Rector,
Conf. univ. dr. Ramona Flavia Ratiu

PROCEDURA OPERAȚIONALĂ *privind notificarea incidentelor de securitate*
Cod: PO-DPO-14
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.

Pagina de gardă 1
Cuprins 2
1. Scopul procedurii 3
2. Domeniul de aplicare al procedurii 3
3. Documente de referință 3
4. Definiții și abrevieri 4
5. Descrierea procedurii 4
6. Responsabilități în desfășurarea procedurii 6
7. Formular evidență modificări 7
8. Formular analiză procedură 7
9. Lista de distribuire a procedurii 7
10. Anexe 8
10.1. Diagrama de proces pentru realizarea procedurii operaționale 8
10.2. Model de informare al persoanelor vizate 9
10.3. Raport privind clasificarea incidentului de securitate 10

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 reglementeze modul de lucru aplicat în ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ*** pentru a răspunde cerințelor articolelor 33 și 34 din Regulamentul (UE) 679/2016, privind notificarea autorității de supraveghere, respectiv informarea persoanelor vizate afectate, în cazul unei încălcări a securității datelor cu caracter personal.

1.1. Cadru 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").

2. Domeniul de aplicare al procedurii

Procedura se aplică pentru orice tip de incident de securitate care are ca rezultat o încălcare a securității datelor cu caracter personal, în următoarele situații:

- datele cu caracter personal se referă la persoane rezidente în Uniunea Europene (UE) și Spațiul Economic European (SEE), indiferent de locul în care aceste date sunt supuse prelucrării;
- datele cu caracter personal sunt supuse prelucrării în UE și / sau în SEE, indiferent de țara de rezidență a persoanei vizate.

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. Definiţii 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 informaţii privind o persoană fizică identificată sau identificabilă ("persoana vizată")
3.	Prelucrare	înseamnă 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, cum ar fi colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, divulgarea prin transmitere, diseminarea sau punerea la dispoziţie în orice alt mod, alinierea sau combinarea, restricţionarea, ştergerea 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

5. Descrierea Procedurii

5.1. Identificarea incidentului de securitate şi a riscurilor cauzate de acesta

În cazul identificării unui incident de securitate este necesară realizarea unei evaluări privind riscurilor pentru drepturile şi libertăţile persoanelor vizate. În funcţie de tipul incidentului identificat, se va desemna o echipă de răspuns care va fi implicată în realizarea evaluării.

Echipa de răspuns la incident va fi constituită exclusiv din:

- Responsabilul cu protecţia datelor;
- Structura organizatorică deţinătoare a informaţiilor;
- Persoana responsabilă de activitatea de prelucrare;
- Departamentul direct implicat în generarea incidentului;
- Secretariatul sau alte departamente relevante.

Le momentul analizării riscurilor generate de incidentul de securitate se va ține seama de următorii factori:

- tipul de incident (încălcarea confidenţialităţii, încălcarea integrităţii, încălcarea disponibilităţii)
- uşurinţa cu care pot fi identificate persoanele fizice afectate;
- gravitatea consecinţelor asupra persoanelor;

- caracteristicile speciale ale persoanelor (copii sau alte persoane vulnerabile);
- dacă datele personale au fost criptate şi dacă da, gradul de complexitate al criptării utilizate;
- măsura în care datele au fost pseudonimizate;
- tipurile de date afectate (de exemplu numele, adresa, date privind sănătatea etc.);
- volumul de date afectate;
- numărul persoanelor vizate afectate.

Metoda de evaluare a riscurilor, raţionamentul şi concluziile vor fi documentate într-**un Raport privind clasificarea incidentului de securitate** (Anexa nr. 2), întocmit de Responsabilul cu protecţia datelor.

5.2. Deciziile referitoare la notificare şi informare

Dacă concluziile evaluării indică un risc pentru drepturile şi libertăţile persoanelor vizate afectate de încălcare, Responsabilul cu protecţia datelor **va recomanda Managementului notificarea autorităţii de supraveghere**.

Dacă concluziile evaluării indică un risc ridicat pentru drepturile şi libertăţile persoanelor vizate afectate de încălcare. **Responsabilul cu protecţia datelor va recomanda Managementului dacă este necesară informarea** (Anexa nr. 1) persoanelor vizate afectate.

Informarea nu este necesară dacă:

I. în cazul datelor cu caracter personal afectate a fost aplicată criptarea sau alte măsuri de protecţie tehnice şi organizatorice prin care se asigură că datele devin neinteligibile oricărei persoane care nu este autorizată să le acceseze,
II. acţiunile deja întreprinse sau planificate pentru soluţionarea incidentului sunt considerate suficiente pentru diminuarea riscului pentru drepturile şi libertăţile persoanelor vizate şi acesta nu mai este susceptibil să se materializeze,
III. ar necesita un efort disproporţionat.

Deciziile vor fi documentate în Raportul clasificare incident, întocmit de Responsabilul cu protecţia datelor. Rezultatul evaluării riscului va cuprinde una dintre următoarele decizii:

I. încălcarea datelor cu caracter personal nu necesită notificare,
II. încălcarea datelor cu caracter personal necesită numai notificarea autorităţii de supraveghere,
III. încălcarea datelor cu caracter personal necesită notificarea autorităţii de supraveghere şi informarea persoanelor vizate.

Decizia de a informa sau nu persoana vizată se poate modifica pe baza răspunsului autorităţii de supraveghere şi a altor informaţii care sunt descoperite pe parcursul investigaţiei încălcării.

5.3. Notificarea autorităţii de supraveghere

În cazul în care ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREŞ*** este operatorul datelor cu caracter personal afectate de incident, Responsabilul cu protecţia datelor va întreprinde acţiunile necesare pentru notificarea autorităţii de supraveghere. Datele de contact ale Autorităţii de supraveghere din România sunt:

Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal

B-dul G-ral Gheorghe Magheru 28-30, Sector 1, cod poştal 010336, Bucureşti, România
Tel: 031 805 92 11,031 805 92 12
Fax: 031 805 96 02
E-mail: anspdcp@dataprotection.ro
www.dataprotection.ro
Notificarea autorităţii de supraveghere se va face fară întârzieri nejustificate şi, dacă este posibil, în cel mult 72 de ore de la confirmarea incidentului. In cazul în care există motive întemeiate pentru depăşirea acestui termen, aceste motive trebuie furnizate ca parte a notificării.
Notificarea va fi transmisă ANSPDCP utilizând formularul disponibil pe site-ul autorităţii www.dataprotection.ro (Formular Breşă RGPD).

Următoarele informaţii trebuie furnizate ca parte a notificării:

- natura încălcării datelor cu caracter personal, inclusiv, dacă este posibil:
  - categoriile şi numărul aproximativ al persoanelor vizate,
  - categoriile şi numărul aproximativ de date cu caracter personal afectate,
- numele şi datele de contact ale responsabilului cu protecţia datelor sau ale altui punct de contact unde pot fi obţinute mai multe informaţii,
- o descriere a consecinţelor probabile ale încălcării datelor cu caracter personal,
- o descriere a măsurilor luate sau propuse a fi luate pentru a aborda încălcarea datelor cu caracter personal, inclusiv, dacă este cazul, măsuri de atenuare a posibilelor sale efecte adverse,
- în cazul în care notificarea nu a fost trimisă în termenul de 72 de ore, motivele întârzierii.

Dacă este necesar, informaţiile vor putea fi furnizate în etape, fără întârzieri nejustificate.
Responsabilul cu protecţia datelor ar trebui să obţină o confirmare scrisă din partea autorităţii de supraveghere că a fost primită notificarea, inclusiv data şi ora la care a fost primită.

5.4. Informarea persoanelor vizate

Odată ce s-a hotărât de către Management că se justifică informarea persoanelor vizate afectate, Responsabilul cu protecţia datelor va întreprinde acţiunile necesare pentru a comunica acestora, fără întârzieri nejustificate, încălcarea securităţii datelor lor cu caracter personal. Comunicarea se va face personal, prin e-mail sau poştă, folosind modelul de Informare persoană vizată (a se vedea Anexa 10.2).
Deşi nu este obligatorie informarea persoanelor vizate afectate în cazul în care ar implica eforturi disproporţionate, Responsabilul cu protecţia datelor trebuie să ia in considerare în acest caz o formă de comunicare publică.
Informaţiile referitoare la informarea persoanelor vizate afectate vor fi înregistrate în Registru incidente.

6. Responsabilităţi în urmarea Procedurii

Responsabilul cu protecţia datelor trebuie să:

- evalueaze, împreună cu echipa de răspuns la incident, riscurile încălcării securităţii datelor pentru drepturile şi libertăţile persoanelor vizate,
- elaboreze recomandări către Management cu privire la notificarea sau nu a autorităţii de supraveghere şi a persoanelor vizate,

- întreprindă acţiunile necesare pentru notificarea autorităţii de supraveghere şi informarea persoanelor vizate atunci când se decide şi se impune acest lucru.

7. Formular evidenţă modificări

Nr. crt.	Ediția	Data ediției	Revizia	Data reviziei	Nr. pag.	Descriere modificare	Semnătura conducătorului compartimentului
1	2	4	5	6	7	8	9
1	I		0	-	15	-Elaborare conf. Regulamentului UE679/2016 şi a ghidurilor emise de EDPB -Elaborare conform OSGG 600/2018	
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								

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

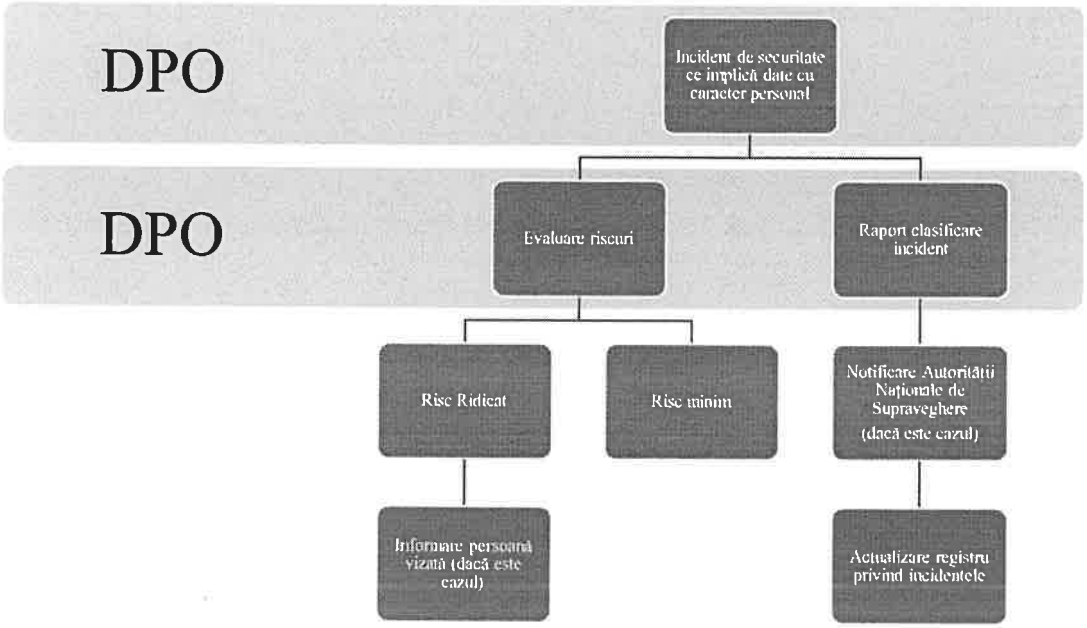
1 copie						
1 copie						
1 copie						
1 copie						
1 copie						
1 copie						
1 copie						
1 copie						
1 copie						
1 copie						

10. Anexe

10.1. Diagrama de proces pentru realizarea procedurii operaționale
10.2. Model de informare al persoanelor vizate
10.3. Raport privind clasificarea incidentului de securitate

10.1

Diagrama de proces pentru realizarea procedurii operaționale



10.2

Model de informare al persoanelor vizate

Stimată doamnă / Stimate domn,

Dorim să vă asigurăm că ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ*** depune toate eforturile pentru a proteja datele cu caracter personal pe care le colectăm şi le folosim şi, în cea mai mare parte, reuşim să facem acest lucru.

Cu toate acestea, considerăm că trebuie să vă informăm cu privire la un incident recent despre care credem că ar fi putut afecta datele cu caracter personal pe care le deţinem referitoare la dumneavoastră.

La data de **[...]** am identificat că **[...]** (scurtă descriere a evenimentului). Ca rezultat al acestui incident, credem că datele cu caracter personal referitoare la dumneavoastră, inclusiv **(enumeraţi categoriile de date cu caracter personal afectate)** au fost **(furate, accesate, modificate sau pierdute).**

Acest lucru poate duce la un risc crescut pentru dumneavoastră care poate avea ca posibile consecinţe **[...] (descriere a posibilelor consecinţe asupra persoanei vizate)**.

În momentul identificării incidentului am pornit o investigaţie a circumstanţelor incidentului, astfel încât să putem remedia cauzele şi să prevenim repetarea acestuia. De asemenea, pentru reducerea consecinţelor incidentului am luat următoarele măsuri **[...] (descriere a măsurilor luate)** şi intenţionăm să luăm şi următoarele măsuri suplimentare **[...] (descriere a măsurilor suplimentare).**

Vă vom informa dacă descoperim informaţii noi pe care ar trebui să le cunoaşteţi. De asemenea, colaborăm cu Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal şi **[...] (numele instituţiei, după caz)** pentru a aborda incidentul dintr-o perspectivă juridică.

Pentru informaţii suplimentare despre acest incident vă rugăm să ne contactaţi la dpo@....ro , la telefon **[...]** sau să ne scrieţi la adresa: **[...]**

Cu stimă,

(nume, funcţie, semnătură)

10.3

Raport privind clasificarea incidentului de securitate

1. IDENTIFICAREA ŞI DESCRIEREA INCIDENTULUI

Cine a anunțat incidenul	Nume:	
	Departament	
	Contact:	
Data şi ora detectării:		
Unde a fost detectat incidentul:		
Descrierea incidentului:		
Data şi ora confirmării:		

2. ACȚIUNI IMEDIATE ÎNTREPRINSE

Scurtă descriere a acțiunilor:	

3. CINE A FOST ANUNȚAT DE INCIDENT

»

	IT&C		Poliția
	Furnizorul sistemului / aplicației		ISU
	Resurse umane		Parchet
	Juridic		CERT-RO
	Management		ANSPDCP
Alții (precizați mai jos)			
Detalii			

4. PERSOANE VIZATE AFECTATE

	Angajați		Furnizori		Persoane adulte vulnerabile
	Clienți		Colaboratori		Nu se cunosc încă
	Utilizatori		Copii		Altele (furnizați detalii mai jos)
Detalii					
Câte persoane ar putea fi afectate?					

5. CATEGORIILE DE DATE CU CARACTER PERSONAL IMPLICATE

	Date personale comune		**Categorii speciale de date**
	Date de identificare		Origine rasială sau etnică
	Date de contact		Opinii politice

	Identificatori online (nume utilizator, parolă etc.)		Confesiune religioasă sau convingeri fice
	Date financiare		Apartenența la sindicate
	Detalii familie		Date despre viața sexuală sau orientare lă
	Numere de identificare		
	Numere de identificare naționale		Date privind sănătatea
	Informații financiare		Date genetice sau biometrice
	Informații profesionale		Infracțiuni, condamnări, măsuri de tate
Altele (furnizați detalii mai jos)			
Detalii			

6. MĂSURI TEHNICE ŞI ORGANIZATORICE ADOPTATE PENTRU DIMINUAREA/LIMITAREA/ELIMINAREA RISCULUI

	Măsuri tehnice		**Măsuri organizatorice**
	Criptarea datelor (ex. parole)		Instruirea specifică a personalului
	Anonimizarea datelor		Adoptarea de proceduri specifice pentru evitarea incidentului
	Soluții de backup		Politica biroului curat
	Soluții de revocare a datelor comunicate în mediul online		Politici privind comunicarea în mediul online
			Politici privind securitatea informatică
Altele (furnizați detalii mai jos)			
Detalii			

7. EVALUAREA RISCURILOR

CRITERIU	**CIRCUMSTANȚE**	**SCOR**

Tipul încălcării Tipul de încălcare care a avut loc poate afecta nivelul de risc prezentat persoanelor fizice. De exemplu, o încălcare a confidenţialităţii prin care anumite informaţii au fost dezvăluite părţilor neautorizate poate avea consecinţe diferite pentru o persoană faţă de cazul unei încălcări în care informaţiile s-au pierdut şi nu mai sunt disponibile.	Confidenţialitate	10
	Integritate	10
	Disponibilitate	5
Tipul, sensibilitatea şi volumul datelor personale Cu cât sunt mai sensibile datele compromise, cu atât riscul va fi mai mare pentru persoanele afectate. O combinaţie de date cu caracter personal este de obicei mai sensibilă decât o singură informaţie cu caracter personal. Trebuie luate în considerare şi alte date cu caracter personal care pot fi deja disponibile cu privire la persoana vizată.	Date comune, cantitate mică	1
	Date comune, cantitate mare	5
	Date sensibile, cantitate mică	5
	Date sensibile, cantitate mare	10
Identificarea persoanelor vizate Un factor important de luat în considerare este cât de uşoară este identificarea persoanelor vizate pentru o persoană care are acces la datele cu caracter personal compromise.	Identificare imposibilă	0
	Identificare dificilă	2
	Identificare uşoară	5
Gravitatea consecinţelor pentru indivizi. În funcţie de natura datelor personale implicate într-o încălcare, de exemplu, categorii speciale de date, daunele potenţiale pentru persoanele care ar putea rezulta pot fi deosebit de grave, în special atunci când încălcarea ar putea duce la furt de identitate sau fraudă vătămare fizică, stres psihologic, umilire sau deteriorarea reputaţiei.	Fără consecinţe	1
	Consecinţe minime	2
	Consecinţe medii	5
	Consecinţe mari	10
Caracteristici speciale ale operatorului de date Domeniul de activitate şi activităţile desfăşurate de operator pot afecta nivelul de risc pentru persoane ca urmare a unei încălcări.	Prelucrare date comune	1
	Prelucrare date sensibile	5
Caracteristici speciale ale individului O încălcare poate afecta datele personale cu privire la copii sau alte persoane vulnerabile, care pot fi expuse unui risc mai mare faţă de alte categorii de persoane. Pot exista şi alţi factori ai individului care pot afecta nivelul de impact asupra lor.	Alte categorii	1
	Persoană vulnerabilă	5
	Copil	10

Numărul de persoane afectate O încălcare poate afecta doar una sau câteva persoane sau câteva mii. În general, cu cât numărul de persoane afectate este mai mare, cu atât impactul unei încălcări poate fi mai mare. Cu toate acestea, o încălcare poate avea un impact sever chiar şi asupra unei persoane, în funcţie de natura datelor personale şi de contextul în care acestea au fost compromise. în fiecare caz analizat, trebuie luate în considerare în mod obiectiv probabilitatea şi gravitatea impactului asupra persoanelor afectate	Mai puţin de 100 de persoane	1
	Între 100 şi 1000 de persoane	3
	Între 1000 şi 100 000 de persoane	5
	Peste 100 000 de persoane	10
Riscul potenţial calculat ca suma scorurilor selectate la fiecare criteriu:	Minim: 10 Maxim: 60	

Notificarea încălcărilor către ANSPDCP se va face pentru fiecare încălcare care îndeplineşte simultan următoarele condiţii:

- Valoarea cantitativă a riscului potenţial calculat depăşeşte 30;
- Dacă sunt aplicabile simultan cel puţin 3 circumstanţe calitative (cu majuscule).

Informarea încălcărilor către persoanele vizate se va face pentru fiecare încălcare care îndeplineşte simultan următoarele condiţii:

- Valoarea cantitativă a riscului potenţial calculat depăşeşte 40;
- Dacă sunt aplicabile simultan cel puţin 3 circumstanţe calitative

8. DECIZII REFERITOARE LA INFORMARE ŞI NOTIFICARE

	Justificare decizii:
	Notificarea ANSPDPC
	Notificarea altei autorităţi de supraveghere (precizaţi):
	Informarea persoanelor vizate
	Nu este necesară notificarea ANSPDPC
	Nu este necesară informarea persoanelor vizate

9. MĂSURI CE SE RECOMANDĂ A FI LUATE PE VIITOR

Pentru a nu se mai repeta astfel de situaţii, se va urmări:

i. [...]
ii. [...]
iii. [...]

10. SANCȚIUNI APLICATE ÎN SITUAȚII SIMILARE

i. [...]
ii. [...]
iii. [...]

11. ANEXE

a. Anexa 1 – [...]
b. Anexa 2 – [...]
c. Anexa 3 – [...]