Rector,
Conf. univ. dr. Ramona Flavia Rațiu

POLITICĂ **Bune practici pentru gestionarea incidentelor**
Cod: PLT-DPO-02
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. Scop

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 politici (**„Politica"**) care să stabilească bunele practici care se recomandă a fi urmate pentru situația producerii unui incident de securitate în cadrul ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ***.

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").

Articolul 32 Securitatea prelucrării

(1) Având în vedere stadiul actual al dezvoltării, costurile implementării și natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și riscul cu diferite grade de probabilitate și gravitate pentru drepturile și libertățile persoanelor fizice, operatorul și persoana împuternicită de acesta implementează măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător acestui risc, incluzând printre altele, după caz:

(a) pseudonimizarea și criptarea datelor cu caracter personal;

(b) capacitatea de a asigura confidențialitatea, integritatea, disponibilitatea și rezistența continue ale sistemelor și serviciilor de prelucrare;

(c) capacitatea de a restabili disponibilitatea datelor cu caracter personal și accesul la acestea în timp util în cazul în care are loc un incident de natură fizică sau tehnică;

(d) un proces pentru testarea, evaluarea și aprecierea periodice ale eficacității măsurilor tehnice și organizatorice pentru a garanta securitatea prelucrării.

(2) La evaluarea nivelului adecvat de securitate, se ține seama în special de riscurile prezentate de prelucrare, generate în special, în mod accidental sau ilegal, de distrugerea, pierderea, modificarea, divulgarea neautorizată sau accesul neautorizat la datele cu caracter personal transmise, stocate sau prelucrate într-un alt mod.

(3) Aderarea la un cod de conduită aprobat, menționat la articolul 40, sau la un mecanism de certificare aprobat, menționat la articolul 42, poate fi utilizată ca element prin care să se demonstreze îndeplinirea cerințelor prevăzute la alineatul (1) din prezentul articol.

(4) Operatorul și persoana împuternicită de acesta iau măsuri pentru a asigura faptul că orice persoană fizică care acționează sub autoritatea operatorului sau a persoanei împuternicite de operator și care are acces la date cu caracter personal nu le prelucrează decât la cererea operatorului, cu excepția cazului în care această obligație îi revine în temeiul dreptului Uniunii sau al dreptului intern.

Articolul 33 Notificarea autorității de supraveghere în cazul încălcării securității datelor cu caracter personal

(1) În cazul în care are loc o încălcare a securității datelor cu caracter personal, operatorul notifică acest lucru autorității de supraveghere competente în temeiul articolului 55, fără

întârzieri nejustificate și, dacă este posibil, în termen de cel mult 72 de ore de la data la care a luat cunoștință de aceasta, cu excepția cazului în care este susceptibilă să genereze un risc pentru drepturile și libertățile persoanelor fizice. În cazul în care notificarea nu are loc în termen de 72 de ore, aceasta este însoțită de o explicație motivată din partea autorității de supraveghere în cazul în care.

(2) Persoana împuternicită de operator înștiințează operatorul fără întârzieri nejustificate după ce ia cunoștință de o încălcare a securității datelor cu caracter personal.

(3) Notificarea menționată la alineatul (1) cel puțin:

(a) descrie caracterul încălcării securității datelor cu caracter personal, inclusiv, acolo unde este posibil, categoriile și numărul aproximativ al persoanelor vizate în cauză, precum și categoriile și numărul aproximativ al înregistrărilor de date cu caracter personal în cauză;

(b) comunică numele și datele de contact ale responsabilului cu protecția datelor sau un alt punct de contact de unde se pot obține mai multe informații;

(c) descrie consecințele probabile ale încălcării securității datelor cu caracter personal;

(d) descrie măsurile luate sau propuse spre a fi luate de operator pentru a remedia problema încălcării securității datelor cu caracter personal, inclusiv, după caz, măsurile pentru atenuarea eventualelor sale efecte negative.

(4) Atunci când și în măsura în care nu este posibil să se furnizeze informațiile în același timp, acestea pot fi furnizate în mai multe etape, fără întârzieri nejustificate.

(5) Operatorul păstrează documente referitoare la toate cazurile de încălcare a securității datelor cu caracter personal, care cuprind o descriere a situației de fapt în care a avut loc încălcarea securității datelor cu caracter personal, a efectelor acesteia și a măsurilor de remediere întreprinse. Această documentație permite autorității de supraveghere să verifice conformitatea cu prezentul articol.

2. Domeniul de aplicare al politicii

Politica 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. 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 și al Consiliului
2.	DPO	Responsabil cu protecția datelor

5. Ce este o încălcare a securității datelor cu caracter personal?

Încălcarea securității datelor cu caracter personal este un eveniment care amenință securitatea datelor cu caracter personal pe care ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ*** le prelucrează (**Incidentul**).

Cauzele unui Incident pot fi printre cele mai variate:

- Incidentul poate fi pur întâmplător (un accident) sau poate rezulta din culpa (neglijența) ori chiar intenția cuiva. Chiar și dacă nu au existat consecințe negative pentru persoana vizată, pentru ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ*** sau pentru oricine altcineva, eveniment de tipul celui de mai sus rămâne o încălcare a securității datelor cu caracter personal.
    - De exemplu, *dacă un hoț intră într-o cameră unde sunt stocate suporturi ale datelor cu caracter personal (documente, stații de lucru etc.), aceasta constituie un Incident chiar și dacă respectivele suporturi nu au fost consultate sau furate.*

Există **trei aspecte principale** care caracterizează securitatea datelor cu caracter personal: confidențialitate, integritate și disponibilitate. În consecință, și încălcarea securității datelor cu

caracter personal (Incidentul) poate fi de trei tipuri: încălcarea confidențialității datelor, încălcarea integrității datelor și încălcarea disponibilității datelor.

Confidențialitatea presupune că datele cu caracter personal nu trebuie să fie accesate de persoane care nu au autorizare în acest sens.

Exemple de încălcare a confidențialității datelor:

- *transmiterea prin email sau poștă tradițională a unei scrisori care include date cu caracter personal către destinatarul greșit. Nu contează dacă destinatarul greșit este o persoană cu care **UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ** are foarte multe contacte (ex. un furnizor cu care lucrăm de mult timp) sau în care avem încredere;*
- *transmiterea unui email în masă și includerea adreselor destinatarilor în câmpul CC în loc de BCC;*
- *pierderea unui stick USB care conține documente ce includ date cu caracter personal;*
- *pierderea (eg, într-un taxi) a unui plic cu documente printate care conțin date cu caracter personal;*
- *aruncarea unui document care conține date cu caracter personal într-un coș de gunoi normal în loc de folosirea unui shredder special.*

Integritatea presupune că datele cu caracter personal nu trebuie să fie modificate decât la cererea persoanei vizate (potrivit dreptului său la rectificarea datelor) sau atunci când realizăm că trebuie actualizate sau schimbate altfel. Modificarea se va realiza în toate cazurile de persoana autorizată.

Exemple de încălcare a integrității datelor:

- *modificarea accidentală a datelor beneficiarilor;*
- *înlocuirea accidentală a datelor din sistem cu date care nu mai sunt actuale sau cu date a căror corectitudine nu a fost verificată.*

Disponibilitatea presupune că datele cu caracter personal trebuie să poată fi accesate și prelucrate în alt mod fără obstacole. Desigur, datele vor fi disponibile numai persoanelor autorizate și persoanei vizate (potrivit dreptului său de acces la date).

Exemple de încălcare a disponibilității datelor:

- *distrugerea sau pierderea accidentală a unor documente care conțin date cu caracter personal;*
- *ștergerea accidentală a unor documente electronice care conțin date cu caracter personal (eg, pe calculator sau stick USB);*
- *pierderea accidentală a cheii (parolei) care permite acces la datele criptate;*
- *imposibilitatea temporară a accesării datelor prelucrate prin mijloace automate din cauza unei întreruperi în alimentarea cu energie electrică.*

Incidentul poate fi o combinație de două sau mai multe dintre tipurile de încălcări de date cu caracter personal. De exemplu: *sistemul IT este afectat de un virus care criptează documentele (hacker-ul cerând o recompensă în schimbul decriptării documentelor) – în acest*

caz, avem de-a face atât cu o încălcare a disponibilității datelor, cât și cu o încălcare a confidențialității acestora în cazul în care hacker-ul a obținut acces la datele cu caracter personal din sistem.

6. **Ce procedură trebuie să urmați atunci când suspectați că a avut loc un Incident?**

UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ este obligată de lege să raporteze autorității de supraveghere (Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal, ANSPDCP) Incidentul imediat și în orice caz nu mai târziu de 72 de ore de când a aflat despre el. De aceea este esențial să informați imediat personalul împuternicit cu atribuții în domeniul protecției datelor, ori de câte ori suspectați că a avut loc sau că este posibil să fi avut loc un Incident.
Datele de contact ale acestuia sunt:
Denumire: **AMPLUSNET S.R.L.**
Adresă de email: **...(adresa de email dpo@companie.ro)**

Aveți obligația de a raporta Incidentul nu doar atunci când ați fost martor nemijlocit la acest eveniment, ci și atunci când pe baza a diverse indicii ajungeți la concluzia că este posibil ca un Incident să fi avut loc. Orice dubiu pe care îl aveți trebuie să conducă la raportare. De exemplu, trebuie să raportați dacă primiți un email prin care un furnizor sau beneficiar vă informează despre faptul că a primit un mesaj suspicios de la un expeditor care pretinde că este un angajat al ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ***, dar care a folosit un email cu o altă extensie decât cea a adresei de email de serviciu a angajaților noștri.

Chiar și atunci când sunteți informat(ă) de un alt angajat al ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ*** despre un eveniment care ar putea constitui un Incident, aveți obligația de a raporta acel eveniment dacă nu sunteți sigur(ă) dacă acel angajat a făcut deja aceasta.

Raportarea Incidentului va avea prioritate asupra oricăror altor obligații profesionale. Chiar și sarcinile de lucru urgente vor putea fi îndeplinite doar după ce v-ați îndeplinit obligația de raportare. Nimeni nu vă va sancționa pentru că vă aduceți la îndeplinire această obligație conform Politicii.

Este foarte important să vă păstrați calmul. Nimeni nu vă va solicita să fiți un expert în protecția datelor, ci doar să cooperați cu cei care sunt experții.

Ca regulă, raportarea va avea loc în scris (ex, prin email). În scopul informării cât mai rapide, veți compune un email scurt către salariatul împuternicit care să descrie elementele esențiale ale Incidentului, urmând să rămâneți disponibil(ă) pentru a îi oferi salariatului împuternicit detalii atunci când vi le va solicita. În concret, prin email-ul de mai sus veți comunica următoarele:

- În ce a constat Incidentul?
- Când și unde a avut loc?
- Care sunt circumstanțele Incidentului?
- Cum și de la cine ați aflat despre Incident?

- Când ați aflat despre Incident (data, ora și minutul)?
- Ce altă persoană în afară de dumneavoastră are sau ar putea avea cunoștință despre Incident (martori, persoane de la care ați obținut informații cu privire la eveniment)?

Dacă nu aveți toate aceste informații, nu așteptați să le obțineți. Comunicați imediat salariatului împuternicit informațiile pe care le aveți dintre cele de mai sus și rămâneți în toate cazurile la dispoziția acestuia/ acesteia pentru a îi oferi clarificări suplimentare.

7. **Documentarea Incidentelor**

Responsabilul cu Protecția Datelor sau persoana cu atribuții din cadrul ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ*** va ține un registru care va include informațiile solicitate de RGPD cu privire la toate cazurile de încălcare a securității datelor cu caracter personal (Incidentele) apărute în activitatea ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ.***

În plus față de registrul cazurilor de încălcare a securității datelor cu caracter personal, pentru fiecare caz de încălcare, Responsabilul cu Protecția Datelor sau persoana cu atribuții din cadrul ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ*** va păstra documente cu privire la:

- data începerii și data finalizării procedurii cu privire la Incident;
- momentul la care ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ*** a luat cunoștință de Incident;
- descrierea Incidentului: situația de fapt; caracterul încălcării; categoriile de persoane vizate (unde este posibil); numărul aproximativ de persoane vizate (unde este posibil); categoriile de înregistrări de date (unde este posibil); numărul aproximativ de înregistrări de date (unde este posibil);
- descrierea consecințelor probabile (efectelor) ale Incidentului;
- descrierea măsurilor luate pentru a remedia Incidentul, inclusiv, după caz, măsurile pentru atenuarea eventualelor efecte negative ale sale;
- evaluarea nivelului de risc al Incidentului pentru drepturile și libertățile persoanelor vizate;
- informații privind notificarea Incidentului către autoritatea de supraveghere;
- detalii privind informarea persoanelor vizate despre Incident;
- documente doveditoare atașate, inclusiv documente care pot servi la a demonstra respectarea procedurilor în caz de încălcare a securității datelor cu caracter personal.

8. **Dispoziții speciale privind încălcarea securității datelor cu caracter personal în cadrul activității *UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ* în calitate de persoană împuternicită**

Atunci când ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ*** acționează în calitate de persoană împuternicită (sau subîmputernicit), aceasta are, potrivit RGPD, obligația de a sprijini operatorul de date cu caracter personal în realizarea obligațiilor de notificare a autorității de supraveghere și de informare a persoanelor vizate (dacă este cazul) cu privire la încălcarea securității datelor cu caracter personal. Potrivit RGPD, aceste obligații

trebuie incluse în contractul dintre ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ*** și operator.

Acolo unde acordul dintre ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ*** și operator nu precizează în suficient detaliu cele de mai sus într-un caz dat, se vor aplica prevederile de mai jos.

UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ nu este împuternicită sau obligată să notifice Incidentul către autoritatea de supraveghere sau să informeze persoanele vizate despre acesta ori să țină registrul de încălcări în numele operatorului.

În schimb, ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ*** prin personalul cu atribuții sau Responsabilul cu Protecția Datelor este obligată să raporteze imediat operatorului despre existența Incidentului și să îi transmită acestuia din urmă o descriere a Incidentului. ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ*** are obligația de a înștiința operatorul fără întârzieri nejustificate după ce ia cunoștință de Incident. Dacă există dubiu, este recomandabil ca Incidentul să fie raportat operatorului.

Atunci când raportează operatorului, ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ*** va oferi toate informațiile pe care le are cu privire la Incident sau cu privire la evenimentul care ar putea constitui un incident. Dacă este cazul, ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ*** va raporta operatorului în mai multe etape, pe măsură ce ajunge să cunoască informații suplimentare despre Incident.

UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ va sprijini operatorul pentru a își îndeplini obligațiile care îi revin acestuia din urmă potrivit legislației datelor cu caracter personal în caz de încălcare a securității datelor cu caracter personal. Aceasta include, dar fără a se limita la, faptul că ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ*** va acționa potrivit instrucțiunilor documentate (inclusiv în formă electronică) ale operatorului.

Pentru evitarea oricărui dubiu, ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ*** nu va examina probabilitatea riscurilor anterior notificării operatorului, aceasta fiind responsabilitatea operatorului. ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ*** aduce această responsabilitate la cunoștința operatorului (chiar dacă acesta o cunoaște deja) la prima comunicare cu acesta privitoare la Incident. ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ*** doar va informa operatorul despre incident fără întârzieri nejustificate, potrivit acestei subsecțiuni (Dispoziții speciale privind încălcarea securității datelor cu caracter personal în cadrul activității ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ*** în calitate de persoană împuternicită).

Atunci când ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ*** acționează în calitate de persoană împuternicită pentru mai mulți operatori vizați de Incident, ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ*** va informa fiecare dintre operatorii vizați despre Incident.

Atunci când ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ*** are calitatea de subîmputernicit, își va îndeplini față de persoana împuternicită obligațiile de mai sus (pe care le-ar fi avut ca persoană împuternicită față de operator).

Obligațiile ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ*** din această subsecțiune (Dispoziții speciale privind încălcarea securității datelor cu caracter personal în cadrul activității ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ*** în calitate de persoană împuternicită) vor fi aduse la îndeplinire de salariatul împuternicit. Angajații sunt în continuare obligați să sprijine salariatul împuternicit în îndeplinirea responsabilităților sale în această privință.

Dispoziții speciale privind încălcarea securității datelor cu caracter personal în cadrul activității ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ*** în calitate de operator asociat

Atunci când ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ*** acționează în calitate de operator asociat, acesta are obligația de a stabili în mod clar rolul și responsabilitățile fiecărui operator asociat (alături de ceilalți astfel de operatori asociați) în cazul în care are loc un incident cu privire la prelucrările pe care le realizează în acea calitate.

Acolo unde acordul dintre ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ*** și celălalt operator asociat/ ceilalți operatori asociați nu precizează în suficient detaliu rolul și responsabilitățile fiecăruia, ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ*** va agrea imediat cu ceilalți operatori asociați care dintre operatorii asociați va fi responsabil cu aducerea la îndeplinire a obligațiilor de notificare a incidentului către autoritatea de supraveghere sau, după caz, de informare a persoanelor vizate.

Pentru evitarea oricărui dubiu, ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ*** va completa registrul de evidență a cazurilor de încălcare a securității datelor cu caracter personal inclusiv în cazul încălcărilor care vizează prelucrările ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ*** în calitate de operator asociat.

Obligațiile ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ*** din această subsecțiune (Dispoziții speciale privind încălcarea securității datelor cu caracter personal în cadrul activității ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ*** în calitate de operator asociat) vor fi aduse la îndeplinire de salariatul împuternicit. Angajații sunt în continuare obligați să sprijine salariatul împuternicit în îndeplinirea responsabilităților sale în această privință.

9. Momentul de la care *UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ* a luat cunoștință de încălcarea securității datelor cu caracter personal

Pentru scopurile acestei politici, momentul de la care ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ*** va fi considerată că a luat cunoștință de încălcarea securității datelor cu caracter personal va fi:
Momentul la care primul angajat a luat cunoștință de eveniment – dacă decizia salariatului împuternicit cu privire la faptul dacă evenimentul respectiv constituie sau nu o încălcare a securității datelor cu caracter personal nu necesită realizarea de verificări suplimentare.

Momentul la care salariatul împuternicit a colectat ultima informație a cărei examinare, împreună cu informațiile colectate anterior, permite un nivel rezonabil de certitudine că a avut loc o încălcare a securității datelor – dacă decizia cu privire la faptul dacă evenimentul respectiv constituie sau nu o încălcare necesită realizarea de verificări suplimentare.

10. 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	-	12	-Elaborare conf. Regulamentului UE679/2016 şi a ghidurilor emise de EDPB -Elaborare conform OSGG 600/2018	
2							
3							
4							
5							

11. Formular analiză politică

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								

12. Lista de distribuire a politicii

Nr. ex.	Compartiment	Nume și prenume	Data primirii politicii	Semnătura	Data retragerii politicii	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						