Rector,
Conf. univ. dr. Ramona Flavia Rațiu

PROCEDURA OPERAȚIONALĂ
privind respectarea conceptului Privacy by Design / By default conform art. 25 din GDPR
Cod: PO-DPO-05
Ediția [I], Revizia [0], Data 01.10.2024

Avizat,
Prorector Managementul Calității și Proiecte
Conf. univ. dr. Bălan Sorina Mihaela

Elaborat,
Responsabil protecția datelor
AMPLUSNET S.R.L.

1. Scopul procedurii

Având în vedere preocuparea ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ*** (***„Instituției"***) pentru respectarea legislației, în general, și a normelor destinate să protejeze datele cu caracter personal și viața privată a persoanelor fizice, în special, se impune adoptarea acestei proceduri („**Procedura**") care să guverneze respectarea prevederilor art. 25 din GDPR privitor la asigurarea protecției datelor începând cu momentul conceperii și în mod implicit (Privacy by Design / by Default). în cazul activităților de prelucrare desfășurate în cadrul **UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ.**

1.1. Cadrul Legal

Începând cu data de 25 mai 2018, principalul act normativ aplicabil la nivelul întregii Uniuni Europene este Regulamentul (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 abrogare a Directivei 95/46/CE, cunoscut și sub denumirea Regulamentul general privind protecția datelor („GDPR" sau „Regulamentul").

Astfel, conform articolul 25 din Regulament, *(1) Având în vedere stadiul actual al tehnologiei, costurile implementării, și natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și riscurile cu grade diferite de probabilitate și gravitate pentru drepturile și libertățile persoanelor fizice pe care le prezintă prelucrarea, operatorul, atât în momentul stabilirii mijloacelor de prelucrare, cât și în cel al prelucrării în sine, pune în aplicare măsuri tehnice și organizatorice adecvate, cum ar fi pseudonimizarea, care sunt destinate să pună în aplicare în mod eficient principiile de protecție a datelor, precum reducerea la minimum a datelor, și să integreze garanțiile necesare în cadrul prelucrării, pentru a îndeplini cerințele prezentului regulament și a proteja drepturile persoanelor vizate.*
(2) Operatorul pune în aplicare 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. Respectiva obligație se aplică volumului de date colectate, gradului de prelucrare a acestora, perioadei lor de stocare și accesibilității lor. În special, astfel de măsuri asigură că, în mod implicit, datele cu caracter personal nu pot fi accesate, fără intervenția persoanei, de un număr nelimitat de persoane.
(3) Un mecanism de certificare aprobat în conformitate cu articolul 42 poate fi utilizat drept element care să demonstreze îndeplinirea cerințelor prevăzute la alineatele (1) și (2) ale prezentului articol."

Orientările nr. 4/2019 privind articolul 25 Asigurarea protecției datelor începând cu momentul conceperii și în mod implicit

2. Domeniul de aplicare

2.1. Domeniul material de aplicare

Procedura se aplică tuturor activităților de prelucrare a datelor cu caracter personal ce sunt desfășurate în cadrul ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ*** sau sub controlul direct sau asociat al acesteia atunci când activitatea este susceptibilă să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice.

2.2. Obligația fundamentală constă în punerea în aplicare a măsurilor adecvate și a garanțiilor necesare care să asigure respectarea efectivă a principiilor de protecție a datelor și, prin urmare, a drepturilor și libertăților persoanelor vizate începând cu momentul conceperii și în mod implicit. Articolul 25 stabilește atât elementele legate de concepere, cât și de protecția implicită care trebuie luate în considerare. Elementele respective vor fi aprofundate în cadrul acestor orientări.

2.3. Articolul 25 alineatul (1) stipulează că, atunci când planifică o nouă operațiune de prelucrare, operatorii trebuie să ia în considerare DPbDD într-o fază incipientă. Operatorii trebuie să pună în aplicare DPbDD înainte de prelucrare și în permanență la momentul prelucrării, revizuind regulat eficacitatea măsurilor și a garanțiilor selectate. DPbDD se aplică și sistemelor existente care prelucrează date cu caracter personal.

3. Documente de referință

Au fost analizate:

- Regulamentul (UE) 679/2016 al Parlamentului European și al Consiliului („GDPR" sau „Regulamentul")
- Legea nr. 190/2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului
- Politica ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ*** privind Protecția Datelor

Totodată, în vederea redactării Procedurii au fost analizat Ghidurile și Opiniile emise de Comitetul European pentru Protecția Datelor.

4. Definiții și abrevieri

4.1. Definiții ale termenilor

Nr. crt.	Termenul	Definiția și/sau, dacă este cazul, actul care definește termenul
1.	Regulamentul	Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului
2.	Date cu caracter personal	Înseamnă orice informații privind o persoană fizică identificată sau identificabilă ("persoana vizată")
3.	Prelucrare	înseamnă 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

4.2. Abrevieri ale termenilor

Nr. crt.	Abrevierea	Termenul abreviat
1.	GDPR	Regulamentul (UE) 2016/679 al Parlamentului European şi al Consiliului
2.	DPO	Responsabil cu Protecția Datelor
3	DPbDD	Privacy by Design / By default – Asigurarea protecției începând cu momentul conceperii şi în mod implicit.

5. Descrierea procedurii

5.1. DPbDD este o cerință aplicabilă în egală măsură tuturor operatorilor, inclusiv întreprinderilor mici şi companiilor multinaționale sau instituțiilor publice. Acestea fiind spuse, nivelul de complexitate asociat punerii în aplicare a DPbDD poate varia în funcție de fiecare operațiune de prelucrare în parte. În toate cazurile însă, indiferent de dimensiune, punerea în aplicare a DPbDD este benefică atât pentru operator, cât şi pentru persoana vizată.

5.2. Identificarea necesității efectuării unei evaluări a impactului

Anterior demarării oricărei activități de prelucrarea a datelor se impune consultarea Responsabilului cu protecția datelor desemnat în cadrul ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ*** privind prevederile art. 25 din GDPR şi are legislației conexe.

Responsabilul cu protecția datelor („**DPO**") va evalua dacă activitatea de prelucrare descrisă se încadrează în rândul activităților care se impun a fi evaluate sub aspectul prevederilor art. 25 din GDPR.

5.3. Analizarea activității de prelucrare a datelor cu caracter personal ce urmează a fi desfăşurată

Persoana responsabilă de activitatea de prelucrarea a datelor va întocmi o prezentare ce va include cel puțin:

- scurtă descriere a activității de prelucrare a datelor, descriere ce trebuie să includă:
  - persoanele vizate de activitatea de prelucrare;
  - scopul activității;
  - durata de stocare a datelor colectate;
  - categoriile de date ce vor fi colectate;
  - mijloacele de prelucrare utilizate;
  - teritoriul vizat;
  - destinatarii datelor cu caracter personal;
  - măsurilor tehnice şi organizatorice avute în vedere pentru protejarea datelor.
- identificarea operatorului de date precum şi, dacă este cazul, a operatorilor asociați şi a persoanele împuternicite

5.4. Studierea principiilor fundamentale

5.4.1. Identificarea măsurilor adecvate prin raportare la scopul urmărit

Responsabilul cu protecția datelor împreună cu persoana responsabilă de activitatea de prelucrare vor argumenta măsurile implementate prin raportare la cerințele impuse de art. 5 din Regulament dar și a principiilor consacrate specifice art. 25, și anume:

- **Proactiv, nu Reactiv; Preventiv nu Remedial;**
- **Confidențialitate ca setare implicită;**
- **Confidențialitate încorporată în design;**
- **Funcționalitate completă: sumă pozitivă, nu sumă zero;**
- **Securitate end-to-end: protecție completă a ciclului de viață;**
- **Vizibilitate și transparență: mențineți-l deschis;**
- **Respectarea confidențialității utilizatorului: păstrați-l centrat pe utilizator.**

5.4.2. **Responsabilul cu protecția datelor analizează modul** în care fiecare cerință este planificată, clarificată și justificată pentru a fi în conformitate cu Regulamentul. Totodată, Responsabilul cu protecția datelor va semnala dacă anumite cerințe nu sunt îndeplinite sau dacă măsurile implementate nu sunt suficiente. Dacă este cazul, revizuiește descrierea acestora sau propune măsuri suplimentare.

5.5. **Elementele care trebuie luate în considerare** pentru protecția drepturilor persoanelor vizate.

Articolul 25 alineatul (1) enumeră elementele pe care operatorul trebuie să le ia în considerare atunci când determină măsurile unei operațiuni de prelucrare specifice. În cele ce urmează, vă vom oferi orientări cu privire la modul de aplicare al acestor elemente în procesul de concepere, care include conceperea setărilor implicite. Toate aceste elemente contribuie la stabilirea adecvării sau a inadecvării unei măsuri pentru punerea în aplicare eficace a principiilor. Prin urmare, fiecare dintre aceste elemente reprezintă nu un obiectiv propriu-zis, ci un factor care trebuie avut în vedere pentru realizarea obiectivului:

5.5.1. **„stadiul actual al dezvoltării"/„stadiul actual al tehnologiei"** - să țină cont de progresul actual al tehnologiei care este disponibilă pe piață. Aceasta cerință prevede ca operatorii să cunoască și să se mențină la curent cu progresele tehnologice, cu modul în care tehnologia poate prezenta riscuri sau oportunități în ceea ce privește protecția datelor pentru operațiunea de prelucrare, precum și cu privire la modul de punere în aplicare și actualizare a măsurilor și a garanțiilor care asigură punerea în aplicare eficace a principiilor și a drepturilor persoanelor vizate având în vedere peisajul tehnologic în continuă evoluție.

5.5.2. **„costurile implementării"** - ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ*** poate să țină seama de costurile implementării la alegerea și aplicarea măsurilor tehnice și organizatorice adecvate și a garanțiilor necesare pentru punerea în aplicare eficace a principiilor menite să protejeze drepturile persoanelor vizate. Aceste costuri se referă la resurse în general, inclusiv la resursele de timp și la cele umane. Elementul de cost nu impune operatorului să cheltuie o sumă disproporționată de resurse atunci când există măsuri alternative, mai puțin costisitoare dar eficace. Costurile implementării reprezintă un factor care trebuie avut în vedere la realizarea protecției datelor începând cu momentul conceperii, nu un motiv pentru care să nu realizeze

protecția.

5.5.3. **„natura, domeniul de aplicare, contextul și scopurile prelucrării"** - Pe scurt, conceptul de natură poate fi înțeles drept caracteristicile inerente ale prelucrării. Domeniul de aplicare se referă la dimensiunea și la gama activităților de prelucrare. Contextul se referă la circumstanțele prelucrării, care pot influența așteptările persoanei vizate, în timp ce scopurile se referă la obiectivele prelucrării.

5.5.4. **„riscurile cu grade diferite de probabilitate și gravitate pentru drepturile și libertățile persoanelor fizice pe care le prezintă prelucrarea"** - La efectuarea unei analize a riscurilor în vederea respectării articolului 25, operatorul trebuie să identifice riscurile pe care le presupune o încălcare a principiilor pentru drepturile persoanelor vizate și să stabilească probabilitatea și severitatea riscurilor identificate, pentru a pune în aplicare măsuri care să le reducă în mod eficace. Atunci când se efectuează evaluări ale riscurilor, o evaluare sistematică și aprofundată a prelucrării este crucială.

5.6. **Factorul de timp**

5.7. **„Momentul stabilirii mijloacelor de prelucrare"** se referă la intervalul de timp în care operatorul decide modul în care se va realiza prelucrarea și maniera în care va avea loc aceasta, precum și mecanismele care vor fi utilizate pentru efectuarea prelucrării respective. În cadrul acestui proces decizional, operatorul trebuie să evalueze măsurile și garanțiile adecvate în vederea punerii în aplicare în mod eficace a principiilor și a drepturilor persoanelor vizate în cadrul prelucrării, precum și să țină cont de elemente precum stadiul actual al tehnologiei, costurile implementării, natura, domeniul de aplicare, contextul și scopurile, precum și de riscuri. Tot aici se încadrează și momentul de achiziționare și implementare a programelor software, a hardware-ului și a serviciilor de prelucrare a datelor.

5.8. Odată ce a fost inițiată prelucrarea, operatorul are în permanență **obligația de a menține DPbDD,** adică de a pune în aplicare constant și în mod eficace principiile pentru a proteja drepturile, de a fi la curent cu stadiul actual al tehnologiei, de a reevalua nivelul de risc etc. Natura, domeniul de aplicare și contextul operațiunilor de prelucrare, precum și riscul, pot suferi modificări în timpul prelucrării, ceea ce înseamnă că operatorul trebuie să-și reevalueze operațiunile de prelucrare prin revizuiri și evaluări periodice ale eficacității măsurilor și garanțiilor alese.

5.9. **În mod implicit, se prelucrează numai datele cu caracter personal care sunt necesare fiecărui scop specific al prelucrării** - Termenul „în mod implicit" în cazul prelucrării datelor cu caracter personal se referă la alegerea valorilor de configurare sau a opțiunilor de prelucrare fixe sau prescrise într-un sistem de prelucrare, cum ar fi o aplicație software, un serviciu ori un dispozitiv, sau într-o procedură manuală de prelucrare și care afectează volumul de date cu caracter personal colectate, măsura în care sunt prelucrate, perioada de stocare și accesibilitatea acestora.

5.10. <u>Validarea mecanismelor instituite ca urmare a analizei DPbDD</u>

Persoana responabilă de activitatea de prelucrare împreună cu Responsabilul cu protecția datelor colectează și sistematizează informațiile privind activitatea de prelucrare pentru ca mai apoi să întocmească Raportului de conformitate la prevederile art. 25, Raport ce trebuie să conțină:

- măsurile selectate pentru a asigura respectarea principiilor fundamentale;
- măsurilor selectate pentru a asigura securitatea datelor, în funcţie de respectarea celor mai bune practici de securitate;
- riscurile în funcţie de gravitatea şi probabilitatea lor;
- un plan de acţiuni bazat pe măsurile suplimentare identificate în etapele anterioare; pentru fiecare măsură se va indica cel puţin persoana responsabilă de implementarea acesteia şi timpul estimat;
- avizul Responsabilului de protecţia datelor (conform articolului 35 alineatul (2) din GDPR); punctul de vedere al persoanelor vizate sau al reprezentanţilor acestora, dacă este cazul (articolul 35 alineatul (9) din GDPR).

5.10.1. Obținerea unui aviz consultativ din partea Autorității naționale de supraveghere

În cazul în care evaluarea impactului asupra protecţiei datelor indică faptul că prelucrarea ar genera un risc ridicat în absenţa unor măsuri luate de operator pentru atenuarea riscului, înainte de începerea prelucrării, Responsabilul cu protecţia datelor va iniţia demersurile pentru consultarea Autorității naționale de supraveghere.

5.11. **Demararea activității de prelucrare a datelor**

Conducerea ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ*** care urmează să deruleze prelucrarea decide dacă măsurile stabilite, riscurile reziduale şi planul de acţiune sunt acceptabile, cu justificări, ţinând seama de beneficiile şi punctele de vedere identificate anterior.

Conducerea ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ*** care urmează să deruleze prelucrarea poate decide după cum urmează:

I. Validarea oficială a raportului de evaluare şi demararea activității de prelucrare
II. Condiționează demararea activității de prelucrare de implementarea unor măsuri suplimentare şi refacerea evaluării de impact
III. Respinge activitatea de prelucrare prin raportare la riscurile generate.

6. Responsabilităţi în derularea activităţii

- Conducerea ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ*** care urmează să deruleze activitatea de prelucrarea va analiza raportul şi va lua o decizie privind demararea lucrărilor
- Responsabil cu protecţia datelor va realizează evaluarea specifică privind protecţia datelor împreună cu persoana responsabilă de activitatea de prelucrare, va aviza Raportul de conformitate cu art. 25 şi dacă este cazul va consulta Autoritatea națională de supraveghere.
- Persoana responsabilă de activitatea de prelucrare va asista Responsabilul cu protecţia datelor pe tot parcursul Procedurii.

7. Formular evidenţă modificări

Nr. crt.	Ediţia	Data ediţiei	Revizia	Data reviziei	Nr. pag.	Descriere modificare	Semnătura conducătorului compartimentului
1	2	4	5	6	7	8	9
1.	I		0	-	18	-Elaborare conf. Regulamentului UE679/2016 - Consultare ghiduri EDPB	
2.							
3.							
4.							
5.							

8. Formular analiză procedură

Nr. crt.	Departament	Nume şi prenume conducător departament	Înlocuitor de drept sau delegat	Aviz favorabil		Aviz nefavorabil		
				Semnătura	Data	Obs.	Semnătura	Data
1	2	3	4	5	6	7	8	9
1								
2								
3								
4								
5								

9. Lista de distribuire a procedurii

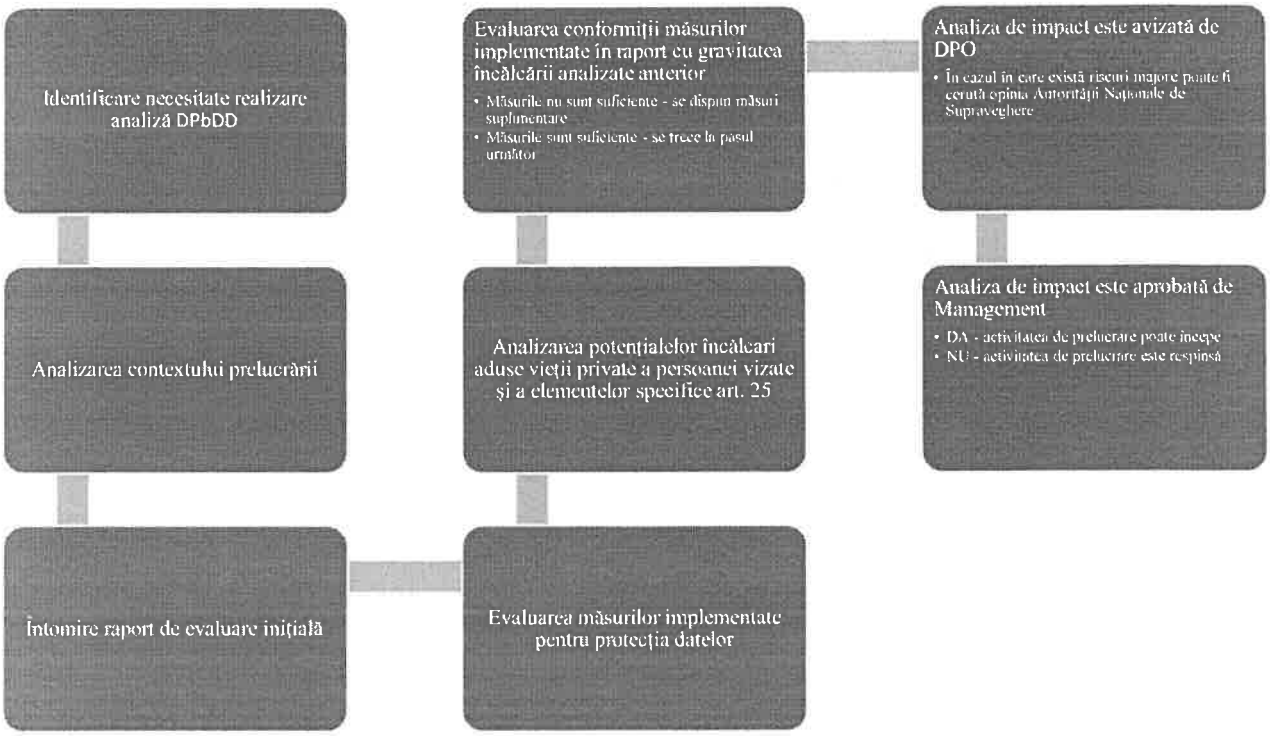
Nr. ex.	Compartiment	Nume şi prenume	Data primirii procedurii	Semnătura	Data retragerii procedurii	Semnătura
1	2	3	4	5	6	7
1 copie						
1 copie						
1 copie						
1 copie						
1 copie						
1 copie						
1 copie						
1 copie						
1 copie						
1 copie						

10. Anexe

10.1. **Anexa 1 - Diagrama de proces pentru realizarea procedurii operaționale**

10.2. **Anexa 2 – Model de Raport de conformitate la art. 25**

Anexa nr. 1
Diagrama de proces pentru realizarea procedurii operaționale


Identificare necesitate realizare analiză DPbDD
Analizarea contextului prelucrării
Întocmire raport de evaluare inițială
Evaluarea măsurilor implementate pentru protecția datelor
Analizarea potențialelor încălcări aduse vieții private a persoanei vizate și a elementelor specifice art. 25
Evaluarea conformității măsurilor implementate în raport cu gravitatea încălcării analizate anterior
• Măsurile nu sunt suficiente - se dispun măsuri suplimentare
• Măsurile sunt suficiente - se trece la pasul următor
Analiza de impact este avizată de DPO
• În cazul în care există riscuri majore poate fi cerută opinia Autorității Naționale de Supraveghere
Analiza de impact este aprobată de Management
• DA - activitatea de prelucrare poate începe
• NU - activitatea de prelucrare este respinsă

Anexa nr. 2

Model de Raportul de conformitate la prevederile art. 25

1. Descrierea activității de prelucrate şi identificarea persoanelor vizate.
2. Identificare prelucrări
   - **2.1.** Scopul prelucrărilor identificate
   - **2.2.** Descriere prelucrări
   - **2.3.** Prelucrări identificate
3. Analizarea prelucrării prin raportare la:
   - **3.1.** Legi, standarde şi regulamente pe care se bazează prelucrările
   - **3.2.** Structuri pe care au loc prelucrările
   - **3.3.** Organizații implicate în prelucrări

Tip prelucrare	Părți implicate în prelucrare

3.4. Transfer internațional de date

Tip transfer	Organizaţie către care se face transferul internaţional de date de natură personală

3.5. Documente utilizate

3.5.1. Categoriile de date cu caracter personal ce vor fi prelucrate

3.6. Active utilizate în prelucrarea datelor

Active	Descriere

4. Proporționalitate şi necesitate

4.1. Scopurile prelucrărilor sunt specificate, explicite şi legitime?

4.2. Temeiurile juridice care fac ca prelucrarea să fie legală (GDPR)?

Baza legală pentru prelucrarea datelor personale (Art.6)	Criteriu de prelucrare categorii speciale de date de natură personală(Art.9)

4.3. Datele colectate sunt adecvate, relevante şi limitate la ceea ce este necesar în raport cu scopurile pentru care sunt prelucrate ("minimizarea datelor")?

4.4. Datele sunt corecte şi actualizate?

4.5. Care este metoda şi durata de stocare a documentelor?

Modul de stocare a documentelor	Locaţie de stocare	Durata de stocare

5. Protecţia drepturilor persoanelor vizate
5.1. Cum sunt informate persoanele vizate cu privire la prelucrare?
5.2. Cum se obţine consimţământul persoanelor vizate?
5.3. Cum pot persoanele vizate să-şi exercite dreptul de acces?
5.4. Cum pot persoanele vizate să-şi exercite dreptul de portabilitate a datelor?
5.5. Cum pot persoanele vizate să îşi exercite dreptul la rectificare?
5.6. Cum pot persoanele vizate să îşi exercite dreptul de ştergere?
6. Măsuri existente
6.1. Menţionaţi măsurile de securitate tehnice şi organizatorice existente

Menţionaţi măsurile de securitate tehnice şi organizatorice / controalele existente sau avute în vedere (dacă se aplică)	Descriere

7. Identificarea evenimentelor nedorite
7.1. Care sunt evenimentele nedorite identificate?

Care sunt evenimentele nedorite identificate?	Descriere

8. Analiza riscurilor
8.1. Care ar putea fi impactul principal asupra persoanelor vizate în cazul apariţiei evenimentului?

Evenimente	Impact

8.2. Care sunt principalele ameninţări care ar putea duce la apariţia evenimentului?

Evenimente	Ameninţare

8.3. Surse de risc

Evenimente	Surse de risc

8.4. Care dintre controalele/măsurile existente contribuie la tratarea riscului?

Evenimente	Controale / Măsuri existente

8.5. Cum estimaţi severitatea riscului în funcţie de impactul potenţial şi de controalele existente? Cum estimaţi probabilitatea riscului, în special în ceea ce priveşte ameninţările, sursele de risc şi controalele existente?

Evenimente	Nivel impact / probabilitate

8.6. Care din controalele/masurile planificate contribuie la tratarea riscului identificat?

Evenimente	Controale / Masuri existente

8.7. Cum estimaţi severitatea riscului în funcţie de impactul potenţial şi de măsurile planificate? Cum estimaţi probabilitatea riscului, în special în ceea ce priveşte ameninţările, sursele de risc şi controaiele/măsurile planificate?

Evenimente	Nivel impact / probabilitate

9. Elemente specifice art. 25

Nr.crt.	CRITERIU	RĂSPUNS / DA 10 / NU 0 / Parţial 5	SCOR
	Asigurarea transparenței		
1	Claritatea - Informațiile sunt formulate într-un limbaj clar şi simplu, concis şi inteligibil.		
2	Semantica - Comunicarea trebuie să aibă un sens clar pentru publicul în cauză.		
3	Accesibilitatea - Informațiile sunt uşor accesibile pentru persoana vizată.		
4	Contextualitatea - Informațiile se furnizează în momentul relevant şi în forma corespunzătoare.		
5	Relevanța - Informațiile trebuie să fie relevante şi aplicabile respectivei persoane vizate.		

6	Proiectarea universală - Informațiile sunt accesibile tuturor persoanelor vizate, inclusiv prin utilizarea limbajelor citibile automat pentru a facilita și automatiza claritatea.		
7	Nivelul de înțelegere - Persoanelor vizate trebuie să le fie suficient de clar la ce se pot aștepta în ceea ce privește prelucrarea datelor lor cu caracter personal, în special atunci când persoanele vizate sunt copii sau alte grupuri vulnerabile.		
8	Canale multiple - Informațiile trebuie să fie furnizate pe canale și prin mijloace diferite, nu numai sub formă textuală, pentru a spori probabilitatea ca informațiile să ajungă efectiv la persoana vizată.		
9	Mai multe niveluri – Informațiile trebuie structurate într-un mod care să soluționeze tensiunea dintre caracterul complet și înțelegere, ținând cont totodată de așteptările rezonabile ale persoanelor vizate.		
	Instruirea persoanelor cu atribuții specifice		
10	Instruiri specifice cu toți angajații care prelucrează date prin noua activitate propusă		
	Stabilirea cerințelor		
11	Cerințele se axează pe cerințele necesare pentru produsul final		
12	Există cerințe privind protecția datelor + Cerințe pentru securitatea informațiilor		
13	Se respectă principiile de bază ale protecției datelor: legalitate, transparență, minimizare etc.		
14	Au fost definite nivelurile de toleranță la risc		

15	Au fost evaluate riscurile de securitate		
16	S-a realizat evaluarea impactului asupra protecției datelor (DPIA)		
17	Produsul facilitează exercitarea drepturilor: informare/acces/rectificare etc.		
	Design		
18	Minimizare și limitare: Cantitatea de date cu caracter personal colectate și prelucrate trebuie limitată la ceea ce este legal și strict necesar. "Selectați înainte de a colecta".		
19	Ascundere și protejare: Datele cu caracter personal și interrelațiile dintre acestea nu ar trebui să fie comunicate, prelucrate sau stocate la vedere. Printre exemple se numără pseudonimizarea, criptarea și agregarea datelor cu caracter personal.		
20	Separare: Prin separarea prelucrării sau stocării mai multor surse de date cu caracter personal care aparțin aceleiași persoane, se reduce posibilitatea de a crea profiluri complete ale unei singure persoane		
21	Protecția datelor în mod implicit: Toate setările ar trebui să fie configurate, în mod implicit, la cea mai favorabilă confidențialitate.		
22	Informare: Software-ul ar trebui să fie proiectat și configurat astfel încât persoana vizată să fie suficient de informată cu privire la modul de funcționare a softwareuluișila modulîn care suntprelucrate datele cu caracter personal.		
23	Control: Persoana vizată are dreptul de a-șicontrola propriile date cucaracter personal. Aceasta include dreptul de a accesa, actualiza și/sau șterge propriile date		

24	Demonstrare: Operatorul trebuie să fie capabil să documenteze conformitatea cu regulamentul privind protecția datelor și securitatea prelucrării.		
25	Aplicare: Software-ul ar trebui să fie conceput astfel încât să faciliteze documentarea modului în care protejează drepturile persoanei vizate. Documentația ar trebui să acopere responsabilitatea și modul în care este aplicat regulamentul privind protecția datelor.		
26	Agregare: Pentru a garanta protecția drepturilor persoanei vizate, datele cu caracter personal trebuie colectate și prelucrate cu cât mai multă agregare posibil		
	Codarea		
27	Se utilizează instrumente și framework-uri aprobate		
28	Există mecanisme de analiză statică a codului și revizuirea codului		
29	Sunt avute în vedere reducerea oportunităților de exploatare a vulnerabilităților		
	Testarea		
30	Se testează dacă au fost puse în aplicare cerințele privind protecția și securitatea datelor		
31	Se realizează testarea securității		
32	Se realizează testarea dinamică Cross-site scripting și SQL injection.		
33	Se testează gestionarea sesiunilor, utilizarea cookieurilor și controlul accesului		
34	Testarea Fuzz (declanșarea intenționată a unor erori în software) e avută în vedere		

35	Se realizează teste de penetrare/analiză de vulnerabilitate – intern + extern		
	Lansarea		
36	S-a avut în vedere din timp planificarea modului în care organizația poate gestiona incidentele după lansare, precum și procedurile de actualizare a software-ului.		
37	S-a avut în vedere înainte de lansare efectuarea unei analize complete și finale asupra securității datelor		
38	Există un plan de răspuns la incidente aprobat		
	Mentenanța		
39	Se respectă întru totul pașii procedurați în planul de răspuns la incidente		
40	Se realizează întreținerea, service-ul și operarea software-ului		
41	Se testează periodic securitatea datelor, analiza vulnerabilităților, a rezistenței infrastructurii și rețelei		
42	Se urmează procedurile de răspuns la cererile persoanelor vizate		
Punctajul recomandat este de minim 300 puncte pentru a putea constata un nivel ridicat de conformitate la prevederile art. 25 - Privacy by design / by default.		**Total**	**0**
		Minim: 0	
		Mediu: 210	
		Maxim: 420	

10. Concluzii și recomandări
10.1. Concluzii
10.2. Recomandări
11. Persoane interesate
10.1. Persoana care validează Raportul
10.2. Persoana care aproba Activitatea de prelucrare