**UNIVERSITATEA POLITEHNICA TIMIȘOARA**

Piața Victoriei, nr. 2, 300006, Timișoara, județ Timiș, România
*Tel:* +40 256 40 30 11
*Fax:* +40 256 40 30 21
*E-mail:* rector@upt.ro; datepersonale@upt.ro

# PROCEDURA DE NOTIFICARE A ÎNCĂLCĂRII SECURITĂȚII DATELOR CU CARACTER PERSONAL

# CUPRINS

## 1. DEFINIȚII

1. **„date cu caracter personal”** înseamnă orice informații privind o persoană fizică identificată sau identificabilă („persoana vizată”); o persoană fizică identificabilă este o persoană care poate fi identificată, direct sau indirect, în special prin referire la un element de identificare, cum ar fi un nume, un număr de identificare, date de localizare, un identificator online, sau la unul sau mai multe elemente specifice, proprii identității sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale;
2. **„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;
3. **„restricționarea prelucrării”** înseamnă marcarea datelor cu caracter personal stocate cu scopul de a limita prelucrarea viitoare a acestora;
4. **„creare de profiluri”** înseamnă orice formă de prelucrare automată a datelor cu caracter personal care constă în utilizarea datelor cu caracter personal pentru a evalua anumite aspecte personale referitoare la o persoană fizică, în special pentru a analiza sau prevedea aspecte privind performanța la locul de muncă, situația economică, sănătatea, preferințele personale, interesele, fiabilitatea, comportamentul, locul în care se află persoana fizică respectivă sau deplasările acesteia;
5. **„pseudonimizare”** înseamnă prelucrarea datelor cu caracter personal într-un asemenea mod încât acestea să nu mai poată fi atribuite unei anume persoane vizate fără a se utiliza informații suplimentare, cu condiția ca aceste informații suplimentare să fie stocate separat și să facă obiectul unor măsuri de natură tehnică și organizatorică care să asigure neatribuirea respectivelor date cu caracter personal unei persoane fizice identificate sau identificabile;
6. **„sistem de evidență a datelor”** înseamnă orice set structurat de date cu caracter personal accesibile conform unor criterii specifice, fie ele centralizate, descentralizate sau repartizate după criterii funcționale sau geografice;
7. **„operator”** înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care, singur sau împreună cu altele, stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal; atunci când scopurile și mijloacele prelucrării sunt stabilite prin dreptul Uniunii sau dreptul intern, operatorul sau criteriile specifice pentru desemnarea acestuia pot fi prevăzute în dreptul Uniunii sau în dreptul intern;
8. **„persoană împuternicită de operator”** înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care prelucrează datele cu caracter personal în numele operatorului;
9. **„destinatar”** înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism căreia (căruia) îi sunt divulgate datele cu caracter personal, indiferent dacă este sau nu o parte terță. Cu toate acestea, autoritățile publice cărora li se pot comunica date cu caracter personal în cadrul unei anumite anchete în conformitate cu dreptul Uniunii sau cu dreptul intern nu sunt considerate destinatari; prelucrarea acestor date de către autoritățile publice respective

respectă normele aplicabile în materie de protecție a datelor, în conformitate cu scopurile prelucrării;

10. **„parte terță”** înseamnă o persoană fizică sau juridică, autoritate publică, agenție sau organism altul decât persoana vizată, operatorul, persoana împuternicită de operator și persoanele care, sub directa autoritate a operatorului sau a persoanei împuternicite de operator, sunt autorizate să prelucreze date cu caracter personal;
11. **„consimțământ”** al persoanei vizate înseamnă orice manifestare de voință liberă, specifică, informată și lipsită de ambiguitate a persoanei vizate prin care aceasta acceptă, printr-o declarație sau printr-o acțiune fără echivoc, ca datele cu caracter personal care o privesc să fie prelucrate;
12. **„încălcarea securității datelor cu caracter personal”** înseamnă o încălcare a securității care duce, în mod accidental sau ilegal, la distrugerea, pierderea, modificarea, sau divulgarea neautorizată a datelor cu caracter personal transmise, stocate sau prelucrate într-un alt mod, sau la accesul neautorizat la acestea;
13. **„sediu principal”** înseamnă:
    (a) în cazul unui operator cu sedii în cel puțin două state membre, locul în care se află administrația centrală a acestuia în Uniune, cu excepția cazului în care deciziile privind scopurile și mijloacele de prelucrare a datelor cu caracter personal se iau într-un alt sediu al operatorului din Uniune, sediu care are competența de a dispune punerea în aplicare a acestor decizii, caz în care sediul care a luat deciziile respective este considerat a fi sediul principal;
    (b) în cazul unei persoane împuternicite de operator cu sedii în cel puțin două state membre, locul în care se află administrația centrală a acesteia în Uniune, sau, în cazul în care persoana împuternicită de operator nu are o administrație centrală în Uniune, sediul din Uniune al persoanei împuternicite de operator în care au loc activitățile principale de prelucrare, în contextul activităților unui sediu al persoanei împuternicite de operator, în măsura în care aceasta este supusă unor obligații specifice în temeiul prezentului regulament;
14. **„reprezentant”** înseamnă o persoană fizică sau juridică stabilită în Uniune, desemnată în scris de către operator sau persoana împuternicită de operator în temeiul articolului 27, care reprezintă operatorul sau persoana împuternicită în ceea ce privește obligațiile lor respective care le revin în temeiul prezentului regulament;
15. **„întreprindere”** înseamnă o persoană fizică sau juridică ce desfășoară o activitate economică, indiferent de forma juridică a acesteia, inclusiv parteneriate sau asociații care desfășoară în mod regulat o activitate economică;
16. **„autoritate de supraveghere”** înseamnă o autoritate publică independentă instituită de un stat membru în temeiul articolului 51;
17. **„autoritate de supraveghere vizată”** înseamnă o autoritate de supraveghere care este vizată de procesul de prelucrare a datelor cu caracter personal deoarece:
    (a) operatorul sau persoana împuternicită de operator este stabilită pe teritoriul statului membru al autorității de supraveghere respective;
    (b) persoanele vizate care își au reședința în statul membru în care se află autoritatea de supraveghere respectivă sunt afectate în mod semnificativ sau sunt susceptibile de a fi afectate în mod semnificativ de prelucrare;

(c) la autoritatea de supraveghere respectivă a fost depusă o plângere;

18. **„încălcarea securității datelor cu caracter personal”** înseamnă o încălcare a securității care duce în mod accidental sau ilegal, la distrugerea, pierderea, modificarea, sau divulgarea neautorizată a datelor cu caracter personal transmise, stocate sau prelucrate într-un alt mod, sau la accesul neautorizat la acestea.

## 2. SCOPUL ȘI DOMENIUL DE APLICARE

### 2.1.SCOPUL

2.1.1. Prezenta procedură documentează cerințele GDPR privind procedura de raportare și tratare a incidentelor de securitate și are rolul de a prezenta modalitatea concretă de notificare a Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal și de informare a persoanei vizate în cazul în care se produce o încălcare a securității datelor cu caracter personal.

2.1.2. Prin procedură se urmărește asigurarea unui flux corect, eficient și legal al notificărilor transmise către Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal și al informațiilor persoanelor vizate în cazul încălcării securității datelor cu caracter personal în temeiul GDPR și al legislației conexe.

2.1.3. Potrivit Regulamentului (UE) 2016/679, instituția are obligația de a raporta încălcarea securității datelor cu caracter personal către Autoritatea Națională, în termen de 72 de ore de la constatarea încălcării. Dacă este depășit acest termen, trebuie furnizate motive temeinice pentru întârziere.

2.1.4. Potrivit Regulamentului (UE) 2016/679, instituția are obligația informării persoanelor vizate cu privire la încălcarea securității datelor cu caracter personal, dacă încălcarea respectivă este succeptibilă să genereze un risc ridicat de afectare negativă a drepturilor și libertăților persoanelor vizate, fără întârzieri justificative.

### 2.2.DOMENIUL DE APLICARE

Prezenta procedură se aplică personalului angajat al Universității Politehnica Timișoara (personal didactic, didactic auxiliar, administrativ), cât și persoanelor care dobândesc statutul de student/ masterand/ doctorand în urma concursurilor de admitere organizare de către universitate.

Prezenta procedură este întocmită în scopul pregătirii pentru eventualitatea producerii unei încălcări a securități datelor cu caracter personal și planul de reacție la acesta, precum și a atribuțiilor persoanelor implicate în procesul de notificare a Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal și de informare a persoanelor vizate afectate.

### 2.3.DOMENIUL DE REFERINȚĂ

*** Regulamentul (UE) 679/2016 al Parlamentului European și al Consiliului privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulament general privind protecția datelor).

*** Decizia nr.128/22.06.2018 a Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal, privind aprobarea formularului tipizat al notificării de încălcare a securității datelor cu caracter personal în conformitate cu Regulamentul (UE) 679/2016 al Parlamentului European și al Consiliului privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulament general privind protecția datelor).

## 3. REGULI PRIVIND PROCEDURA DE RAPORTARE ȘI TRATARE A ÎNCĂLCĂRII SECURITĂȚII DATELOR CU CARACTER PERSONAL

### 3.1.ASPECTE GENERALE

Încălcarea securității datelor cu caracter personal înseamnă o încălcare a securității care duce, în mod accidental sau ilegal, la distrugerea, pierderea, modificarea sau divulgarea neautorizată a datelor cu caracter personal transmise, stocate sau prelucrate într-un alt mod sau la accesul neautorizat la acestea. Aceasta include încălcările cauzate atât în mod accidental,cât ți în mod intenționat.

Încălcările de securitate vor fi raportate Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal.

În cazul în care încălcarea este susceptibilă să genereze un risc ridicat pentru drepturile și libertățile persoanelor vizate, vor fi informate persoanele în cauză în mod direct și fără întârzieri nejustificate.

Încălcarea securității datelor cu caracter personal, poate afecta confidențialitatea, integritatea sau disponibilitatea datelor cu caracter personal.

Încălcarea securității datelor cu caracter personal pot cuprinde:

- Accesul unui terț neautorizat;
- Acțiunea (sau inacțiunea) intenționată sau accidentală a unui operator sau unei persoane împuternicite de operator;
- Trimiterea unor date cu caracter personal către un destinatar greșit;
- Pierderea sau furtul unor dispozitive informatice care conțin date cu caracter personal;
- Modificatea datelor cu caracter personal fără permisiunea titularului.

### 3.2. REGULI CU PRIVIRE LA COMUNICAREA ÎNCĂLCĂRII SECURITĂȚII DATELOR CU CARACTER PERSONAL

I. Structurile care prelucrează datele cu caracter personal au obligația ca în momentul producerii sau sesizării unei încălcări a securității datelor cu caracter personal, să înștiințeze, fără întârzieri nejustificate, responsabilul cu protecția datelor.

II. Responsabilul cu protecția datelor cu caracter personal, are următoarele responsabilități:

- Informează de îndată conducerea universității;
- Conlucrează cu structura care a sesizat încălcarea securității datelor cu caracter personal în vederea analizării acestei încălcări;

- Notifică Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal cu privire la încălcarea securității datelor cu caracter personal. Potrivit art.33, alin.(1) și alin.(4) din Regulamentul (UE) 2016/679, Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal trebuie informată în cel mult 72 de ore de la data la care universitatea a luat la cunoștință d încălcarea securității datelor, iar în cazul în care notificarea nu are loc în 72 de ore, trebuie însoțită de o explicație motivată privind depășirea acestui termen. În măsura în care nu este posibil să fie furnizate toate informațiile în același timp, acestea pot fi furnizate în mai multe etape, fără întârzieri nejustificate.
- Informează persoana vizată în cazul în care încălcarea securității datelor cu caracter personal este susceptibilă să genereze un risc ridicat pentru drepturile și libertățile persoanei fizice.

### 3.3. ÎNREGISTRAREA ÎNCĂLCĂRII SECURITĂȚII DATELOR CU CARACTER PERSONAL

Persoana responsabilă de înregistrarea incidentelor cu privire la încălcarea securității datelor cu caracter personal în Universitatea Politehnica Timișoara – Cosmin Constantin MUȘAT.

**Responsabil instituțional cu protecție a datelor cu caracter personal**

Piața Victoriei, nr. 2, 300006, Timișoara, județ Timiș, România
*Tel:* +40 256 40 30 11, *Fax:* +40 256 40 30 21, e-*mail:* datepersonale@upt.ro

Reguli generale privind înregistrarea:

- Toate documentele transmise către Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal și/sau persoanele vizate se înregistrează cronologic în registratura generală a universității:
- Este interzisă circulația în cadrul universității, a documentelor cu privire la încălcarea securității datelor cu caracter personal care nu sunt înregistrate.

Separat de înregistrările menționate mai sus, responsabilul cu protecția datelor va păstra o evidență a încălcării securității datelor cu caracter personal într-un registru de evidență a încălcării securității datelor cu caracter personal.

### 3.4. ANALIZA ÎNCĂLCĂRILOR SECURITĂȚII DATELOR CU CARACTER PERSONAL

În analiza incidentelor de securitate, se vor avea în vedere următoarele aspecte:

- Prejudicii de natură fizică, materială sau morală pentru persoanele fizice, cum ar fi: pierderea controlului asupra propriilor date cu caracter personal, limitarea propriilor drepturi, discriminarea, furtul sau frauda identității, pierderea financiară;
- Numărul persoanelor vizate;
- Pierderea confidențialității datelor cu caracter personal protejate prin secret profesional.

În vederea analizării acestora, responsabilul cu protecția datelor cu caracter personal, va obține informații de la structura care prelucra datele în momentul producerii încălcării securității datelor. Această analiză este necesară în vederea informării corecte a Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal, cât și a persoanei vizate.

**Persoanele din cadrul structurilor care întocmesc documente și transmit informații despre persoanele vizate, fără respectarea prevederilor legale în domeniul protecției datelor cu caracter personal, poartă întreaga răspundere asupra încălcării securității datelor.**

### 3.5. NOTIFICAREAAUTORITĂȚII NAȚIONALE DE SUPRAVEGHERE A PRELUCRĂRII DATELOR CU CARACTER PERSONAL

În cadrul universității se transmit notificări cu privire la încălcarea securității datelor cu caracter personal prin următoarele mijloace:

- Electronic/on-line pe site-ul Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal la adresa www.dataprotection.ro , secțiunea Notificare/Breșă RGPD

Pentru transmiterea notificării se va folosii modelul aprobat prin Decizia nr.128/2018 a Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal.

Persoana responsabilă de Notificarea Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal este Cosmin Constantin MUȘAT – responsabil instituțional cu protecția datelor cu caracter personal. Termenul de trimitere a notificării este de 72 de ore. Dacă este depășit acest termen, trebuie furnizate motive temeinice pentru întârziere.

Vor fi păstrate toate documentele referitoare la toate cazurile de încălcare a securității datelor cu caracter personal, fapt care permite Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal să verifice conformitatea cu prevederile Regulamentului (UE) 2016/679.

### 3.6. INFORMAREA PERSOANELOR VIZATE CU PRIVIRE LA ÎNCĂLCAREA SECURITĂȚII DATELOR CU CARACTER PERSONAL

În cazul în care încălcarea este susceptibilă să genereze un risc ridicat pentru drepturile și libertățile persoanelor vizate, acestea vor fi informate fără întârzieri nejustificate. Informarea către persoanele vizate va descrie, într-un limbaj clar și simplu, caracterul încălcării securității datelor cu caracter personal și va cuprinde următoarele informații:

- Numele și datele de contact ale responsabilului cu protecția datelor cu caracter personal sau un alt punct de contact de unde se pot obține mai multe informații;
- Descrierea consecințelor posibile ale încălcării securității datelor cu caracter personal;
- Descrierea măsurilor luate sau propuse spre a fi luate pentru a remedia problema încălcării securității datelor cu caracter personal, inclusiv, după caz, măsurile luate pentru atenuarea eventualelor efecte negative.

Persoana responsabilă de transmiterea informării către persoana vizată este responsabilul cu protecția datelor personale din universitate. Universitatea informează persoanele vizate cu privire la încălcarea datelor cu caracter personal prin următoarele mijloace:

- e-mail (utilizând adresele de e-mail având formatul prenume.nume@upt.ro, respectiv prenume.nume@student.upt.ro )
- pe suport de hârtie, prin intermediul serviciilor poștale.

Informarea persoanei vizate nu este necesară, atunci când:

- au fost implementate măsuri de protecție tehnice și organizatorixe adecvate, care au fost aplicate în cazul datelor cu caracter personal afectate de încălcarea securității, în special măsuri prin care se asigură că datele cu caracter personal devin neinteligibile oricărei persoane care nu este autorizată să le acceseze, cum ar fi criptarea;
- au fost luate măsuri ulterioare prin care se asigură că riscul ridicat pentru drepturile șo libertățile persoanelor vizate nu mai este susceptibil să se materializeze;
- ar necesita un efort disproporționat, caz în care se va efectua pe loc o informare publică sau se ia o măsură similară prin care persoanele vizate sunt informate într-un mod eficace.

### 3.7. SEMNARE

Toate documentele întocmite cu privire la raportarea și tratarea incidentelor de securitate pentru a fi transmise în exteriorul universității, vor fi semnate de către următoarele entități:

- Rectorul universității
- Consilierul Juridic al universității;
- Responsabilul cu protecția datelor cu caracter personal al universității.

### 3.8. CONCLUZII

În situația în care se constată că încălcarea securității datelor cu caracter personal a fost rezultatul unei erori umane sau al unei probleme sistemice, se vor stabili următoarele măsuri:

- Actualizarea sau completarea procedurilor existente ale universității;
- Instruirea personalului în cadrul universității în vederea aplicării procedurilor existente aprobate.

**ANEXĂ:**

Notificare de încălcare a securităţii datelor cu caracter personal pentru operatorii de date cu caracter personal, în conformitate cu Regulamentul (UE) nr. 679/2016 al Parlamentului European şi al Consiliului din 27 aprilie 2016 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE (Regulamentul general privind protecţia datelor)

**SECŢIUNEA 1: Identificarea operatorului**

1. Denumirea operatorului Sector Privat |_| Sector Public |_|

| | | |
|---|---|---|
| | CIF/CUI | |

2. Identitatea şi datele de contact ale responsabilului cu protecţia datelor sau ale unui alt punct de contact de unde se pot obţine mai multe informaţii

| | |
|---|---|
| Numele și prenumele | Număr de telefon |
| | |
| Adresă de e-mail | Adresă de corespondență |
| | |

3. Este notificare nouă sau o completare a notificării iniţiale?

Notificare nouă |_|

Completare notificare nr. |_____| *se va trece numărul de înregistrare al notificării din registrul general al autorităţii

Informaţii iniţiale privind încălcarea securităţii datelor cu caracter personal (se vor specifica în completările ulterioare, dacă este cazul)

4. Data şi ora incidentului (dacă se cunosc; dacă este necesar, se poate face o estimare) şi ale depistării incidentului

4.1.Data şi ora incidentului

| |
|---|
| |

4.2.Data şi ora depistării incidentului

| |
|---|
| |

5.Caracterul încălcării securităţii datelor cu caracter personal (de exemplu: confidenţialitate/integritate/disponibilitate)

6.Natura şi conţinutul datelor cu caracter personal în cauză

7.Măsurile tehnice şi organizatorice aplicate (sau care urmează a fi aplicate) de către operator

8.Utilizarea relevantă a altor operatori (dacă este cazul)

**SECŢIUNEA 2:**

**I.Informaţii suplimentare privind încălcarea securităţii datelor cu caracter personal**

9.Rezumatul incidentului care a generat încălcarea securităţii datelor cu caracter personal (inclusiv localizarea fizică a încălcării şi suporturile de stocare implicate)

10.Numărul persoanelor fizice vizate (estimare, după caz)

11.Eventualele consecinţe şi efecte adverse (riscuri) pentru persoanele fizice vizate

12.Măsurile tehnice şi organizatorice luate de operator în scopul atenuării eventualelor efecte negative

**II.Eventuale informări suplimentare către persoanele fizice vizate**

13.Conţinutul informării sau motivele pentru care nu s-a făcut informarea persoanelor fizice vizate

14.Mijloace de comunicare utilizate pentru transmiterea informărilor

15.Numărul persoanelor fizice vizate informate

**III.Eventuale aspecte transfrontaliere**

16.Încălcare a securităţii datelor cu caracter personal care implică persoane fizice vizate din alte state membre

Da |_| Nu |_|

17.Notificarea altor autorităţi naţionale competente

Da |_| Nu |_|

Dacă da, menţionaţi autorităţile competente:

| |
|---|
| |