Evaluarea Riscului

by Petrus Cindea petrus.cindea@gmail.com
tel.0722.622.067

GDPR despre Evaluarea Riscului

Recital 76

- **Probabilitatea** de a se materializa si **gravitatea** (**impactul**) **riscului pentru drepturile si libertatile persoanei vizate** trebuie sa fie determinate in functie de natura, domeniul de aplicare, contextul si scopurile prelucrarii datelor cu caracter personal.
- Riscul trebuie apreciat pe baza unei **evaluari obiective** prin care se stabileste daca operatiunile de prelucrare a datelor prezinta un **risc sau un risc ridicat.**

Art.32 aliniatul 2

- La evaluarea nivelului adecvat de securitate, se tine seama in special de **riscurile** prezentate de prelucrare, generate in special, in mod accidental sau ilegal, de **distrugerea**, **pierderea**, **modificarea**, **divulgarea neautorizata** sau **accesul neautorizat** la datele cu caracter personal transmise, stocate sau prelucrate intr-un alt mod.

Dreptul la “privacy”

DEFINITIE

Interesul individului in a-si proteja “**spatiul personal” liber de interferenta cu alte persoane sau organizatii**

Protectia “privacy”-ului este necesara cel putin din anumite motive:

- **Psihologice**
- **Sociale**
- **Economice**
- **Politice**
- **Religioase**

Protectia “privacy”-ului este un proces continuu de a tine in **echilibru interesul legitim al individului pentru “privacy” versus alte interese legitime ale celorlalti indivizi sau organizatii**

by Petrus Cindea petrus.cindea@gmail.com
tel.0722.622.067

Dimensiunile “Privacy”-ului

“Privacy”-ul Comunicatiilor personale
interesul individului de a comunica cu alte prsoane utilizand diverse medii de comunicare fara a fi monitorizat de alti indivizi si organizatii

“Privacy”-ul Corpului
este legat de integritatea corpului, informatii privind sanatatea, decizii de imunizare, transfuzii sange, decizia de sterilizare, prelevare fluide

“Privacy”-ul privind Experienta Personala
informatii legate de experienta personala , ce pot duce la profilare

“Privacy”-ul Datelor Personale
controlul indivudului asupra datelor personale ori de cate ori acestea sunt utilizate de alti indivizi sau organizatii

“Privacy”-ul Comportamentului
preferinte sexuale, obiceiuri, activitate politica sau practica religioasa

by Petrus Cindea petrus.cindea@gmail.com
tel.0722.622.067

Prelucrari de date personale cu potential risc ridicat

- Prelucrarea **categoriilor speciale** de date:

  -date privind originea rasiala sau etnica, opiniile politice, confesiunea religioasa, convingerile filozofice sau apartenenta la sindicate

  -datele genetice, biometrice, privind sanatatea

  -date privind viata sexuala sau orientarea sexuala

  -date privind condamnarile penale si infractiunile sau masuri de securitate conexe

  -date ale unor persoane vulnerabile in special copii
- Prelucrarea implica un **volum mare** de date cu caracter personal si **afecteaza un numar larg** de persoane vizate
- Prelucrari de date ce presupune un proces decizional individual **automatizat**, inclusiv crearea de **profiluri cu efect legal sau semnificativ.**
- Prelucrari de tip "**marketing to individuals**"
- Prelucrari ce presupun **transferul** datelor in afara UE
- Prelucrari ce presupun utilizarea de **tehnologii noi**
- Prelucrari ce reprezinta **activitate principala** pentru operator sau procesator

by Petrus Cindea petrus.cindea@gmail.com
tel.0722.622.067

Cand se impune efectuarea
EVALUARII IMPACTULUI ASUPRA PROTECTIEI DATELOR

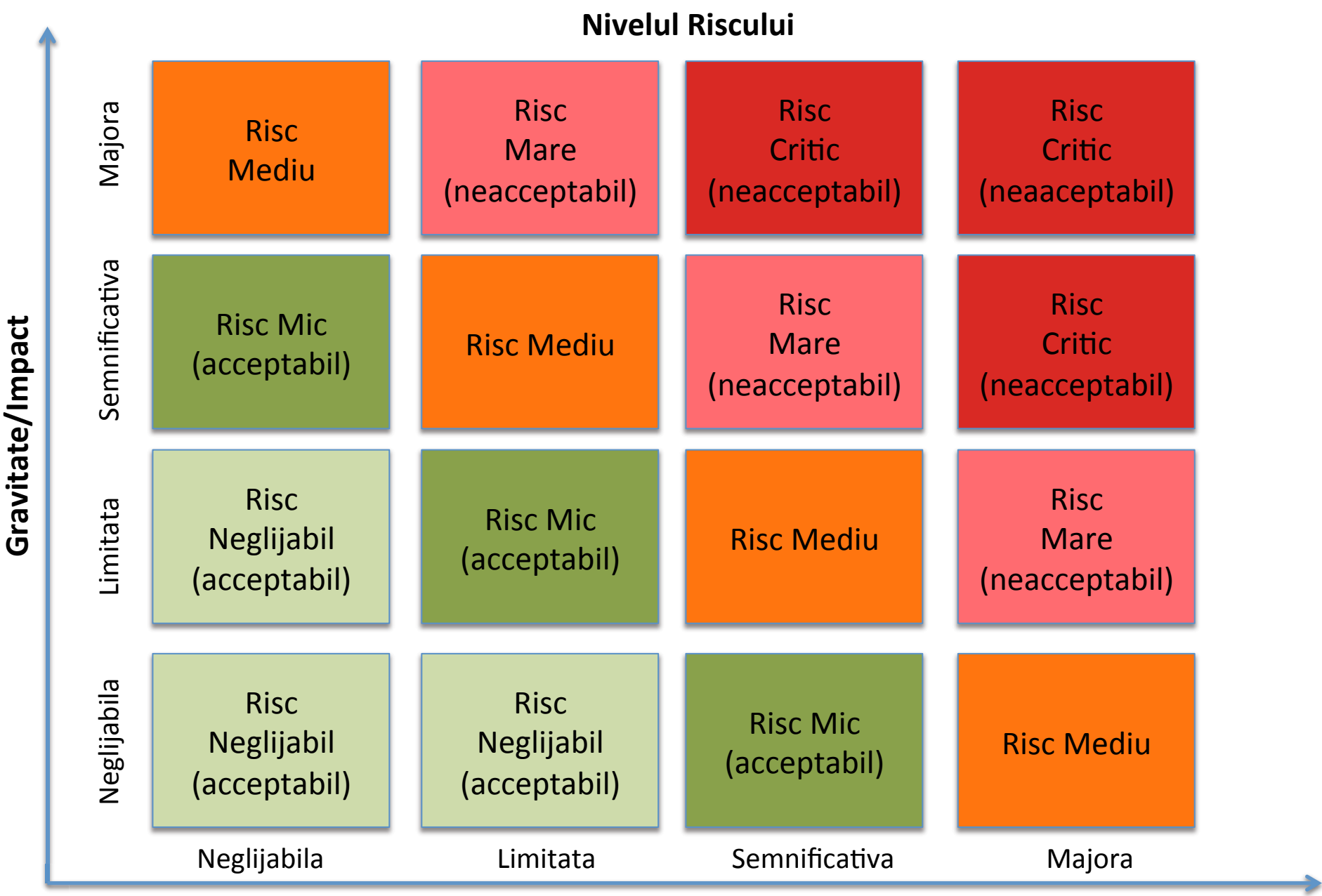
- In cazul unei **evaluari sistematice si cuprinzatoare** a aspectelor personale referitoare la persoane fizice, care se bazeaza pe **prelucrarea automata**, inclusiv crearea de **profiluri**, si care sta la baza unor decizii care produc **efecte juridice** privind persoana fizica sau o **afecteaza semnificativ**.

- In cazul prelcrarii pe **scala larga** a unor **categorii speciale** de date, sau a unor ate cu caracter personal privind **condamnari penale si infarctiuni**.

- In cazul unei **monitorizari sistematice pe scala larga a unei zone accesibile publicului**.

by Petrus Cindea petrus.cindea@gmail.com
tel.0722.622.067

Metoda calitativa de evaluare a riscului



by Petrus Cindea petrus.cindea@gmail.com tel.0722.622.067

Scala de evaluare a gravitatii (impactului)

Gradul de afectare al persoanelor vizate **dupa implementarea masurilor de** control (nivelul impactului dupa implementarea masurilor de control)

- **Neglijabila**: persoanele vizate sau nu vor fi afectate sau vor face fata catorva inconveniente, ce vor fi depasite fara nici o greutate (timp pierdut reintroducand informatia, nemultumire, iritare etc.)

- **Limitata**: persoanele vizate pot face fata unor inconveniente semnificative, pe care le vor putea depasii in ciuda catorva dificultati (extra costuri, refuzul accesului la diverse servicii, frica, neintelegerea situatiei, stres, indispozitii fizice minore, etc.)

- **Semnificativa**: persoanele vizate pot face fata unor consecinte semnificative, pe ar trebui sa le poata depasi chiar daca cu dificultati serioase (frauda de fonduri, “blacklisting” de catre banci, deteriorarea proprietatii, concediere, citatie, inrautatirea starii de sanatate, etc.)

- **Majora**: persoanele vizate pot face fata unor consecinte semnificative sau chiar ireversibile pe care ar puea sa nu le poata depasi (probleme grave financiare precum fonduri , pierderea capacitatii de a lucra, afectiuni fizice sau psihologice, moarte, etc.

by Petrus Cindea petrus.cindea@gmail.com
tel.0722.622.067

Scara de evaluare a probabilitatii

Probabilitatea ca **sursa** de risc selectata sa concretizeze (materializeze) **amenintarea** prin exploatarea **vulnerabilitatilor** aferente **activelor** (**asset**-urilor) tehnice si organizationale

- **Neglijabila**: nu pare sa fie posibila pentru sursele de risc selectate (ex. furtul documentelor printate depozitate intr-o locatie protejata de un sistem de control acces cu cititor magnetic si cod de acces)
- **Limitata**: pare sa fie dificila pentru sursele de risc selectate (ex. furtul documentelor printate depozitate intr-o locatie protejata de un sistem de control acces cu cititor magnetic)
- **Semnificativa**: pare sa fie posibila pentru sursele de risc selectate (ex. furtul documentelor printate aflate intr-un birou ce nu poate fi accesat decat dupa o verificare a persoanei la intrarea in cladire-receptie)
- **Majora**: pare sa fie extrem de usoara pentru sursele de risc selectate (ex. furtul documentelor depozitate in lobby)

Etapele Evaluarii Riscurilor

- Identificarea asset-urilor
- Identificarea amenintarilor
- Identificarea masurilor de securitate tehnice si organizatorice existente
- Identificarea vulnerabilitatilor aferente asset-urilor
- Identificarea impactului (consecintele materializarii riscului)

- Evaluarea gravitatii impactului (consecintele gravitatii)
- Evaluarea probabilitatii de concretizare (materializare) a amenintarii
- Determinarea nivelului de risc

- Evaluarea nivelului de risc bazat pe criteriile de evaluare a riscurilor

Exemple de asset-uri

- **Tehnice**
  - Hardware
  - Electronic data media
  - Software
  - Canale de comunicatii
  - Site
  - Etc.
- **Organizatorice**
  - Oameni
  - Documente scrise/ tiparite
  - Elemente de stocare fizica
  - Canale de transmitere a documentelor
  - Etc.

Cele TREI tipuri riscuri care se analizeaza

- **Accesul neautorizat** (nelegitim) la datele cu caracter personal
- **Modificarea nedorite** (neautorizate) a datelor cu caracter personal
- **Disparitia** (distrugerea) datelor cu caracter personal

by Petrus Cindea petrus.cindea@gmail.com
tel.0722.622.067

Tipul surselor ce pot genera riscuri

- **Sursa umana din interior**- angajati, operatori interni, IT manageri, manageri, etc.
- **Sursa umana din exterior**- destinatari ai datelor cu caracter personal, terte parti autorizate, furnizori de servicii, hackeri, vizitatori, exangajati, competitori, clienti, personal de mentenanta, etc
- **Surse neumane**- malware (virusi, etc.), apa (conducte, inundatii etc.), substante inflamabile, corozive sau explozive, dezastre naturale, epidemii, animale etc.

by Petrus Cindea petrus.cindea@gmail.com
tel.0722.622.067

Actiuni ce pot duce la materializarea riscurilor

- **Accesul neautorizat**-utilizarea anormala, observarea, spionaj, alterare, pierdere, manipulare
- **Modificare nedorita**-alterare, utilizare anormala, supraincarcare, manipulare
- **Disparitie**- utilizare anormala, supraincarcare, alterare, distrugere, pierdere,

by Petrus Cindea petrus.cindea@gmail.com
tel.0722.622.067

Amenințări generice

Asset-Activ	Acțiune	Privacy Risc	Exemple de amenințări
Hardware	Utilizare anormală	Dispariția PII*	Stocarea fișierelor personale; uz personal etc.
Hardware	Utillizare anormală	Accesul neautorizat la PII	Utilizarea unităților flash USB sau a discurilor care nu sunt adecvate sensibilității informațiilor; utilizarea sau transportul hardware-ului sensibil în scopuri personale etc
Hardware	Deteriorarea	Dispariția PII	Inundare; foc; vandalism; daune cauzate de uzură naturală; defectarea dispozitivului de stocare etc.
Hardware	Spionaj	Accesul neautorizat la PII	vizualizarea ecranului unei persoane fără știința acesteia; realizarea unei fotografii a unui ecran; geolocalizarea unui echipament hardware; detectarea la distanță a semnalelor electromagnetice etc.
Hardware	Pierderea	Dispariția PII	Furtul unui leptop sau smartphone; eliminarea unui dispozitiv hardware etc.
Hardware	Pierderea	Accesul neautorizat la PII	Furtul unui laptop dintr-o cameră de hotel; furtul din buzunar al unui smartphone; recuperarea neautorizată a unui dispozitiv de stocare aruncat sau a unuia hardware etc.
Hardware	Modificarea	Dispariția PII	Adăugarea de echipamente incompatibile, fapt ce poate duce la defecțiuni; îndepărtarea unor componente esențiale pentru buna funcționare a sistemului etc.
Hardware	Modificarea	Accesul neautorizat la PII	Urmărirea prin intermediul unui dispozitiv hardware de tip keylogger; îndepărtarea unor componente hardware; conectarea unor dispozitive (cum ar fi flas drive-urile USB) pentru a lansa un sistem de operare sau de recuperare de date etc.

*PII – Personaly identifying information-Date cu caracter personal

by Petrus Cindea petrus.cindea@gmail.com tel.0722.622.067

Amenințări generice - continuare

Active	Acțiune	Privacy Risc	Exemple de amenințări
Hardware	Modificarea	Modificări nedorite a PII	Adăugarea de echipamente incompatibile, fapt ce poate duce la defecțiuni; ; îndepărtarea unor componente esențiale pentru buna funcționare a unei aplicații etc.
Hardware	Supraîncărcarea	Dispariția PII	Dispozitiv de stocare plin; supraîncărcarea capacității de procesare; supraîncălzirea; temperaturi excesive etc;
Hardware	Pierderea unui hard drive	Accesul neautorizat la PII	Contracte de mentenanță defectuoase sau procese de eliminare prost efectuate ce pot conduce la acces neautorizat le IPI
Software	Utilizare anormală	Dispariția PII	Ștergerea datelor; utilizarea de soft copiat sau contrafăcut; eroarea unui oprator care poate șterge datele etc.
Software	Utilizare anormală	Accesul neautorizat la PII	Scanare de conținut; referențiere încrucișată neautorizată a datelor; creșterea privilegiilor; ștergerea urmelor de utilizare; transmiterea de mesaje tip spam printr-un program de email; folosirea greșită a funcțiilor unei rețele etc.
Software	Utilizare anormală	Modificări nedorite a PII	Modificări nedorite a datelor în baza de date; ștergerea unor fișiere necesare funcționării corecte a unui soft; modificarea unor date din eroarea unui operator etc.
Software	Deteriorarea	Dispariția PII	Ștergerea unui fișier executabil sau a unui cod sursă; bombă logică etc.

by Petrus Cindea petrus.cindea@gmail.com
tel.0722.622.067

Amenințări generice - continuare

Active	Acțiune	Privacy Risc	Exemple de amenințări
Software	Spionaj	Accesul neautorizat la PII	Scanarea adreselor de rețea și a porturilor; colectarea datelor de configurare; analizarea codurilor sursă cu scopul de localizarea a vulnerabilităților; testarea modului cum răspund bazele de date la interogări dușmănoase etc.
Software	Spionaj	Accesul neautorizat la PII	Scanarea adreselor de rețea și a porturilor; atacarea vulnerabilităților în porturile și serviciile de ascultare, analiză, raportare etc.
Software	Dispariția IPI	Accesul neautorizat la PII	Neprelungirea licențelor de soft folosite pentru accesarea datelor
Software	Modificarea	Dispariția PII	Erori în timpul update-urilor, configurărilor sau mentenanței; infectarea cu malware; înlocuirea unor componente etc.
Software	Modificarea	Accesul neautorizat la PII	Urmărirea prin intermediul unui soft de tip keylogger; infectarea cu malware; instalarea unei unelte de administrare la distanță; substituirea componentelor etc.
Software	Utilizare anormală	Modificări nedorite a PII	Erori în timpul update-urilor, configurărilor sau mentenanței; infectarea cu malware; înlocuirea unor componente etc.
Software	Supraîncărcarea	Dispariția PII	Depășirea dimensiunii unei baze de date; injectarea cu dat din afara gamei de valori etc.
Rețea	Deteriorarea	Dispariția PII	Tăierea cablurilor; recepție wi-fi slabă etc.
Rețea	Spionaj	Accesul neautorizat la PII	Interceptarea traficului prin Ethernet; colectarea de date transmise prin reteaua wi-fi etc.
Rețea	Pierderea	Dispariția PII	Furtul cablurilor de cupru etc.

Amenințări generice - continuare

Active	Acțiune	Privacy Risc	Exemple de amenințări
Rețea	Modificare	Modificări nedorite a PII	Atac de tipul man-in-the-middle sau man-in-the-browser pentru a modifica sau adăuga date la traficul prin rețea; atac reluat (retrimiterea datelor inteceptate) etc.
Rețea	Supraîncărcarea	Dispariția PII	Folosirea eronată a benzii de date; download-area neautorizată; Pierderea legăturii la internet etc.
Persoane	Utilizare anormală	Acces neautorizat la PII	Influențare (prin phising, mită etc.); presiune (șantaj, hărțuire psihologică etc.) etc.
Persoane	Utilizare anormală	Modificări nedorite a PII	Influențare (zvonuri, dezinformare etc.) etc.
Persoane	Deteriorarea	Dispariția PII	Accident profesional; boli profesionale; alte răniri sau boli; deces; afecțiuni neurologice, psihologice sau psihiatrice etc.
Persoane	Spionaj	Acces neautorizat la PII	Divulgare neintenționată a informațiilor în timpul unei conversații; folosirea de echipamente de ascultare în cadrul întâlnirilor etc.
Persoane	Pierderea	Dispariția PII	Realocarea; finalizarea contractului sau rezilierea lui; preluarea parțială sau totală a unei organizații etc.
Persoane	Pierderea	Acces neautorizat la PII	Recrutare ilegală; schimbarea sarcinilor de lucru; preluarea parțială sau totală a unei organizații etc.
Persoane	Supraîncărcarea	Dispariția PII	Volum mare de lucru, stres sau schimbări cu efect negativ în condițiile de luru; însărcinarea angajaților cu obligații peste abilitățile lor; slaba utilizare a aptitudinilor etc.
Persoane	Supraîncărcarea	Modificări nedorite a PII	Volum mare de lucru, stres sau schimbări cu efect negativ în condițiile de luru; însărcinarea angajaților cu obligații peste abilitățile lor; slaba utilizare a aptitudinilor etc.

by Petrus Cindea petrus.cindea@gmail.com
tel.0722.622.067

Amenințări generice - continuare

Active	Acțiune	Privacy Risc	Exemple de amenințări
Documente	Deteriorarea	Dispariția PII	Îmbătrânirea arhivei de documente; arderea unor documente în cursul unui incendiu etc.
Documente	Spionaj	Acces neautorizat la PII	Citirea; fotocopierea; fotgrafierea etc.
Documente	Pierderea	Dispariția PII	Furtul de documente; Pierderea unor dosare în timpul unei relocări; eliminarea etc.
Documente	Pierderea	Acces neautorizat la PII	Furtul unor dosare din birouri; furtul de corespondență din cutia poștală; recuperarea unor documente aruncate etc.
Documente	Modificarea	Modificări nedorite a PII	Modificarea unor cifre dintr-un dosar; înlocuirea originalului cu un fals etc.
Documente	Supraîncărcarea	Dispariția PII	Ștergerea graduală (în timp); ștergerea cu intenție a unor porțiuni dintr-un document etc.
Canalele de transmitere a hârtiilor	Deteriorarea	Dispariția PII	Sfârșitul unui flux de lucru datorat unei reorganizări; Oprirea livrării corespondenței datorită unei greve etc.
Canalele de transmitere a hârtiilor	Spionaj	Acces neautorizat la PII	Citirea documentelor semnate ce sunt în circulație; reproducerea unor documente în tranzit etc.
Canalele de transmitere a hârtiilor	Pierderea	Dispariția PII	Eliminarea unui proces, ulterior unei reorganizări; Pierderea unei companii de livrare a documentelor etc.
Canalele de transmitere a hârtiilor	Modificarea	Dispariția PII	Modificarea modului de transmitere a corespondenței; Reorganizarea canalelor de transmitere a hârtiilor; schimbarea limbajului de lucru etc.

by Petrus Cindea petrus.cindea@gmail.com
tel.0722.622.067

Amenințări generice - continuare

Active	Acțiune	Privacy Risc	Exemple de amenințări
Canalele de transmitere a hârtiilor	Modificarea	Modificari nedorite a PII	Schimbarea unui memo fără înștiințarea autorului; transmiterea mai multor documente contradictorii etc.
Canalele de transmitere a hârtiilor	Supraîncărcarea	Dispariția PII	Supraîncărcarea serviciului de corespondență; Suprasolicitarea procesului de validare etc.

Registrul de Analiza al Riscurilor

- Document ce contine analiza de risc aferenta elementelor ce alcatuiesc un proces cuprinzand urmatoarele elemente
  - Asset-Activ
  - Riscul
  - Sursa Riscului
  - Actiune
  - Amenintare
  - Vulnerabilitatea aferenta asset-ului
  - Impact asupra persoanelor vizate
  - Elementele de control existente
  - Gravitatea impactului
  - Probabilitatea de concretizare (materializare) a riscului
  - Evaluarea Riscului

Model cap de tabel
Registrul de Analiza al Riscurilor

Risc	Impact asupra persoa-nelor vizate	Sursa de risc	Amenintarile principale	Masuri de control existente	Gravitatea impctului	Probabi-litatea riscului	Evaluarea riscului
Acces neautorizat							
Modificare nedorita							
Disparitie							

by Petrus Cindea petrus.cindea@gmail.com
tel.0722.622.067