Regulamentul (UE) General privind Protecţia Datelor – RGPD 2016/679
ISO 27001 – Securitatea Informatiilor

InITinvest Consulting

Program de Constientizare a cerintelor minimale ale RGPD 2016/679

2018

Trainer:

CORINA HOMEUCĂ

CHIEF EXECUTIVE OFFICER

- **Certificare IT Governance internationala in aplicarea Regulamentului 679/2016 EU GDPR**

- 17 ani de experienta, din care:
- 7 ani de **Project Management, Audit & Consultanta IT**
- 10 ani de **dezvoltare de business si inovare** continua
- zeci de proiecte reusite,
- Train of Trainers & Membru in Asociatia Americana de Dezvoltare a Talentelor
- Manager al Sistemelor de Management a Calitatii

Sumar

- Ce este EU GPDR si ce noutati aduce?
- Unde si cui se aplica?
- Cele 6+1 Principii ale GDPR
- Consimtamantul
- Date personale cu caracter special
- Drepturile persoanelor vizate
- Pivacy by Design & Privacy by Default
- Pastrarea evidenţei activitatilor de prelucrare
- Pseudonimizarea
- Bresele de securitate a datelor si timpii de notificare
- Transferul datelor
- Securitatea Informatiilor – ISO 27001
- Zonele de risc
- Ce am de facut pentru a asigura Securitatea, Integritatea si Disponibilitatea Informatiilor si, implicit a Datelor Personale?

Ce este Regulamentul (UE) General privind Protecţia Datelor – RGPD 2016/679 ?

Legislatia aplicabila unitar pe intreg teritoriul UE incepand cu 28 Mai 2018

- **transparenţa faţă de persoana vizată** și responsabilizarea operatorului de date faţă de modul în care prelucrează datele cu caracter personal.
- stabilește o serie de garanţii specifice pentru a proteja cât mai efficient **viaţa privată a minorilor, în special în mediul on-line**.
- introduce noi drepturi: **dreptul de a fi uitat, dreptul la portabilitatea datelor și dreptul la restricţionarea prelucrării**.
- introduce s**ancţiuni severe**, pâna la **10 – 20 milioane de euro sau între 2%**
- **și 4% din cifra de afaceri la nivel internaţional**, pentru operatorii din sectorul privat, precum si alte amenzi stabilite de autoritatile de supraveghere locale pentru autoritatile publice;
- **Dreptul persoanelor vizate de a fi despagubite pentru orice prejudiciu, atat material cat si nematerial** de operatorul de date, dar si de procesator – actiunile in masa sunt incurajate.

Ce sunt datele personale?

Date personale:

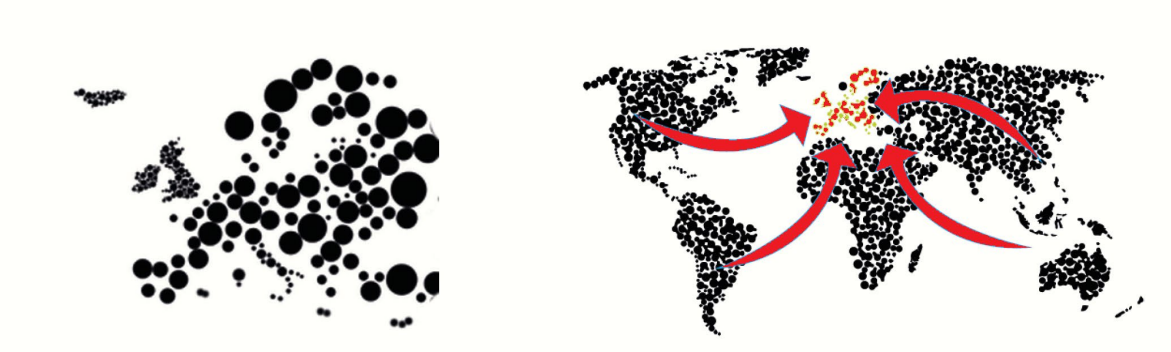
”orice informatii privind o persoana fizica identificata sau identificabila ("persoana vizata");

o persoana fizica identificabila este o persoana care poate fi identificata, direct sau indirect, în special prin referire la un element de identificare, cum ar fi un ***nume, un numar de identificare, date de localizare, un identificator online, sau la unul sau mai multe elemente specifice, proprii identitatii sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale.”***

Date personale sensibile (o categorie speciala de date personale) care indica: originea rasială sau etnică, opiniile politice, filozofice sau religioase, apartenenţa sindicală; date privind sănătatea sau orientarea sexuală, date genetice sau biometrice; date referitoare la infracţiuni sau condamnări penale; date referitoare la minori etc.

Unde si cui se aplica?

Date cu caracter personal - **orice** informaţii privind o persoană fizică identificată sau identificabilă ("persoana vizată");
Prelucrare (procesare) - **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.
Operator (Collector); **Persoana imputernicita de operator** (Processor)



pe teritoriul UE, activităţilor derulate la sediul unui operator sau al unei persoane împuternicite de operator pe teritoriul Uniunii, indiferent dacă prelucrarea are loc sau nu pe teritoriul Uniunii.

când activităţile de prelucrare sunt legate de: oferirea de bunuri sau servicii unor astfel de **persoane vizate în UE**, indiferent dacă se solicita sau nu efectuarea unei plăţi de către persoana vizată; sau monitorizarea comportamentului lor dacă acesta se manifestă în cadrul Uniunii.

Roluri GDPR

- **Persoana vizata – orice persoana fizica de pe teritoriul UE**
- **Operator** (Controller)- persoana fizică sau juridică, autoritatea publică, agenţia sau alt organism care, singur sau împreună cu altele, stabileşte scopurile şi mijloacele de prelucrare a datelor cu caracter personal; atunci când scopurile şi mijloacele prelucrării sunt stabilite prin dreptul Uniunii sau dreptul intern, operatorul sau criteriile specifice pentru desemnarea acestuia pot fi prevăzute în dreptul Uniunii sau în dreptul intern;
- **Persoana imputernicita de operator** (Processor) - persoana fizică sau juridică, autoritatea publică, agenţia sau alt organism care prelucrează datele cu caracter personal în numele operatorului;

Roluri GDPR

- **Tert -** o persoană fizică sau juridică, autoritate publică, agenţie sau organism **altul** decât *persoana vizată, operatorul, persoana împuternicită de operator şi persoanele care, sub directa autoritate a operatorului sau a imputernicitului prelucreaza date* personale.

- **Destinatar** - persoana fizică sau juridică, autoritatea publică, agenţia sau alt organism căreia (căruia) îi sunt divulgate datele cu caracter personal, indiferent dacă este sau nu o parte terţă. Cu toate acestea, autorităţile publice cărora li se pot comunica date cu caracter personal în cadrul unei anumite anchete în conformitate cu dreptul Uniunii sau cu dreptul intern nu sunt considerate destinatari; prelucrarea acestor date de către autorităţile publice respective respectă normele aplicabile în materie de protecţie a datelor, în conformitate cu scopurile prelucrării;

Responsabil cu Protecţia Datelor

Cine este obligat sa angajeze/contracteze DPO?

1. Organizatia care:

- **este o autoritate publică sau un organism public**,
- desfășoară o activitate principală care conduce la **realizarea unei monitorizări constante și sistematice pe scară largă a persoanelor**;
- desfășoară o activitate principală care constă în prelucrarea pe scară largă de **date sensibile** (date privind originea rasială sau etnică, convingerile religioase, apartenenţa sindicală, date genetice, biometrice, privind starea de sănătate) sau **referitoare la condamnări penale și infracţiuni**.

Responsabilitati ale DPO

- **să informeze și să consilieze** operatorul sau persoana împuternicită de operator, precum și angajaţii acestora cu privire la **obligaţiile** existente în domeniul protecţiei datelor cu caracter personal sau Studii de IMPACT si **sa verifice** efectuarea acestora;
- **să monitorizeze respectarea RGPD** și a legislaţiei naţionale în domeniul protecţiei datelor;
- **să coopereze cu autoritatea pentru protecţia datelor** și să reprezinte punctul de contact în relaţia cu aceasta.

Cele 6+1 Principii ale GDPR

1. **Legalitate, echitate şi transparenţă**
2. **Limitări legate de scop;**
3. **Reducerea la minimum a datelor** - adecvate, relevante şi limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate;
4. **Exactitatea** datelor;
5. **Limitări** legate de stocare
6. Integritate si confidentialitate – **securitatea datelor**

Principiul **Responsabilitatii**

Art.5 (2) - ***Operatorul este responsabil de respectarea acestor principii*** *şi poate* ***demonstra*** *această respectare (" **responsabilitate**").*

Considerentul 74 subliniaza ***responsabilitatea şi răspunderea operatorului pentru orice prelucrare a datelor cu caracter personal efectuată de către acesta sau în numele său.***

Consimtamantul

- Operatorul TREBUIE sa **demonstreze** că persoana vizată şi-a dat consimţământul pentru prelucrarea datelor sale cu caracter personal
- cererea privind consimţământul trebuie să fie
  - prezentată într-o formă care o **diferenţiază** în mod clar de celelalte aspecte,
  - într-o formă **inteligibilă şi uşor accesibilă,** utilizând un limbaj clar şi simplu.
- Persoana vizată are dreptul să îşi retragă în orice moment consimţământul.
- **Nu este legat de oferirea de servicii**
- prelucrarea datelor cu caracter personal ale unui **copil** este legală dacă copilul are cel puţin vârsta de 16 ani. Dacă copilul are sub vârsta de 16 ani, consimtamantul trebuie sa fie autorizat de titularul răspunderii părinteşti,
- **Persoana vizata trebuie sa fie informata:**
  - **Cine?**
  - **Ce si in ce scop?**
  - **Cum?**
  - **De ce?**
  - **Unde?**
  - **Pana cand?**

Masuri speciale

Date sensibile

sau

Prelucrarea efectuată are ca scop și ca efect:

- **monitorizarea permanentă pe scară largă** a unei zone accesibile publicului;
- evaluarea sistematică și aprofundată a unor aspecte personale, inclusiv **profilarea**, pe baza căreia sunt luate decizii care produc efecte juridice referitoare la o persoană fizică sau care o afectează pe aceasta în mod semnificativ.

Prelucrarea efectuată implică transferuri de date în afara Uniunii Europene, către state care nu asigură un nivel de protecţie adecvat recunoscut de Comisia Europeană.

Drepturile persoanelor vizate

GDPR pune accent pe transparenţa informaţiilor, a comunicărilor şi a modalităţilor de exercitare a drepturilor persoanei vizate

- **Dreptul la Informare şi acces la datele sale cu caracter personal**
- **Dreptul de acces al persoanei vizate**
- **Dreptul la rectificare şi ştergere**
- **Dreptul la ştergerea datelor ("dreptul de a fi uitat")**
- **Dreptul la restricţionarea prelucrării**
- **Dreptul la portabilitatea datelor**
- **Dreptul la opoziţie şi procesul decizional individual automatizat**

Drepturile persoanelor vizate - restrictii

a)securitatea naţională;
b)apărarea;
c)securitatea publică;
d)prevenirea, investigarea, depistarea sau urmărirea penală a infracţiunilor sau executarea sancţiunilor penale, inclusiv protejarea împotriva ameninţărilor la adresa securităţii publice şiprevenirea acestora;
e)alte obiective importante de interes public general ale Uniunii sau ale unui stat membru, în special un interes economic sau financiar important al Uniunii sau al unui stat membru, inclusiv în domeniile monetar, bugetar şi fiscal şi în domeniul sănătăţii publice şi al securităţii sociale;
f)protejarea independenţei judiciare şi a procedurilor judiciare;
g)prevenirea, investigarea, depistarea şi urmărirea penală a încălcării eticii în cazul profesiilor reglementate;
h)funcţia de monitorizare, inspectare sau reglementare legată, chiar şi ocazional, de exercitarea autorităţii oficiale în cazurile menţionate la literele (a)-(e) şi (g);
i)protecţia persoanei vizate sau a drepturilor şi libertăţilor altora;
(j) punerea în aplicare a pretenţiilor de drept civil

Pastrarea evidenţei activitatilor de prelucrare – art. 30

Evidenţa păstrată de operator va cuprinde:
(a) numele și datele de contact ale operatorului și, după caz, ale operatorului asociat, ale reprezentantului operatorului și ale responsabilului cu protecţia datelor;
(b) scopurile prelucrării;
(c) o descriere a categoriilor de persoane vizate și a categoriilor de date cu caracter personal;
d) categoriile de destinatari
(e) dacă este cazul, transferurile de date cu caracter personal către o ţară terţă sau o organizaţie internaţională, inclusiv identificarea ţării terţe sau a organizaţiei internaţionale respective;
(f) termenele-limită preconizate pentru ștergerea diferitelor categorii de date;
(g) o descriere generală a măsurilor tehnice și organizatorice de securitate

Transferul datelor

Se poate realiza doar intre operatori intre care exista:

- conformitate RGPD;
- baza legala sau contractuala-sunt operatori asociati.

Esenţa acordului dintre operatorii asociati este făcută cunoscută persoanei vizate.

- Persoana vizata isi exprima punctul de vedere fata de fiecare operator separat.

In cazul în care datele cu caracter personal nu au fost obţinute de la persoana vizată, operatorul furnizează persoanei vizate informaţii cu privire la:
a)identitatea şi datele de contact ale operatorului şi, după caz, ale reprezentantului acestuia;
b)datele de contact ale responsabilului cu protecţia datelor, după caz;
c)scopurile în care sunt prelucrate datele cu caracter personal, precum şi temeiul juridic al prelucrării; **d)**categoriile de date cu caracter personal vizate;
e)destinatarii sau categoriile de destinatari ai datelor cu caracter personal, după caz; **f)**dacă este cazul**, intenţia operatorului de a transfera date cu caracter personal către un alt destinatar.**

Bresele de securitate a datelor si timpii de notificare

Obligatiile cu privire la timpii de notificare in cazul scurgerilor de date cu caracter personal, in functie de destinatar:

- **ANSDCP – 72 ore, se transmite formularul de notificare, cuprinzand informatiile:**

a) caracterul încălcării securităţii datelor cu caracter personal, inclusiv, acolo unde este posibil, categoriile şi numărul aproximativ al persoanelor vizate în cauză, precum şi categoriile şi numărul aproximativ al înregistrărilor de date cu caracter personal în cauză;
b)comunică numele şi datele de contact ale responsabilului cu protecţia datelor sau un alt punct de contact de unde se pot obţine mai multe informaţii;
c)descrie consecinţele probabile ale încălcării securităţii datelor cu caracter personal;
d)descrie măsurile luate sau propuse spre a fi luate de operator pentru a remedia problema încălcării securităţii datelor

- **Persoanle vizate a caror date au fost divulgate – imediat, cuprinzand o** descriere într-un limbaj clar şi simplu a caracterului încălcării securităţii datelor si informatiile de la pct. b), c), d) de mai sus.

EXISTA si exceptii de la notificarea obligatorie a persoanei vizate (art. 34 (3))

Pivacy by Design & Privacy by Default

Privacy by Design - luarea în considerare a protecţiei datelor cu caracter personal încă de la momentul conceperii unui nou proiect sau process de lucru.

Privacy by Default - aplicarea de măsuri tehnice și organizatorice adecvate pentru a asigura că, în mod implicit, sunt prelucrate numai date cu caracter personal care sunt necesare pentru fiecare scop specific al prelucrării

Pseudonimizarea

Prelucrarea datelor cu caracter personal într-un asemenea mod, încât acestea **să nu mai poată fi atribuite unei anume persoane vizate** fără a se utiliza informaţii suplimentare, cu condiţia ca aceste informaţii suplimentare să fie stocate separat şi să facă obiectul unor măsuri de natură tehnică şi organizatorică care să asigure neatribuirea respectivelor date cu caracter personal unei persoane fizice identificate sau identificabile.

Amenzi

- **Pana la 10 000 000 EUR sau, în cazul unei organizatii, de până la 2 % din cifra de afaceri mondială totală anuală** (cea mai mare valoare) pentru incalcarea prevederilor privind: consimţământul copiilor, categorii speciale de date cu caracter personal, privacy by design si by default, obligatiilor operatorilor si persoanelor imputernicite de acestia, evidentele prelucrarilor, Cooperarea cu autoritatea de supraveghere**,** asigurarea sigurantei datelor, desemnarea Responsabilului cu prelucrarea datelor, certificarea ISO 27001 la nivel de organizatie etc.

- **Pana la 20 000 000 EUR sau, în cazul unei organizatii, de până la 4 % din cifra de afaceri mondială totală anuală (**cea mai mare valoare) pentru incalcarea :

a)principiilor de bază pentru prelucrare, inclusiv condiţiile privind **consimţământul**,
b)drepturile persoanelor vizate;
c)transferurile de date cu caracter personal către un destinatar dintr-o ţară terţă sau o organizaţie internaţională, în conformitate cu articolele 44-49;
d)orice obligaţii în temeiul legislaţiei naţionale adoptate în temeiul capitolului IX;
e)nerespectarea unui ordin sau a unei **limitări** temporare sau definitive asupra prelucrării, sau a **suspendării** fluxurilor de date, emisă de către autoritatea de supraveghere în temeiul articolului 58 alineatul (2), sau **neacordarea accesului,** încălcând articolul 58 alineatul (1).

Principiile GDPR - Exercitiu

O companie de consultanta IT, INIT CONSULTING, ofera servicii de consultanta clientilor UE. Ca parte a acestor servicii, clientii pot accesa portalul companiei pentru a-si monitoriza conturile si a realiza anumite actiuni.
INIT CONSULTING, a externalizat prin contract serviciile de intretinere a portalului, catre Web IT Manage, o companie specializata. Clientii sunt rugati sa isi creeze un profil online pe portal, pentru a-l putea accesa, transmitand astfel date personale.

Principiul 1: Legalitate, echitate si transparenta
Inainte de crearea profilului online pe portal, clientului i se solicita sa citeasca **notificarea** privind prelucrarea datelor personale.
Notificarea furnizeaza informatii relevante privind **colectarea si prelucrarea** datelor lui personale, **incluzand si informatii despre INIT CONSULTING, si la ce vor fi utilizate acestea. Inclusiv informatia ca Web IT Manage va colecta si procesa datele.**

Consimtamantul privind colectatea si prelucrarea datelor personale si sensibile este astfel obtinut de la client.

Principiile GDPR - Exercitiu

Principiul 2: Limitari legate de scop

Se solicita ca Notificarea privind prelucrarea datelor clientului sa fie citita **inainte** de crearea profilului online pe portal, specificand, de asemenea, **scopul pentru fiecare tip de date personale colectat. Un anume tip de date** personale este astfel utilizat pentru **anumite** scopuri.

Principiul 3: Reducerea la minimum a datelor- adecvate, limitate si relevante

In timpul procesului de creare a profilului online pe portal, INIT CONSULTING si Web IT Manage se asigura ca ei **colecteaza doar acele informatii strict necesare** pentru identificarea clientului si le furnizeaza cu informatiile de cont.

Principiul 4: Exactitatea datelor

Pentru a asigura exactitatea si actualizarea datelor personale, **fiecarui client i se cere sa revizuiasca si ca confirme exactitatea datelor, anual, la momentul log-arii pe portal.**

Orice modificare solicitata este directionata, impreuna cu justificarea necesara, catre Web IT Manage, care va face modificarile conform solicitarilor.

Principiile GDPR - Exercitiu

Principiul 5: Limitari legate de stocare

INIT CONSULTING si Web IT Manage au inlocuit o politica de stocare a datelor prin care se cere ca orice profil online de pe portal (si care are legatura cu stocarea datelor personale), **care a fost inactiv pentru 24 de luni sa fie suspendat, criptat si arhivat**.

Politica aceasta subiniaza, de asemenea, procedurile exacte care trebuie urmate intocmai **cand se intampla cele mentionate mai sus, inclusive procedurile de urmat pentru stergerea si distrugerea profilelor** online de pe portal si a datelor personale stocate pentru persoanele care nu mai sunt clienti ai INIT CONSULTING.

Principiul 6: Integritate si confidentialitate – securitatea datelor

Atat INIT CONSULTING cat si Web IT Manage au luat **masuri tehnice si organizationale** pentru a securiza datele personale ale clientului impotriva prelucrarii lor neautorizate sau ilegale, priederi accidentale sau distugeri.

Exista acorduri contractuale relevante care subliniaza **responsabilitatile si obligatiile ambelor entitati juridice si ambele companii sunt certificate ISO 27001.**

ISO 27001 – Standardul in Securitatea Informatiilor

Acest Standard in domeniul Securitatii informatiilor raspunde cerintelor Principiului Integritate si confidentialitate – securitatea datelor

Se recomanda astfel sa se incheie acorduri contractuale relevante care sa evidentieze **responsabilitatile si obligatiile ambelor entitati juridice, o masura acceptata si recomandata fiind ca ambele companii sa fie certificate ISO 27001.**

Informatiile. Securitatea Informatiilor

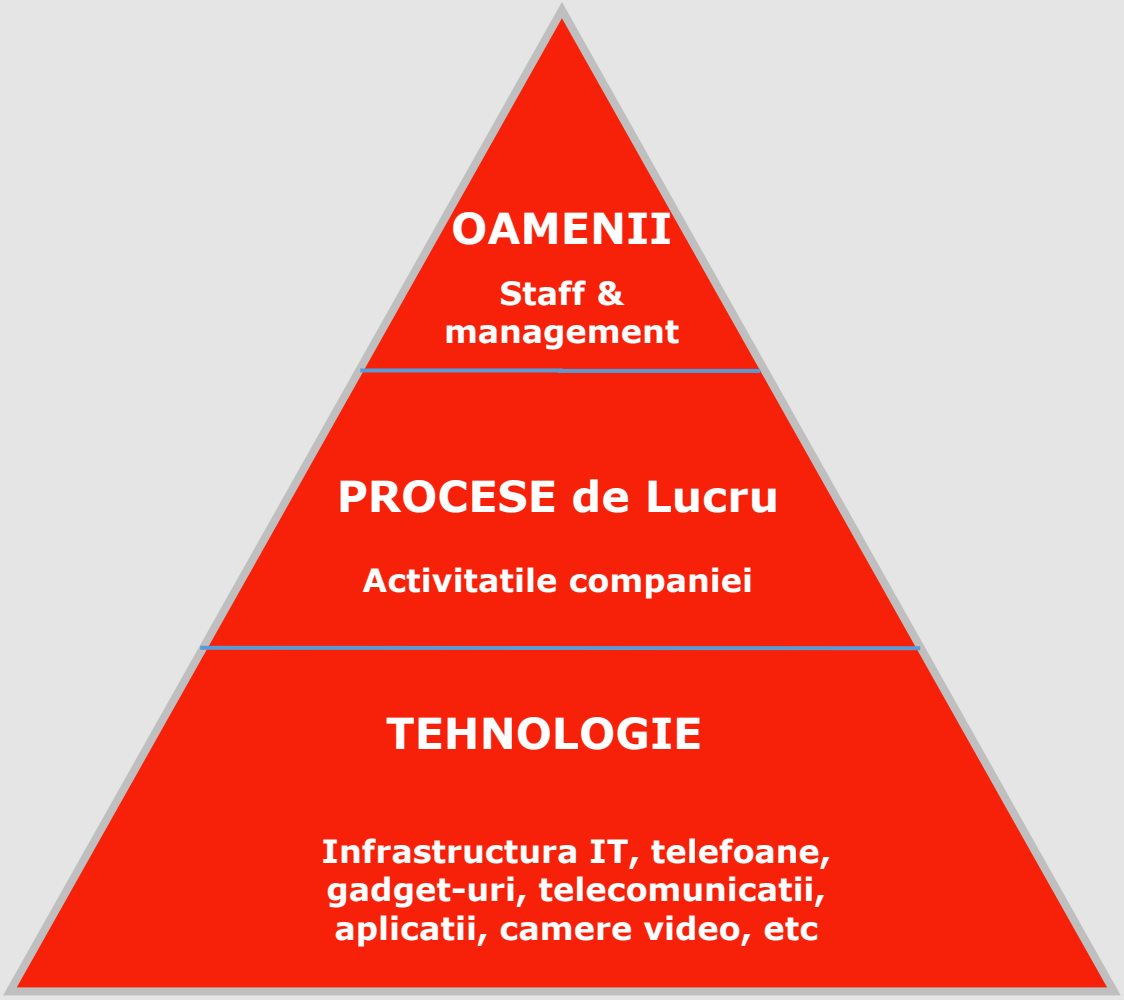
Informația există în mai multe forme:

- Imprimate sau scrise pe hârtie
- Stocată electronic
- Transmis prin poștă sau prin mijloace electronice
- Vizuale, de ex. videoclipuri, diagrame
- Publicat pe Web
- Verbal, de ex. conversații, apeluri telefonice
- Intangibil, de ex. cunoștințe, experiență, expertiză, idei

Securitatea informațiilor reprezinta acele masuri/ tehnici/proceduri ce pastreaza informațiile valoroase protejate, in siguranta.
Nu este ceva ce cumperi, este ceva ce faci
Este un **proces**, nu un produs
Se realizează utilizând o combinație de strategii și abordări adecvate:

- Determinarea riscurilor pentru informație și tratarea acestora în mod corespunzător Protecția C.I.A. (**confidențialitate**, **integritate** și **disponibilitate**)
- **Evitarea, prevenirea, detectarea și recuperarea** in urma incidentelor
- **Securitatea oamenilor, proceselor și tehnologiei ... nu doar IT!**

Informatiile. Securitatea Informatiilor



Securitatea Informatiilor. Elemente de control

- **Politica de securitate a informațiilor**
- **Inventarul si gestionarea activelor** - evaluarea, clasificarea și protejarea bunurilor **informaționale** valoroase
- **Securitatea HR** - securitate pentru cei care se alătură, se muta intre echipe sau parasesc compania
- **Siguranța fizică și de mediu** - împiedică accesul neautorizat, furtul, compromisul, deteriorarea informațiilor și facilitățile de calcul, întreruperile de curent
- **Administrarea și gestionarea operațiunilor** - asigură funcționarea corectă și sigură a IT-ului
- **Controlul accesului** - restricționează accesul neautorizat la activele informatice
- **Achiziționarea, dezvoltarea și întreținerea sistemelor informatice** - construirea de sisteme de securitate
- **Gestionarea incidentelor legate de securitatea informațiilor** - rezolvați în mod sensibil incidentele de securitate care apar
- **Gestionarea continuității afacerii** - mențineți procesele de afaceri esențiale și restaurați orice eșec
- **Conformitate** - evitați încălcarea legilor, reglementărilor, politicilor și altor obligații de securitate

Clasificarea Informatiilor.

CONFIDENŢIAL:
Dacă aceste informații sunt scoase din afara organizației, aceasta va duce la pierderi majore financiare și / sau de imagine. Compromisul acestor informații poate duce la neconformități grave (de exemplu, încălcarea confidențialității). Accesul la aceste informații trebuie restricționat pe baza conceptului de necesitate de a ști. Divulgarea cere aprobarea proprietarului informațiilor. În cazul în care informațiile trebuie divulgate terților, este necesar un acord de confidențialitate semnat.
Exemple: contracte cu clienții, ratele de tarifare, secrete comerciale, informații personale, planuri noi de dezvoltare a produselor, bugete, rapoarte financiare (înainte de publicare), parole, chei de criptare.

NUMAI PENTRU UZ INTERN/ RESTRICTIONATE:
Scurgerea sau dezvăluirea acestor informații în afara organizației este puțin probabil să dăuneze grav, dar poate duce la pierderi financiare și / sau jenă.
Exemple: circulare, politici, materiale de instruire, e-mailuri generale ale companiei, politici și proceduri de securitate, intranet corporativ.

PUBLIC:
Aceste informații pot fi divulgate gratuit oricui, deși publicarea trebuie aprobată în mod explicit de către Managementul Organizatiei sau Marketing.
Exemple: broșuri de marketing, comunicate de presă, site web.

Securitatea Informatiilor.
Ce am de facut?

Securitatea Fizica

DA

- Citiți și respectați politicile și procedurile de securitate
- Afișați Cardurile de acces/ identitate în timp ce vă aflați în incintă
- Fiti atent si raportați pe oricine fără card de identitate
- Vizitați Zona de securitate intranet sau contactati Responsabilul cu Securitatea Informatiilor pentru sfaturi privind cele mai multe probleme de securitate a informațiilor

NU

- NU permiteți accesul vizitatorilor neautorizați în incintă
- NU aduceți arme, materiale periculoase / combustibile, dispozitive de înregistrare etc., în special în zonele protejate
- NU utilizați dispozitive IT personale în scopuri de lucru, cu excepția cazului în care sunt autorizate explicit de conducere

Securitatea Informatiilor.
Ce am de facut?

InITinvest Consulting

Utilizarea Internetului

DA

- Accesul online in timpul orelor de lucru trebuie realizat doar in scopul executarii activitatilor profesionale ce intra in fisa postului

NU

- Evitați site-urile care ar fi clasificate ca obscene, rasiste, ofensive sau ilegale - orice ar fi jenant
- Nu accesați site-urile de licitații sau de cumpărături online, cu excepția cazurilor în care este autorizat de managerul dvs.
- DO NOT hack!
- Nu descărcați sau încărcați software comercial sau alt material protejat prin drepturi de autor fără licența și permisiunea EXPLICITA de la managerul dvs.

! Utilizarea Internetului este monitorizata statistic!!!

Securitatea Informatiilor.
Ce am de facut?

InITinvest Consulting

Accesul la e-mail

DA

- Utilizați e-mailurile de serviciu doar în scopuri profesionale
- Urmați regulile de stocare/arhivare a e-mailurilor
- Dacă primiți e-mail spam, ștergeți-l. Dacă este ofensator sau primiți o mulțime, sunați la Internal IT

NU

- Nu utilizați adresa de e-mail in scop personal
- Nu transmiteti scrisori în lanț, glume necorespunzătoare, videoclipuri etc.
- Nu trimiteți e-mailuri în afara organizației decât dacă sunteți **autorizat** să faceți acest lucru
- Fiți foarte atenți la atașamentele de e-mail și la link-uri, în special în e-mailurile nesolicitate (majoritatea sunt infectate cu virusi)

Securitatea Informatiilor.
Ce am de facut?

Incidentele de Securitate

DA

- Raportați incidentele de securitate, preocupările și problemele legate de securitatea informațiilor la Internal IT cu privire la:
- Mesaje SPAM sau cu un continut neadecvat
- Apeluri telefonice care solicita date personale sau confidentiale
- Documente cu date personale/ restrictionate lasate la vedere

NU

- **Nu discutați** despre incidentele de securitate cu cineva **din afara** organizației
- **Nu încercați să interveniți, să împiedicați sau să împiedicați pe oricine altcineva să raporteze incidente**

Securitatea Informatiilor. Ce am de facut?

Asigurarea Conformitatii cu cerintele de Securitate

- Asigurați-vă că PC-ul dvs. este actualizat și are patch-uri antivirus
- Dezactivati ecranul/contul (Lock -Windows-L) înainte de a lasa computerul nesupravegheat și deconectați-l la sfârșitul zilei.
- NU LASATI LA VEDERE DOCUMENTE CU DATE PERSONALE!!!
- Suporturile pe care se afla informațiile valoroase (documentele, CD-urile, stick-urile USB, etc.) se păstrează în siguranță sub cheie cu acces controlat
- Păstrați informatiile in siguranta în timp ce călătoriți:
  - Reduceti vocea la telefonul mobil in locuri publice
  - Fii discret cu privire la echipamentul tău IT si nu lasa laptopul/ mobilul nesupravegheat sau in masina
- **Îndeplinește-ți obligațiile de securitate:**
  - Respectați legile privind protecția și confidențialitatea, drepturile de autor și licențele, NDA (Acordurile de dezvăluire a informațiilor) și contractele
  - Respectați politicile și procedurile corporative
  - Rămâneți la curent cu securitatea informațiilor:
  - Vizitați zona de securitate intranet atunci când aveți un timp pentru a fi la zi
- Nu va conectati la hubspot-uri externe/ fara parola pentru a accesa Internetul in scop de Business. Foloseste doar surse autorizate de companie!!!
- **NU colectati date personale fara consimtamant sau baza legala!**
- **Daca incepeti un proiect nou, implementati de la inceput (by design& by default) masurile de protectie a datelor cu caracter personal!!!!!**

Va multumim!

(+40) 332 882 879

office@initinvest.ro
contact@justgetit.ro

www.initinvest.ro
www.justgetit.ro

InITinvest Consulting

Just G.E.T. IT by InITinvest