarea datelor cu caracter personal - înseamnă orice operațiune sau set de operațiuni efectuate asupra datelor 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.

Încălcarea securității datelor cu caracter personal - înseamnă o încălcare a securității care duce, în mod accidental sau ilegal, la distrugerea, pierderea, modificarea, sau divulgarea neautorizată a datelor cu caracter personal transmise, stocate sau prelucrate într-un alt mod, sau la accesul neautorizat la acestea.

Schimbari in organizatii ca urmare a adoptarii GDPR



Aspecte organizatorice și tehnice

Articolul 5 "Principii legate de prelucrarea datelor cu caracter personal"

"Datele cu caracter personal sunt:

- **prelucrate în mod legal, echitabil și transparent față de persoana vizată….**
- **colectate în scopuri determinate, explicite și legitime și nu sunt prelucrate ulterior într-un mod incompatibil cu aceste scopuri…**
- **adecvate, relevante și limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate („reducerea la minimum a datelor")…**
- **exacte și, în cazul în care este necesar, să fie actualízate ….**
- **păstrate într-o formă care permite identificarea persoanelor vizate pe o perioadă care nu depășește perioada necesară îndeplinirii scopurilor….**
- **prelucrate într-un mod care asigură securitatea adecvată a datelor cu caracter personal….**

Astfel, operatorul de date cu caracter personal este obligat:

- Realizeze o analiza completa cu privire la datele prelucrate, scopul prelucrarii datelor, a legitimitatii acestor prelucrari, precum si a aspectelor tehnice ce tin de colectarea, actualizarea, prelucrarea, stocarea, transmiterea si distrugerea datelor;
- Documenteze aceste procese intr-o Politica de prelucrare a datelor.

Responsabilitatea Operatorului

Articolul 24 „Responsabilitatea Operatorului”:

„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”

Implementarea articolului presupune:

- Definirea responsabilităților ce țin de asigurarea protecției datelor cu caracter personal;
- Definirea și implementarea proceselor și procedurilor operationale relevante;
- Implementarea unei metodologii de analiza de risc;
- Definirea și implementarea unor controale tehnice pentru asigurarea protejării datelor cu caracter personal funcție de nivelul de risc la care sunt expuse.

Măsuri Organizatorice

Articolul 37 „Desemnarea responsabilului cu protecția datelor”:

„Operatorul și persoana împuternicită de operator desemnează un responsabil cu protecția datelor”

Implementarea articolului presupune:

- Instituirea unui rol de Responsabil de protejarea datelor cu caracter personal;
- În cazul în care există rolul de Ofițer de Securitate a Informației el poate prelua și responsabilitățile ce țin de protecția datelor cu caracter personal;
- Trebuie sa aiba competente in domeniu;
- Poate fi angajat intern sau externalizat.

Măsuri Organizatorice

Articolul 38 „Sarcinile responsabilului cu protecția datelor”:

- Raportează direct la cel mai înalt nivel de management;
- Nu poate fi demis pentru sarcinile de lucru ce țin de protecția datelor;
- Nu primeste instructiuni cu privire la indeplinirea sarcinilor;
- Informarea și consilierea operatorului precum și a angajaților cu privire la obligațiile care le revin în referitoare la protecția datelor;
- Monitorizarea respectării regulamentului GDPR și a politicilor operatorului în ceea ce privește protecția datelor cu caracter personal, inclusiv acțiunile de sensibilizare și de formare a personalului;
- Furnizarea de consiliere în ceea ce privește evaluarea impactului asupra protecției datelor și monitorizarea funcționării acesteia;
- Cooperarea cu autoritatea de supraveghere;
- Asumarea rolului de punct de contact pentru Autoritatea de supraveghere privind aspectele legate de prelucrare.

Aspecte organizatorice și tehnice

Articolul 25 „Asigurarea protecției datelor începând cu momentul conceperii și în mod implicit" introduce conceptul „security by design" la prelucrarea datelor cu caracter personal:

"...operatorul, atât în momentul stabilirii mijloacelor de prelucrare, cât și în cel al prelucrării în sine, pune în aplicare măsuri tehnice și organizatorice adecvate care sunt destinate să pună în aplicare în mod eficient principiile de protecție a datelor cu caracter personal..."

Astfel, operatorul de date cu caracter personal este obligat:

- Să prevadă măsurile de protecție a datelor cu caracter personal începând cu etapa de concepere a sistemelor de prelucrare a datelor respective;
- Să se asigure că măsurile respective sunt implementate și menținute pe parcursul procesului de prelucrare;
- Să evalueze continuu măsurile implementate din punct de vedere al eficacității lor.

Măsuri Organizatorice

Articolul 35 „Evaluarea impactului asupra protecției datelor”:

„Având în vedere natura, domeniul de aplicare, contextul și scopurile prelucrării, în cazul în care un tip de prelucrare, în special cel bazat pe utilizarea noilor tehnologii, este susceptibil să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice, operatorul efectuează, înaintea prelucrării, o evaluare a impactului operațiunilor de prelucrare prevăzute asupra protecției datelor cu caracter personal. O evaluare unică poate aborda un set de operațiuni de prelucrare similare care prezintă riscuri ridicate similare. ”

Implementarea articolului presupune:

- Definirea și implementarea unei metodologii de analiză de risc care să cuprindă și analiza de impact;
- Definirea explicită a responsabilităților ce țin de efectuarea analizei de risc și impact cu documentarea rezultatelor și deciziilor luate.

Măsuri tehnice

Articolul 32 „Securitatea Prelucrării”:

„...operatorul 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 continuă 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 periodica a eficacității măsurilor tehnice și organizatorice pentru a garanta securitatea prelucrării”

Măsuri tehnice

Articolul 32 „Securitatea Prelucrării” presupune:

- Implementarea unor mecanisme și procese care ar permite criptarea datelor precum și gestionarea cheilor de criptare;
- Implementarea unor mecanisme ce ar permite ca datele de identificare ale unei persoane să fie înlocuite cu un pseudonim;
- Implementarea unor controale la nivel de sisteme informatice ce ar asigura integritatea lor, disponibilitatea lor și confidențialitate datelor care sunt prelucrate cum ar fi: acces control, monitorizare log-uri, mecanisme de backup, configurări de securitate, sisteme de tip IPS/IDS etc.
- Implementarea unor planuri de Continuitate a Afacerii și proceduri de recuperare după incidente și dezastre;
- Testări de penetrare și evaluări periodice a securității sistemelor informatice care procesează date cu caracter personal;
- Audit intern regulat;

Măsuri tehnice

Articolul 33 „Notificarea autorității de supraveghere în cazul încălcării securității datelor cu caracter personal”:

„În cazul în care are loc o încălcare a securității datelor cu caracter personal, operatorul notifică acest lucru autorității de supraveghere competente în temeiul articolului 55, fără întârzieri nejustificate și, dacă este posibil, în termen de cel mult 72 de ore de la data la care a luat cunoștință de aceasta, cu excepția cazului în care este susceptibilă să genereze un risc pentru drepturile și libertățile persoanelor fizice…”

Art 34 “Informarea persoanei vizate cu privire la încălcarea securităţii datelor cu caracter personal”

În cazul în care încălcarea securităţii datelor cu caracter personal este susceptibilă să genereze un risc ridicat pentru drepturile şi libertăţile persoanelor fizice, operatorul informează persoana vizată fără întârzieri nejustificate cu privire la această încălcare.

Măsuri tehnice

Implementarea articolelor 33 si 34 presupune:

- Definirea și implementarea unui proces de identificare a încălcării securității datelor cu caracter personal (e.g. sisteme de management al logurilor, sisteme de tip DLP, IDS etc.);
- Definirea unui proces de documentare a cazurilor de încălcare și păstrarea înregistrărilor;
- Definirea și implementarea unui proces de notificare.


HOTEL
facebook®
You can check out any time you like, but you can never leave.
IN
©2010 Stephanie McMillan.org

Măsuri tehnice

Articolul 17 „Dreptul la ștergere”:

„Persoana vizată are dreptul de a obține din partea operatorului ștergerea datelor cu caracter personal care o privesc, fără întârzieri nejustificate, iar operatorul are obligația de a șterge datele cu caracter personal fără întârzieri nejustificate”

Implementarea articolului presupune:

- Definirea și implementarea unui proces ce ar permite identificarea datelor cu caracter personal procesate si a locatiilor unde sunt tinute;
- Implementarea unor mecanisme ce ar permite identificarea în timp util a datelor necesare pentru a fi șterse;
- Capacitatea de a șterge datele.

Măsuri tehnice

Articolul 18 „Dreptul la restricționarea prelucrării”:

„Persoana vizată are dreptul de a obține din partea operatorului restricționarea prelucrării”

Implementarea articolului presupune:

- Definirea și implementarea unui proces ce ar permite evidențierea datelor cu caracter personal procesate;
- Implementarea unor mecanisme ce ar permite identificarea în timp util a datelor necesare;
- Implementarea unor mecanisme de marcare ca ne-procesabil a unui numit set de date cu caracter personal;
- Implementarea unui mecanism de notificare a părților terțe implicate în procesarea datelor cu caracter personal privind restricțiile impuse.

Măsuri tehnice

Articolul 19 „Obligația de notificare privind rectificarea sau ștergere a datelor cu caracter personal sau restricționarea prelucrării”:

„Operatorul comunică fiecărui destinatar căruia i-au fost divulgate datele cu caracter personal orice rectificare sau ștergere a datelor cu caracter personal sau restricționare a prelucrării efectuate în conformitate cu articolul 16, articolul 17 alineatul (1) și articolul 18, cu excepția cazului în care acest lucru se dovedește imposibil sau presupune eforturi disproporționate. Operatorul informează persoana vizată cu privire la destinatarii respectivi dacă persoana vizată solicită acest lucru.”

Implementarea articolului presupune:

- Implementarea unui mecanism de jurnalizare a acțiunilor efectuate asupra datelor cu caracter personal, inclusive din punct de vedere al transmiterii acestora catre diverse entitati terte;
- Definirea și implementarea unui proces de comunicare cu tertii cu privire la rectificarea sau stergerea datelor.

Măsuri tehnice

Articolul 20 „Dreptul la portabilitatea datelor”:

„….În exercitarea dreptului său la portabilitatea datelor în temeiul alineatului (1), persoana vizată are dreptul ca datele cu caracter personal să fie transmise direct de la un operator la altul acolo unde acest lucru este fezabil din punct de vedere tehnic…

Implementarea articolului presupune:

- Implementarea unui mecanism de asigurare a transferului de date intr-un mod securizat;
- Implementarea unui mecanism de stergere a datelor din evidentele proprii ale operatorului.

Măsuri tehnice

Articolul 30 „Evidențele activităților de prelucrare”:

„Fiecare operator și, după caz, reprezentantul acestuia păstrează o evidență a activităților de prelucrare desfășurate sub responsabilitatea lor. ”

Implementarea articolului presupune:

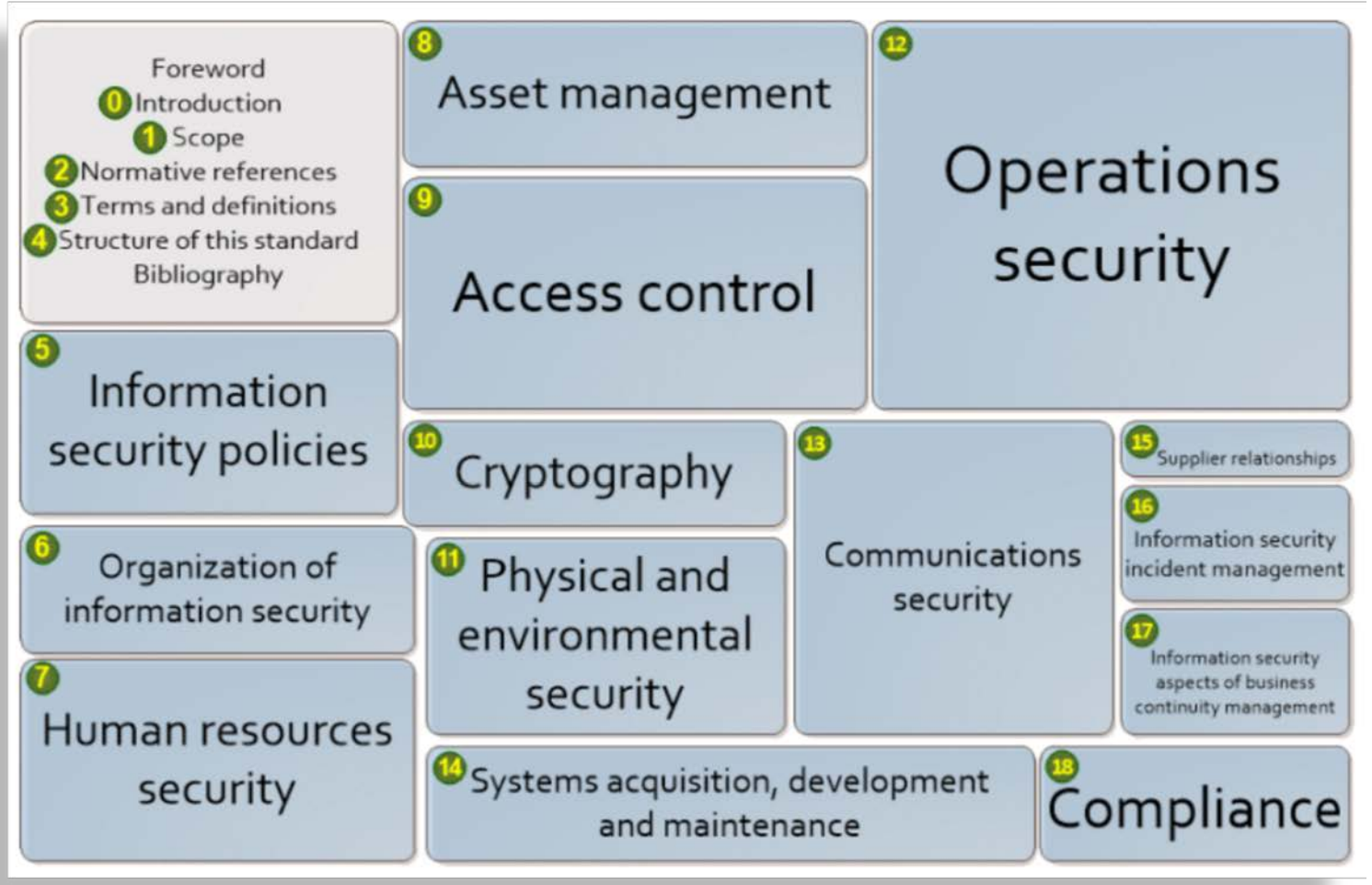
- Documentarea schemei de procesare a datelor;
- Implementarea unui mecanism de jurnalizare a acțiunilor efectuate asupra datelor cu caracter personal;
- Definirea și implementarea unei politici de păstrare a informației jurnalizate.

Implementarea unui sistem de management pentru GDPR

Implementarea cu succes a cerințelor GDPR poate fi realizat printr-o abordare complexă și sistemică asemănătoare implementării unui Sistem de Management al Securității Informației (SMSI):

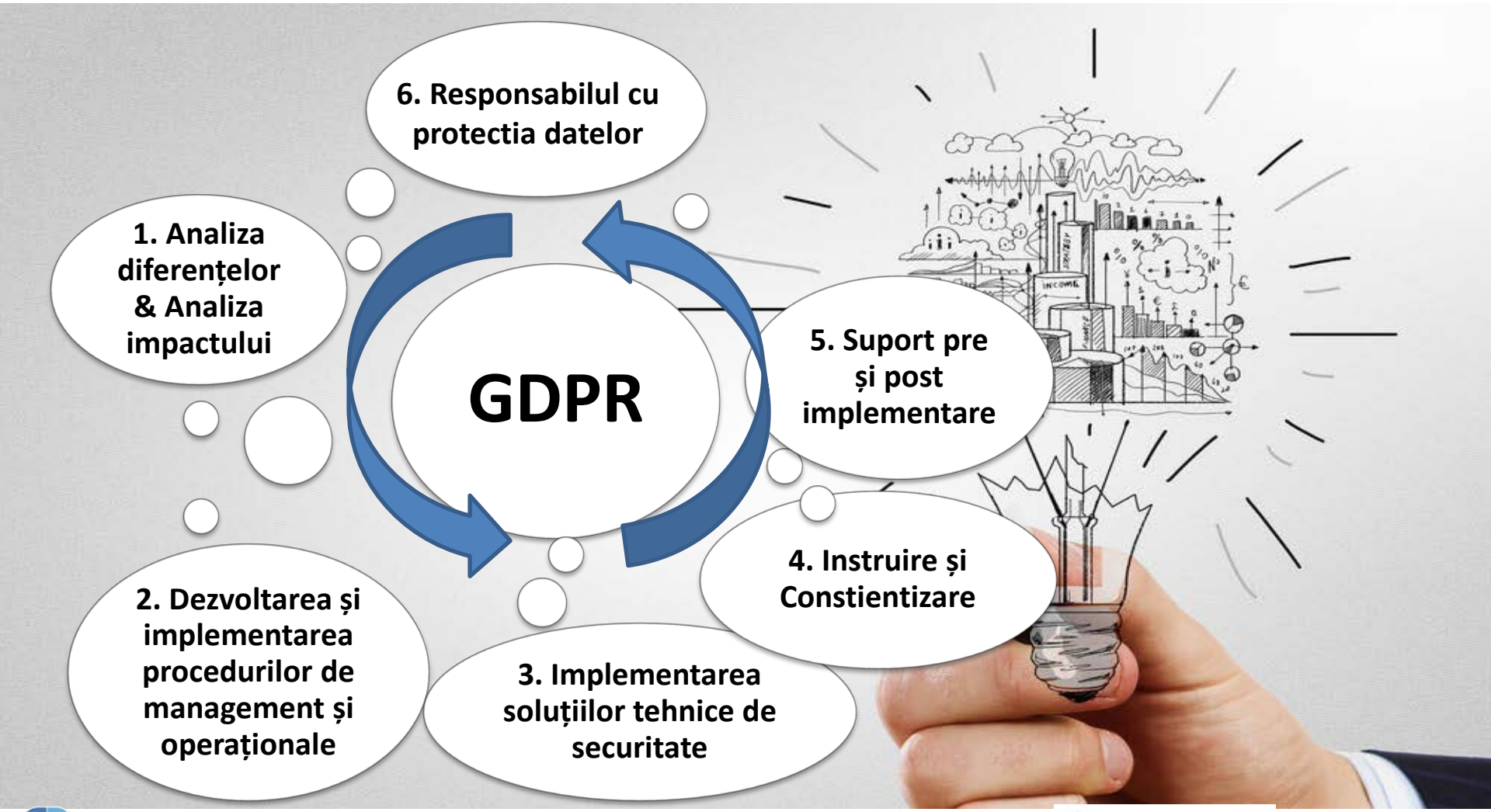
- Definirea rolurilor și a responsabilităților privind prelucrarea datelor cu caracter personal;
- Identificarea și punerea în evidență a datelor cu caracter personal care sunt procesate de operator;
- Identificarea sistemelor care procesează și stochează datele respective;
- Efectuarea unei analize de risc privind securitatea datelor cu caracter personal;
- Implementarea controalelor necesare pentru asigurarea protejării datelor respective;
- Evaluarea eficacității controalelor implementate și îmbunătățirea continua a acestora.

SMSI conform ISO 27001:2013



Pașii de implementare

Cum va putem asista?



Regulamentul General privind Protecția Datelor (GDPR)

smart alliance

“Smart Choices for a Smart Future”