

VIMERCATI EAST EUROPE SRL	METODOLOGIA DE EVALUARE SI TRATARE A RISCURILOR LA ADRESA DATELOR CU CARACTER PERSONAL	Pagina 1 din 9
	Cod document: POL-GDPR-01	Versiunea 1.0

DATA	18.07.2018	SEMNATURA
ELABORAT	CONSULTANT – LIVIU MINCIUNA	
VERIFICAT	RPD - COJOCARU ROXANA	
APROBAT	DIRECTOR GENERAL – CONSTANTIN HUMA	

1. SCOP

- 1.1. Identificarea prelucrărilor de date și a funcționalităților ce prezintă un posibil risc ridicat ce poate afecta viața privată a persoanelor vizate.
- 1.2. Identificarea amenințărilor și vulnerabilităților.
- 1.3. Analiza impactului asupra vieții private.
- 1.4. Evaluarea riscurilor.
- 1.5. Identificarea măsurilor de tratare a riscurilor.

2. DOMENIUL DE APLICARE

- 2.1. Metodologia se aplică resurselor suport pentru prelucrarea datelor: hardware, software, personal, servicii și utilități, documente în format tipărit.

3. DOCUMENTE DE REFERINȚĂ

- 3.1. ISO/IEC 27001:2013 - Tehnologia informației - Tehnici de securitate - Sisteme de management al securității informațiilor - Cerințe.
- 3.2. ISO/IEC 27005:2011 – Information Technology. Security techniques. Information security risk management.
- 3.3. ISO/IEC 29134:2017 - Information technology. Security techniques. Guidelines for privacy impact assessment.
- 3.4. REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

4. DEFINIȚII ȘI PRESCURTĂRI

4.1. DEFINIȚII

- 4.1.1. **Date cu caracter personal:** orice informații privind o persoană fizică identificată sau identificabilă ("persoana vizată" sau „subiect”), cum ar fi: nume, un număr de identificare, date de localizare, un identificator online, sau elemente specifice, proprii identității sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale.
- 4.1.2. **Prelucrare:** orice operațiune sau set de operațiuni efectuate asupra datelor cu caracter personal sau asupra seturilor de date cu caracter personal, cu sau fără utilizarea de mijloace automatizate, cum ar fi colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, divulgarea prin transmitere, diseminarea sau punerea la dispoziție în orice alt mod, alinierea sau combinarea, restricționarea, ștergerea sau distrugerea.
- 4.1.3. **Amenințare:** o cauză potențială a unui incident nedorit care poate afecta un sistem sau o organizație.

VIMERCATI EAST EUROPE SRL	METODOLOGIA DE EVALUARE SI TRATARE A RISCURILOR LA ADRESA DATELOR CU CARACTER PERSONAL	Pagina 2 din 9
	Cod document: POL-GDPR-01	Versiunea 1.0

- 4.1.4. **Vulnerabilitate:** o slabiciune a unei resurse sau mai multe care poate fi exploatata de o amenintare; un set de conditii existente care pot permite unei amenintari sa afecteze o resursa.
- 4.1.5. **Risc:** posibilitatea ca o anumită amenințare să exploateze o vulnerabilitate a sistemului sau a unei resurse particulare și să cauzeze distrugerea sau expunerea acestei resurse.
- 4.1.6. **Evaluarea riscului:** procesul general de analiza si estimare a riscului.

5. DESCRIEREA PROCEDURII

Procesul de management al riscurilor este prezentat în figura următoare:



Evaluarea si tratarea riscului cuprinde următoarele etape:

- E1 - Se identifică **prelucrările de date** care prezinta un posibil risc ridicat la adresa vietii private.
- E2 - Se identifică **amenințările** la care sunt pasibile datele cu caracter personal si **vulnerabilitatile** care le determina (scenariile de risc). Sunt identificate **controalele de securitate existente**.
- E3 - Se cuantifică **gradul de impact al amenințărilor (analiza de impact)**. Se cuantifică **probabilitatea materializării amenințării**. Pe baza valorilor cuantificate anterior se calculează **nivelul de risc**.
- E4 – Se face **analiza de risc**.
- E5 – Se identifica si se selecteaza **masurile (controalele) de securitate**, in vederea reducerii riscurilor.
- E6 – Se cuantifica probabilitatea si impactul in urma aplicarii controalelor de securitate selectate. Se calculeaza si se aproba de catre management **riscul rezidual**.
- E7 - Se elaboreaza **planul de tratare a riscurilor**.

1. Identificarea prelucrarilor de date cu posibil risc ridicat

Se identifica prelucrările de date cu posibil risc ridicat la adresa vietii private a persoanelor vizate:

Evaluare, profilare, predictie (aspecte privind performanța persoanei vizate la locul de muncă, situația economică, sănătatea, preferințele sau interesele personale, comportamentul, locația sau mișcările)
Luarea automata a deciziilor cu efect juridic sau similar semnificativ (daca prelucrarea poate duce la excluderea sau discriminarea persoanelor)
Monitorizarea sistematica

VIMERCATI EAST EUROPE SRL	METODOLOGIA DE EVALUARE SI TRATARE A RISCURILOR LA ADRESA DATELOR CU CARACTER PERSONAL	Pagina 3 din 9
	Cod document: POL-GDPR-01	Versiunea 1.0

Prelucrarea unor informatii sensibile (date privind originea rasială sau etnică, opinii politice, credințe religioase sau filosofice, apartenența la un sindicat, date genetice, date biometrice, date privind sănătatea, date referitoare la viața sau orientarea sexuală) sau date cu caracter personal referitoare la condamnări penale și infracțiuni
Prelucrările de date pe scara larga (procent relevant din populatie, volume mari de date, prelucrare permanenta a datelor sau de durata mare, intindere regionala sau nationala)
Prelucrarea de date aparținând unor persoane vulnerabile (copii, bolnavi mintal, solicitanți de azil, batrani, pacienti internati etc.)
Utilizarea unor solutii inovative tehnologice sau organizationale
Prelucrarea datelor poate avea ca efect impiedicarea accesului persoanelor vizate la exercitarea unor drepturi sau utilizarea unor servicii sau a unui contract

Pentru acestea se face analiza de impact si evaluarea riscului.

2. Identificarea scenariilor de risc

Se identifica amenintarile proprii fiecărei categorii de resurse suport pentru datele cu caracter personal, precum si controalele existente. Un exemplu este prezentat in tabelul urmator:

Resursa suport	Tip actiune	Amenintare	Risc la adresa datelor
Hardware	Utilizare improprie	Utilizarea echipamentului continand informatie sensibila in scop personal.	Pierdere
Hardware	Utilizare improprie	Utilizarea echipamentului continand informatie sensibila in scop personal.	Divulgare
Hardware	Utilizare improprie	Utilizarea unităților flash USB sau a discurilor nepotrivite sensibilitatii informațiilor.	Divulgare
Hardware	Deteriorare	Inundatie, incendiu, vandalism.	Pierdere
Hardware	Deteriorare	Deteriorare datorata uzurii. Functionare defectuoasa a dispozitivelor de stocare.	Pierdere
Hardware	Spionaj	Urmărirea ecranului fara stirea utilizatorului. Fotografierea ecranului.	Divulgare
Hardware	Pierdere	Furtul unui laptop, smartphone sau dispozitiv de stocare.	Pierdere
Hardware	Pierdere	Scoaterea din functiune a unui dispozitiv de stocare sau echipament fara salvarea datelor.	Pierdere
Hardware	Pierdere	Furtul unui laptop, smartphone sau dispozitiv de stocare.	Divulgare
Hardware	Pierdere	Scoaterea din functiune necorespunzatoare a unui dispozitiv de stocare sau echipament si recuperarea neautorizata a acestuia.	Divulgare
Hardware	Modificare	Lipsa de control asupra schimbarilor de configurare.	Pierdere
Hardware	Modificare	Lipsa de control asupra schimbarilor de configurare.	Corupere

VIMERCATI EAST EUROPE SRL	METODOLOGIA DE EVALUARE SI TRATARE A RISCURILOR LA ADRESA DATELOR CU CARACTER PERSONAL	Pagina 4 din 9
	Cod document: POL-GDPR-01	Versiunea 1.0

Resursa suport	Tip actiune	Amenintare	Risc la adresa datelor
Hardware	Supraincarcare	Unitatea de stocare este plină. Supraincarcarea capacitatilor de procesare.	Pierdere
Hardware	Supraincarcare	Caderea alimentarii cu energie.	Pierdere
Hardware	Supraincarcare	Supraincalzire.	Pierdere
Hardware	Utilizare improprie	Acorduri necorespunzatoare cu furnizorii de mentenanta, care pot avea ca rezultat accesul neautorizat la date.	Divulgare
Hardware	Deteriorare	Taierea / furtul cablurilor.	Pierdere
Hardware	Supraincarcare	Utilizarea necorespunzătoare a lăţimii de bandă. Descarcari neautorizate.	Pierdere
Hardware	Deteriorare	Receptie Wi-Fi defectuoasa.	Pierdere
Hardware	Spionaj	Interceptarea traficului Ethernet. Achiziţionarea datelor trimise prin intermediul unei reţele Wi-Fi.	Divulgare
Software	Utilizare improprie	Utilizarea de software contrafacut sau copiat.	Pierdere
Software	Utilizare improprie	Prelucrare neautorizata de date. Acordarea necontrolata a unor privilegii.	Divulgare
Software	Utilizare improprie	Lipsa log-urilor de utilizator sau stergerea acestora.	Divulgare
Software	Utilizare improprie	Modificari neautorizate a datelor in bazele de date. Stergerea unor fisiere necesare functionarii corecte a software-ului. Erori ale operatorilor avand ca rezultat modificari ale datelor etc.	Corupere
Software	Deteriorare	Stergerea unor executabile sau a unor coduri sursa etc.	Pierdere
Software	Spionaj	Hacking: Scanarea IP-urilor şi a porturilor. Colectarea datelor de configurare. Analiza codurilor sursă pentru a identifica defectele exploatabile. Testarea modului în care bazele de date răspund unor interogări rău intenţionate etc.	Divulgare
Software	Pierdere	Neînnoirea licenţelor software. Neinstalarea actualizarilor si patch-urilor recomandate de producator.	Pierdere
Software	Modificare	Erori în timpul actualizărilor sau configurarilor.	Pierdere
Software	Modificare	Erori în timpul actualizărilor sau configurarilor.	Corupere
Software	Modificare	Infectarea cu malware.	Pierdere
Software	Modificare	Infectarea cu malware.	Divulgare
Software	Modificare	Infectarea cu malware.	Corupere
Software	Modificare	Instalarea unui instrument de administrare de la distanta.	Divulgare

VIMERCATI EAST EUROPE SRL	METODOLOGIA DE EVALUARE SI TRATARE A RISCURILOR LA ADRESA DATELOR CU CARACTER PERSONAL	Pagina 5 din 9
	Cod document: POL-GDPR-01	Versiunea 1.0

Resursa suport	Tip actiune	Amenintare	Risc la adresa datelor
Software	Supraincarcare	Depășirea mărimii bazei de date; incarcarea datelor peste intervalului normal de valori.	Pierdere
Software	Spionaj	Lipsa procedurilor privind aprobarea drepturilor de acces, inregistrarea si stergerea utilizatorilor, abuz de drepturi.	Divulgare
Software	Deteriorare	Lipsa procedurilor privind aprobarea drepturilor de acces, inregistrarea si stergerea utilizatorilor, abuz de drepturi.	Corupere
Software	Pierdere	Lipsa procedurilor privind aprobarea drepturilor de acces, inregistrarea si stergerea utilizatorilor, abuz de drepturi.	Pierdere
Personal	Utilizare improprie	Influență (phishing, inginerie socială, luare de mită etc.). Presiune (șantaj, hărțuire psihologică etc.).	Divulgare
Personal	Deteriorare	Accident. Imbolnavire. Deces. Afectiuni neurologice sau psihice.	Pierdere
Personal	Spionaj	Divulgarea neintentionata de informatii in timpul conversatiilor. Utilizarea dispozitivelor de ascultare pentru ascultarea întâlnirilor.	Divulgare
Personal	Pierdere	Realocarea personalului. Terminarea sau suspendarea contractului de munca. Preluarea organizatiei sau a unei parti a acesteia.	Pierdere
Personal	Pierdere	Realocarea personalului. Terminarea sau suspendarea contractului de munca. Preluarea organizatiei sau a unei parti a acesteia.	Divulgare
Personal	Supraincarcare	Volumul mare de muncă, stresul sau schimbările negative în condițiile de muncă; alocarea angajaților la sarcini care depășesc abilitățile acestora; utilizarea necorespunzatoare a competențelor.	Pierdere
Personal	Supraincarcare	Volumul mare de muncă, stresul sau schimbările negative în condițiile de muncă; alocarea angajaților la sarcini care depășesc abilitățile acestora; utilizarea necorespunzatoare a competențelor.	Corupere
Personal	Utilizare improprie	Stergerea datelor. Erori umane avand ca rezultat stergerea datelor.	Pierdere
Servicii si utilitati	Supraincarcare	Pierderea conexiunii la Internet.	Pierdere
Servicii si utilitati	Deteriorare	Inundatie. Distrugerii la nivelul infrastructurii.	Pierdere
Servicii si utilitati	Deteriorare	Acces fizic necontrolat sau control inadecvat.	Pierdere

VIMERCATI EAST EUROPE SRL	METODOLOGIA DE EVALUARE SI TRATARE A RISCURILOR LA ADRESA DATELOR CU CARACTER PERSONAL	Pagina 6 din 9
	Cod document: POL-GDPR-01	Versiunea 1.0

Resursa suport	Tip actiune	Amenintare	Risc la adresa datelor
Documente tiparite	Deteriorare	Imbatranirea sau deteriorarea documentelor arhivate.	Pierdere
Documente tiparite	Deteriorare	Arderea documentelor in timpul unui incendiu.	Pierdere
Documente tiparite	Spionaj	Citire, copiere, fotografiere.	Divulgare
Documente tiparite	Pierdere	Furtul documentelor. Pierderea documentelor in timpul mutarilor. Eliminarea necontrolata a documentelor.	Pierdere
Documente tiparite	Pierdere	Furtul documentelor. Pierderea documentelor in timpul mutarilor. Eliminarea necontrolata a documentelor si recuperarea neautorizata a acestora.	Divulgare
Documente tiparite	Modificare	Modificarea unor date intr-un document. Inlocuirea originalului cu un fals.	Corupere
Documente tiparite	Supraincarcare	Stergerea intentionata a unor portiuni din document.	Pierdere
Documente tiparite	Deteriorare	Modificarea modului de livrare a corespondentei. Reorganizarea canalelor de transmitere. Oprirea livrarii corespondentei datorita unei greve. Pierderea firmei de curierat.	Pierdere
Documente tiparite	Spionaj	Citirea documentelor aflate in tranzit.	Divulgare
Documente tiparite	Modificare	Modificarea continutului fara stirea autorului.	Corupere

Nota: Informatia din tabel nu este exhaustiva.

3. Stabilirea probabilitatii si impactului amenintarilor si calculul nivelului de risc

Pentru fiecare categorie de date cu caracter personal ce face obiectul analizei, se cuantifica impactul si probabilitatea asociate fiecarei amenintari si vulnerabilitati.

Se estimeaza valoarea probabilitatii functie de controalele de securitate existente la nivelul resurselor suport:

Neglijabil – multiple controale de securitate existente; niciun incident inregistrat in ultimul an.	1
Limitat – cel putin un control de securitate existent; 1 incident inregistrat in ultimul an.	2
Semnificativ – niciun control de securitate existent; 2 incidente inregistrate in ultimul an.	3
Maxim – niciun control de securitate existent; 3 sau mai multe incidente inregistrate in ultimul an.	4

VIMERCATI EAST EUROPE SRL	METODOLOGIA DE EVALUARE SI TRATARE A RISCURILOR LA ADRESA DATELOR CU CARACTER PERSONAL	Pagina 7 din 9
	Cod document: POL-GDPR-01	Versiunea 1.0

Se estimeaza valoarea impactului pierderii confidentialitatii, disponibilitatii sau integritatii datelor cu caracter personal asupra viatii private a subiectilor (PIA):

Neglijabil - subiectii fie nu vor fi afectați, fie pot întâmpina câteva inconveniente, pe care le vor depăși fără nici o problemă (timpul petrecut pentru reintroducerea informațiilor, deranjamente, iritații etc.). Exemple: date accesibile publicului (ex. directoare telefonice, cărți de adrese sau liste de selecție)	1
Limitat - subiectii pot întâmpina inconveniente semnificative, pe care le vor putea depăși în ciuda unor dificultăți (costuri suplimentare, împiedicarea accesului la servicii, frică, lipsă de înțelegere, stres, boli minore etc.). Exemple: date accesibile doar în baza unui interes legitim (ex. fișiere publice restricționate sau membri ai unei liste de distribuție)	2
Semnificativ - subiectii pot întâmpina consecințe semnificative, pe care le pot depăși cu dificultăți serioase (deturnarea fondurilor, listarea neagră la bănci, pagube materiale, pierderea locului de muncă, acționarea în instanță, agravarea stării de sănătate etc.). Exemple: date a căror divulgare neautorizată poate afecta reputația subiectului (ex. informații despre venituri, prestații sociale, impozite pe proprietate sau sancțiuni)	3
Maxim - subiectii pot întâmpina consecințe semnificative sau chiar ireversibile, pe care nu le pot depăși (dificultăți financiare cum ar fi datoriile neoperabile sau incapacitate de muncă, boli psihologice sau fizice pe termen lung, deces etc.). Exemple: date a căror divulgare, modificare, pierdere sau distrugere neautorizată poate afecta existența sau sănătatea, libertatea și viața subiectului (de exemplu, informații despre angajamentul față de o instituție, sentințe, evaluări de personal, date privind sănătatea, datoriile inoperabile sau situații în care subiectul risca să devină victimă într-un caz penal)	4

Nivelul de risc = probabilitate x impact.

4. Analiza de risc

Nivelul de risc se încadrează în matricea de expunere următoare:

Nivelul riscului				
Probabilitate	Impact			
	Neglijabil 1	Limitat 2	Semnificativ 3	Maxim 4
Neglijabil 1	1	2	3	4
Limitat 2	2	4	6	8
Semnificativ 3	3	6	9	12
Maxim 4	4	8	12	16

Ierarhizarea riscurilor va fi folosită pentru identificarea opțiunilor de tratare a riscurilor:

1-6: Minor: Menținerea controalelor existente
8-12: Semnificativ: Acțiuni corective planificate
16: Major: Acțiuni corective prioritare

VIMERCATI EAST EUROPE SRL	METODOLOGIA DE EVALUARE SI TRATARE A RISCURILOR LA ADRESA DATELOR CU CARACTER PERSONAL	Pagina 8 din 9
	Cod document: POL-GDPR-01	Versiunea 1.0

5. Selectia masurilor (controalelor) de securitate

Pentru riscurile incadrate in categoriile Major si Semnificativ, sunt identificate si selectate controalele de securitate aplicabile (a se vedea Anexa A / ISO 27001:2013, fara a se limita la aceste controale).

6. Calculul riscului rezidual

Se estimeaza noile valori ale probabilitatii si impactului in urma aplicarii masurilor (controalelor) selectate si se calculeaza riscul rezidual.

7. Tratarea riscului

Se elaboreaza planul de tratare a riscului, pentru riscurile incadrate in categoriile Major si Semnificativ, pentru care au fost identificate si selectate controalele de securitate aplicabile.

8. Reevaluarea riscului

Reevaluarea de risc se face la fiecare 3 ani sau daca sunt modificari semnificative in prelucrarile de date efectuate sau in contextul organizatiei.

6. INREGISTRARI

- 6.1. Scenariile de risc
- 6.2. Evaluarea riscului si selectia masurilor de securitate
- 6.3. Planul de tratare a riscului

7. ANEXE

N/A

VIMERCATI EAST EUROPE SRL	METODOLOGIA DE EVALUARE SI TRATARE A RISCURILOR LA ADRESA DATELOR CU CARACTER PERSONAL	Pagina 9 din 9
	Cod document: POL-GDPR-01	Versiunea 1.0

ACTUALIZARI

Nr. Crt.	Sinteza actualizarii	Versiunea curenta	Data