

**Serviciul de Consultanță și Avizare Juridică**


**PROCEDURA OPERAȚIONALĂ**

**privind**

**ASIGURAREA SECURITĂȚII DATELOR CU CARACTER PERSONAL  
ÎN UNIVERSITATEA DE VEST DIN TIMIȘOARA**


**COD: PO.UVT-GDPR-01**

**Aprobat în Ședința Consiliului de Administrație al UVT din data de 19.05.2025**

 <b>Universitatea de Vest din Timișoara</b> <b>Serviciul de Consultanță și Avizare Juridică</b>	<b>Procedura operațională Privind asigurarea securității datelor cu caracter personal în Universitatea de Vest din Timișoara</b> <b>Cod: PO.UVT-GDPR-01</b>	<b>Ediția I</b>
		<b>Pagina 2 din 26</b>

**1. Lista responsabililor cu elaborarea, verificarea și aprobarea ediției sau, după caz, a reviziei în cadrul ediției procedurii operaționale**

	Elemente privind responsabilii/ operațiunea	Numele și prenumele	Structura	Data	Semnătura
	1	2	3	4	5
1.1.	Întocmit		Serviciul Consultanță și Avizare juridică		
1.2.	Verificat		Prorector responsabil cu legislația, conformitate, patrimoniul UVT, relația cu Senatul UVT și comunitatea ALUMNI UVT		
1.3.	Aviz juridic		Serviciul Consultanță și Avizare juridică		
1.4.	Avizat pentru conformitate cu OSGG 600/2018		Corp de Control Intern		
1.5.	Aprobat				

 <b>Universitatea de Vest din Timișoara</b> <b>Serviciul de Consultanță și Avizare Juridică</b>	<b>Procedura operațională Privind asigurarea securității datelor cu caracter personal în Universitatea de Vest din Timișoara</b> <b>Cod: PO.UVT-GDPR-01</b>	<b>Ediția I</b>
		<b>Pagina 3 din 26</b>

## 2. Formular de evidență a modificărilor

Nr crt	Ediția /data	Revizia/data	Nr. pagina	Descrierea modificării	Semnătura persoanei care a elaborat/modificat procedura
1.	Ediția I	-	-	Procedură nouă	


## 3. Lista cuprinzând persoanele la care se difuzează ediția sau, după caz, revizia din cadrul ediției procedurii operaționale

	Scopul difuzării	Exemplar nr.	Facultate/Departament	Funcția	Numele și prenumele	Data primirii	Semnătura
	1	2	3	4	5	6	7
3.1.	aplicare	1	Serviciul de Consultanță și Avizare Juridică, Direcția Digitalizare și Analiza Date, Direcția IT&C				
3.2.	informare	1	Toate structurile organizatorice ale UVT				
3.3.	evidență	1	Serviciul de Consultanță și Avizare Juridică				
3.4.	arhivare	1	Serviciul de Consultanță și Avizare Juridică				

## 4. Scopul procedurii

Prezenta procedură reglementează cadrul legal, măsurile tehnice și organizatorice, cât și modul unitar de desfășurare în condiții de siguranță a activităților privind procesul de colectare și prelucrare a datelor cu caracter personal, atât automat, în sistem informatic, cât și prin intermediul altor mijloace, în cadrul Universității de Vest din Timișoara.



 <b>Universitatea de Vest din Timișoara</b> <b>Serviciul de Consultanță și Avizare Juridică</b>	<b>Procedura operațională Privind asigurarea securității datelor cu caracter personal în Universitatea de Vest din Timișoara</b>  <b>Cod: PO.UVT-GDPR-01</b>	<b>Ediția I</b>
		<b>Pagina 4 din 26</b>

## 5. Domeniul de aplicare


Procedura se aplică de către tot personalul, titular sau asociat al Universității de Vest din Timișoara, ce intră în contact cu datele personale, participă la colectarea sau prelucrarea acestora, în strânsă colaborare cu Responsabilul cu protecția datelor cu caracter personal (denumit în continuare DPO).

### 5. Documente de referință

#### 5.1. Externe:

- **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 (Regulamentul general privind protecția datelor);
- **Legea nr. 190/2018** privind măsurile de punere în aplicare a Regulamentului (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 (Regulamentul general privind protecția datelor);
- **Legea nr. 506/2004** privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice;
- **Decizii ale Autorității Naționale de Supraveghere pentru Protecția Datelor cu Caracter Personal**
- **Legea învățământului superior nr. 199/2023**, cu modificările și completările ulterioare
- **Legea 365/2002** privind comerțul electronic, republicată, cu modificări ulterioare
- **Legea nr. 544/2001** privind liberul acces la informațiile de interes public, cu modificările și completările ulterioare
- **Legea nr. 207/2015** privind Codul de procedură fiscală, cu modificările și completările ulterioare
- **Legea nr. 53/2003** Codul muncii, republicată, cu modificările și completările ulterioare;
- **Legea 102/2005** privind înființarea, organizarea și funcționarea Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal, cu modificările și completările ulterioare;
- **Decizia nr. 133/2018** a președintelui Autorității de supraveghere privind aprobarea Procedurii de primire și soluționare a plângerilor
- **H.G. 301/2012** pentru aprobarea Normelor metodologice de aplicare a Legii 333/2003 privind paza obiectivelor, bunurilor, valorilor și protecția persoanelor, cu modificările și completările ulterioare;



 <b>Universitatea de Vest din Timișoara</b> <b>Serviciul de Consultanță și Avizare Juridică</b>	<b>Procedura operațională Privind asigurarea securității datelor cu caracter personal în Universitatea de Vest din Timișoara</b> <b>Cod: PO.UVT-GDPR-01</b>	<b>Ediția I</b>
		<b>Pagina 5 din 26</b>

- **ORDIN nr. 5.760/2024** pentru aprobarea Regulamentului de organizare și funcționare a Comisiei Naționale de Atestare a Titlurilor, Diplomelor și Certificatelor Universitare (CNATDCU)
- **HOTĂRÂRE nr. 301/ 2012** pentru aprobarea Normelor metodologice de aplicare a Legii nr. 333/2003 privind paza obiectivelor, bunurilor, valorilor și protecția persoanelor

## 5.2. Interne:

- Carta Universității de Vest din Timișoara;
- Regulamentul de Ordine Interioară al Universității de Vest din Timișoara;
- Regulamentele de Organizare și Funcționare ale structurilor tehnico-administrative și de învățământ și cercetare ale Universității de Vest din Timișoara;
- Decizii ale Autorității Naționale pentru Protecția Datelor;

## 6. Definiții și abrevieri

### 6.1. Definiții


Nr. Crt.	Termenul	Definiția
1.	Procedura operațională	Procedură care descrie o activitate sau un proces ce se desfășoară în cadrul UVT, la nivelul uneia sau mai multor structuri organizatorice din UVT, fără aplicabilitate la nivelul întregii entități.
2.	Date cu caracter personal	Orice informații privind o persoană identificată sau identificabilă (persoană vizată).
3.	Încălcarea securității datelor cu caracter personal	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.
4.	Persoane vizate	Persoane ale căror date cu caracter personal sunt colectate și prelucrate.
5.	Prelucrare date cu caracter personal	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 combinare, restricționarea, ștergerea ori distrugerea.
6.	Operator	Persoană fizică sau juridică, autoritatea publică, agenția sau alt organism care, singură sau împreună cu altele, stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal- în cazul de față Universitatea de Vest din Timișoara

7.	Persoană împuternicită de operator	Persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care prelucrează datele cu caracter personal în numele operatorului.
8.	Parte terță	Persoană fizică sau juridică, autorizată să prelucreze date cu caracter personal.
9.	Destinatar	Persoană fizică sau juridică, autoritatea publică, agenția sau alt organism căreia (căruia) îi sunt transmise/divulgate datele cu caracter personal, indiferent dacă este sau nu o parte terță.
10.	Consimțământ al persoanei vizate	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.
11.	Date genetice	Datele cu caracter personal referitoare la caracteristicile genetice moștenite sau dobândite ale unei persoane fizice, care oferă informații unice privind fiziologia sau sănătatea persoanei respective și care rezultă în special în urma unei analize a unei mostre de material biologic recoltate de la persoana în cauză.
12.	Date biometrice	Date cu caracter personal care rezultă în urma unor tehnici de prelucrare specifice referitoare la caracteristicile fizice, fiziologice sau comportamentale ale unei persoane fizice care permit sau confirmă identificarea unică a respectivei persoane, cum ar fi imaginile faciale sau datele dactiloscopice.
13.	Date privind sănătatea	Date cu caracter personal legate de sănătatea fizică sau mentală a unei persoane fizice, inclusiv prestarea de servicii de asistență medicală, care dezvăluie informații despre starea de sănătate a acesteia.

## 6.2. Abrevieri

Nr. Crt.	Abrevierea	Termenul abreviat
1.	UVT	Universitatea de Vest din Timișoara
2.	P.O.	Procedură operațională
3.	GDPR	Regulamentul 2016/679/UE al Parlamentului European și al Consiliului din aprilie 2016 privind protecția datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE
4.	DPO	Responsabil cu protecția datelor cu caracter personal



 <b>Universitatea de Vest din Timișoara</b> <b>Serviciul de Consultanță și Avizare Juridică</b>	<b>Procedura operațională Privind asigurarea securității datelor cu caracter personal în Universitatea de Vest din Timișoara</b> <b>Cod: PO.UVT-GDPR-01</b>	<b>Ediția I</b>
		<b>Pagina 7 din 26</b>

## 7. Descriere procedură

### 7.1. Prevederi generale

Prezenta procedură este elaborată și se aplică în conformitate cu prevederile Regulamentului 2016/679/UE 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 (GDPR).


Procedura descrie condițiile și cerințele obligatorii ce trebuie respectate în procesele instituționale de prelucrare a datelor, în vederea asigurării unui nivel ridicat de securizare a datelor cu caracter personal.

### 7.2. Colectarea datelor cu caracter personal

- Înaintea implicării în orice activitate sau proces de colectare a datelor cu caracter personal ale unei persoane sau categorii de persoane vizate, chiar dacă aceasta presupune doar colectarea datelor în procesul de admitere sau de recrutare, stocarea datelor, utilizarea unui nou instrument online, dezvoltarea unei activități de marketing direct din partea universității, un nou proiect, o conferință sau un eveniment organizat în cadrul universității sau orice alt nou proces de prelucrare a datelor cu caracter personal în cadrul UVT, fiecare operator trebuie să își pună următoarele întrebări:
  - ✓ Sigur este nevoie să fie colectată această informație?
  - ✓ Există o bază legală pentru prelucrare (cum ar fi consimțământul persoanei vizate, interesul legitim al universității pentru îndeplinirea unor clauze precontractuale sau în vederea derulării unui contract deja existent, obligații legale ce îi revin universității)?
  - ✓ Datele colectate pot fi anonimizate sau pseudonimizate?
  - ✓ Datele personale vor fi prelucrate în condiții de siguranță?
  - ✓ Datele personale vor fi transmise către o altă parte pentru a fi prelucrate (către o persoană împuternicită de către UVT)?
  - ✓ Este planificat ca datele colectate să fie transferate către o țară non-UE? Dacă da, există un set adecvat de măsuri de securitate implementate în țara respectivă?
  - ✓ Există altă alternativă de îndeplinire a activității respective, fără a fi necesară prelucrarea sau transferarea datelor personale?

Dacă, în urma analizei punctelor de mai sus, se constată necesitatea colectării acelor categorii de date cu caracter personal în structura respectivă a universității, în vederea prelucrării, atunci utilizatorul datelor cu caracter personal trebuie să se conformeze prevederilor Regulamentului 679/2016 (UE).



 <b>Universitatea de Vest din Timișoara</b>  <b>Serviciul de Consultanță și Avizare Juridică</b>	<b>Procedura operațională Privind asigurarea securității datelor cu caracter personal în Universitatea de Vest din Timișoara</b>  <b>Cod: PO.UVT-GDPR-01</b>	<b>Ediția I</b>
		<b>Pagina 8 din 26</b>

- Este important să se analizeze necesitatea unui studiu de impact de câte ori apar noi activități de colectare a datelor în procesele existente sau sunt identificate noi procese ce presupun colectarea de date cu caracter personal.
- GDPR stabilește integrarea măsurilor de confidențialitate încă din faza de proiectare a proceselor care implică prelucrarea datelor personale ("by design"), asigurând astfel că protecția datelor este luată în considerare încă de la început. De asemenea, aceste măsuri trebuie menținute în mod constant și automat pe parcursul tuturor activităților desfășurate, asigurând în mod implicit protecția datelor ("by default"). Acest principiu are scopul de a garanta un nivel ridicat de securitate a datelor pe tot parcursul procesului de prelucrare.
- Colectarea datelor cu caracter personal este permisă numai utilizatorilor autorizați în acest sens, în îndeplinirea obligațiilor de serviciu prevăzute prin fișa postului.


### 7.3. Prelucrarea datelor cu caracter personal

- Prin prelucrarea datelor se înțelege, în mod sumar, orice operațiune sau set de operațiuni efectuate asupra datelor personale, indiferent dacă acestea se realizează prin mijloace automate sau nu. Aceasta poate include acțiuni precum 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 datelor.

Cu alte cuvinte, prelucrarea datelor cu caracter personal implică orice activitate care utilizează date ce pot identifica direct sau indirect o persoană fizică.

- Datele trebuie să fie prelucrate într-un mod care asigură securitatea adecvată a acestora, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, distrugerii sau deteriorării accidentale, prin luarea de măsuri tehnice și organizatorice corespunzătoare (principiul „integritate și confidențialitate”).
- Conducătorii tuturor structurilor din UVT au obligația să stabilească grade de accesibilitate și permisiuni de prelucrare a datelor personale (chiar și numai în cazul vizualizării acestora), în funcție de sarcinile ce îi revin angajatului prin fișa postului.
- La nivelul fiecărei structuri trebuie implementate măsuri care să permită identificarea facilă a utilizatorului care a creat o înregistrare, a actualizat datele sau a modificat accidental înregistrarea (ex. prin contul și parola de acces pentru înregistrările electronice sau prin semnarea fiecărui document emis în format letric).
- Toți utilizatorii au obligația, și vor fi instruiți în acest sens, de a realiza copii de siguranță ale înregistrărilor/bazelor de date ce conțin date cu caracter personal, deținute sau create în timpul executării sarcinilor de serviciu.
- Datele cu caracter personal vor fi prelucrate exclusiv în scopul pentru care au fost colectate.



 <b>Universitatea de Vest din Timișoara</b>  <b>Serviciul de Consultanță și Avizare Juridică</b>	<b>Procedura operațională Privind asigurarea securității datelor cu caracter personal în Universitatea de Vest din Timișoara</b>  <b>Cod: PO.UVT-GDPR-01</b>	<b>Ediția I</b>
		<b>Pagina 9 din 26</b>

- Modificările necesare a fi aduse datelor cu caracter personal se fac doar de către personal autorizat și având un temei legal (ex. la solicitarea persoanei vizate sau cu informații nou create pe parcursul executării unui contract în derulare cu persoana vizată).
- În situația în care persoana autorizată este indisponibilă din motive obiective și colectarea datelor cu caracter personal într-un anumit proces nu poate fi amânată, va fi delegată o altă persoană pentru realizarea sarcinii, cu obligativitatea de a păstra confidențialitatea datelor la care va avea acces temporar, urmând ca imediat ce persoana autorizată de drept își poate relua activitatea, accesul persoanei de back-up să fie restricționat.
- În cazul în care încetează contractul individual de muncă cu universitatea este obligatoriu să se revoce imediat accesul acestuia la bazele de date.


#### 7.4. Păstrarea datelor cu caracter personal

- Datele cu caracter personal trebuie să nu fie stocate pe o perioadă mai lungă decât cea necesară scopului inițial pentru care au fost colectate, în conformitate cu principiul din GDPR privind „limitarea legată de scop” (Art. 5, (1), b).
- Datele cu caracter personal trebuie păstrate într-o formă care permite identificarea persoanelor vizate, pe o perioadă care nu depășește perioada necesară îndeplinirii scopurilor în care sunt prelucrate datele; datele cu caracter personal pot fi stocate pe perioade mai lungi în măsura în care acestea vor fi prelucrate exclusiv în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice, în conformitate cu articolul 89 alineatul (1) din GDPR, sub rezerva punerii în aplicare a măsurilor de ordin tehnic și organizatoric adecvate în vederea garantării drepturilor și libertăților persoanei vizate (cum ar fi pseudonimizarea), conform principiului „limitării legate de stocare” (Art. 5, (1), e) din GDPR).
- Dacă datele personale nu mai sunt necesare scopului pentru care au fost colectate și perioada de arhivare a expirat, acestea trebuie distruse în condiții de maximă siguranță, indiferent că au fost stocate electronic pe un server al instituției, pe PC-uri personale echipamente mobile sau pe suport de hârtie. Înregistrările pe hârtie trebuie să fie fragmentate în deșeuri, iar înregistrările electronice trebuie șterse definitiv.
- Fiecare structură organizatorică din cadrul Universității de Vest din Timișoara este responsabilă de stabilirea și asigurarea perioadelor corespunzătoare de păstrare a informațiilor cu caracter personal pe care le administrează, în condiții de siguranță și în baza legislației de arhivare în vigoare, coroborată cu nomenclatorul arhivistic specific și procedurile interne ale universității.

#### 7.5. Accesarea și administrarea înregistrărilor și bazelor de date cu caracter personal

- Accesul neautorizat, accidental sau intenționat, la documente sau informații cu caracter personal, care poate duce la distrugerea, pierderea, modificarea sau divulgarea acestora, constituie o „încălcare a securității datelor cu caracter personal”.



 <b>Universitatea de Vest din Timișoara</b> <b>Serviciul de Consultanță și Avizare Juridică</b>	<b>Procedura operațională Privind asigurarea securității datelor cu caracter personal în Universitatea de Vest din Timișoara</b> <b>Cod: PO.UVT-GDPR-01</b>	<b>Ediția I</b>
		<b>Pagina 10 din 26</b>

- Conducătorul de structură este responsabil, alături de persoanele din subordine care operează date cu caracter personal, de respectarea obligației păstrării confidențialității informațiilor pe care le procesează. Un acord de confidențialitate (Anexa nr. 1) trebuie semnat de către fiecare persoană (angajat/colaborator/voluntar UVT) care, prin atribuțiile locului de muncă, are acces la/prelucrează date cu caracter personal, acest document însoțind fișa postului.


#### 7.5.1. Accesul și administrarea documentelor ce conțin date cu caracter personal, stocate/arhivate în format fizic

- Accesul în încăperile/zonele în care sunt stocate sau arhivate documente ce conțin date cu caracter personal este strict permis doar persoanelor autorizate de către conducătorii structurilor din UVT, în funcție de atribuțiile de serviciu ce le revin prin fișa postului.
- În cazul în care zona de lucru este de tip „open-space” și nu pot fi implementate măsuri stricte de acces, angajații ce prelucrează date cu caracter personal au obligația de a se asigura că informațiile nu pot fi vizualizate de către ceilalți angajați sau de către vizitatori. Nu este permisă lăsarea documentelor neasigurate pe birouri, în imprimante; acestea trebuie depozitate în dulapuri închise imediat ce operatorul nu mai efectuează prelucrări asupra acestora sau este obligat să își părăsească biroul.
- Utilizatorii autorizați să acceseze sau să prelucreze date cu caracter personal sunt obligați să asigure confidențialitatea acestora și nu vor permite accesul la documente altor persoane neautorizate.
- Este strict interzisă copierea fizică sau pe echipamente de stocare mobilă a informațiilor confidențiale în alt scop decât cel prevăzut de sarcinile de serviciu pentru care angajatul a fost autorizat.
- Este interzisă scoaterea din perimetrul UVT a oricărui tip de informație confidențială sau de înregistrări ce conțin date cu caracter personal, fără o autorizare prealabilă de la conducătorul ierarhic.

#### 7.5.2. Accesul și administrarea datelor cu caracter personal/bazelor de date stocate electronic

- În cazul în care datele cu caracter personal sunt prelucrate sau stocate prin intermediul calculatorului sau într-o bază de date a universității, accesul la sistem va fi permis doar în baza unor parole/conturi de acces, a căror confidențialitate strictă va fi asigurată de către utilizatori și nu vor fi comunicate altor persoane neautorizate informațiile confidențiale, în mod conștient sau accidental.
- Utilizatorii autorizați nu au voie să copieze pe un mediu de stocare mobil (stick USB, CD, DVD, hard disk extern) sau să printeze documente ce conțin date cu caracter personal, în vederea comunicării către o terță parte, fără o autorizare în acest sens.
- Utilizatorii nu vor permite, intenționat sau accidental, accesul altor utilizatori neautorizați pe calculatorul propriu. Monitoarele calculatoarelor vor fi poziționate în așa fel încât datele să nu poată fi vizualizate decât exclusiv de către utilizatorul autorizat. În același




 <b>Universitatea de Vest din Timișoara</b>  <b>Serviciul de Consultanță și Avizare Juridică</b>	<b>Procedura operațională Privind asigurarea securității datelor cu caracter personal în Universitatea de Vest din Timișoara</b>  <b>Cod: PO.UVT-GDPR-01</b>	<b>Ediția I</b>
		<b>Pagina 11 din 26</b>

timp, utilizatorul are obligația de a se asigura că închide în condiții de siguranță orice fișier, bază de date sau sesiune de lucru, imediat ce nu mai operează.

- Indiferent dacă este vorba de proiectarea, întreținerea, actualizarea datelor sau a softului specifice unei baze de date, accesul unei terțe părți este permis strict în aria de lucru, în prezența utilizatorului autorizat. În cazul în care suportul tehnic este asigurat de o firmă externă (persoană împuternicită de universitate), accesul reprezentanților acesteia este permis doar pe durata derulării contractului și numai în baza unui acord de confidențialitate ce va însoți în mod obligatoriu contractul.
- Înregistrările și bazele de date cu caracter personal create sau actualizate de către angajații UVT, în calitate de utilizatori, trebuie să fie salvate în siguranță și să li se creeze copii (back-up). Intervalul de timp la care se execută aceste copii și locația unde vor fi salvate vor fi stabilite de către conducătorii de structuri, în funcție de importanța și volumul acestor informații. Controlul și responsabilitatea acestei acțiuni revin fiecărui conducător de structură, cu mențiunea că intervalul de timp între două operațiuni de creare a back-up-ului pentru același fișier sau bază de date nu trebuie să depășească 3 luni. O evidență a acestor operațiuni va trebui menținută la nivelul fiecărei structuri.
- În exercitarea atribuțiilor de serviciu, tot personalul universității va utiliza adresele de e-mail instituționale, configurate pe serverul Universității de Vest din Timișoara (domeniul e-uvt.ro).
- Nu este permisă trimiterea prin e-mail, către un cont extern domeniului UVT, a unor documente sau informații ce conțin date cu caracter personal, decât în baza unui temei legal (ex. obligație legală ce îi revine universității, la solicitarea directă și în baza consimțământului persoanei vizate, pentru derularea unui contract ce presupune și un acord de confidențialitate etc.) și cu respectarea măsurilor de securitate, cum ar fi parolarea sau criptarea informației.
- Personalul instituției nu trebuie să transmită sau să primească informații confidențiale ce privesc Universitatea de Vest din Timișoara sau care conțin date personale, folosind conturi de e-mail configurate pe servere care nu sunt proprietatea UVT (ex. Yahoo Mail, Gmail, Hotmail, AOL Mail etc.).
- Este interzisă efectuarea de comunicări de marketing prin utilizarea unor sisteme automate de apelare și comunicare care nu necesită intervenția unui operator uman, prin fax ori prin poșta electronică sau prin orice altă metodă care folosește serviciile de comunicații electronice destinate publicului, cu excepția cazului în care abonatul sau utilizatorul vizat și-a exprimat în prealabil consimțământul expres pentru a primi asemenea comunicări (ex. prin intermediul abonării la newsletter).
- Fără a aduce atingere prevederilor alineatului anterior, dacă universitatea, în calitate de persoană juridică, sau un salariat al universității obține în mod direct adresa de poștă electronică a unui candidat/student/elev/angajat/colaborator/altă categorie de persoană vizată, de exemplu cu ocazia participării la un concurs/furnizării serviciilor educaționale/participării într-un proiect sau la un eveniment organizat de universitate, în conformitate cu prevederile GDPR, persoana fizică sau juridică în cauză poate utiliza adresa respectivă, în scopul efectuării de comunicări viitoare de marketing referitoare la




 <b>Universitatea de Vest din Timișoara</b> <b>Serviciul de Consultanță și Avizare Juridică</b>	<b>Procedura operațională Privind asigurarea securității datelor cu caracter personal în Universitatea de Vest din Timișoara</b> <b>Cod: PO.UVT-GDPR-01</b>	<b>Ediția I</b>
		<b>Pagina 12 din 26</b>

servicii educaționale/proiecte/evenimente similare, cu condiția de a oferi un mod clar și expres persoanelor vizate posibilitatea de a se opune printr-un mijloc simplu și gratuit unei asemenea utilizări (de ex. prin trimiterea unui email), atât la obținerea adresei de poștă electronică, cât și cu ocazia fiecărui mesaj, în cazul în care clientul nu s-a opus inițial.

### 7.5.3. Accesarea și administrarea înregistrărilor sistemelor de supraveghere video

- UVT utilizează subsistemul de supraveghere video pentru asigurarea securității și siguranței instituției. Acest subsistem vine în completarea subsistemelor de detecție și alarmare la tentativa de efracție, de control acces, de detecție, semnalizare și alarmare la incendiu, formând împreună un sistem integrat de securitate fizică. Astfel, subsistemele de supraveghere video funcționează în relație de colaborare cu celelalte subsisteme enumerate mai sus, asigurând elementul de monitorizare în timp real și posibilitatea de vizualizare post-eveniment, precum și înregistrarea, afișarea și transmisia video către diverse persoane desemnate ca utilizatori ai subsistemului de supraveghere.
- UVT are obligația de a administra, în condiții de siguranță și numai pentru scopul specificat, datele personale colectate prin intermediul sistemelor de supraveghere video. UVT nu va prelucra datele personale decât în măsura în care acest demers este necesar pentru îndeplinirea scopului mai sus menționat, cu respectarea măsurilor legale de securitate și confidențialitate a datelor.
- Durata de stocare a datelor obținute prin intermediul sistemului de supraveghere video este de 30 de zile, cu excepția situațiilor expres reglementate de lege sau a cazurilor temeinic justificate. La expirarea termenului, înregistrările se distrug sau se șterg.
- Personalul de pază/administrare/service a acestor sisteme de supraveghere, sub atenta supraveghere a conducătorilor structurilor din cadrul Direcției Generale Administrative, va verifica periodic și va răspunde de siguranța și confidențialitatea datelor personale stocate în sistemul de supraveghere/monitorizare video. Angajamentul de confidențialitate (Anexa nr. I) va fi semnat de către fiecare salariat/colaborator/operator ce intră în contact cu sistemele de supraveghere video, prin prisma sarcinilor de serviciu, ca măsură ce demonstrează instruirea și respectarea confidențialității datelor cu caracter personal.
- Operatorii autorizați ai sistemelor de supraveghere video trebuie să se asigure că nu permit accesul în spațiile de vizualizare sau stocare a imaginilor/înregistrărilor video niciunei persoane neautorizate și că nu vor comunica în mod accidental sau intenționat înregistrări către alți destinatari, fără acordul conducătorului ierarhic și un temei legal bine stabilit.
- O evidență clară a dispunerii sistemului de supraveghere video și a personalului care operează/accesează înregistrările trebuie să fie păstrată la nivelul Direcției Generale Administrative și comunicată către Responsabilul cu protecția datelor cu caracter personal al universității (DPO). Orice modificare adusă sistemului de supraveghere video



 <b>Universitatea de Vest din Timișoara</b> <b>Serviciul de Consultanță și Avizare Juridică</b>	<b>Procedura operațională Privind asigurarea securității datelor cu caracter personal în Universitatea de Vest din Timișoara</b> <b>Cod: PO.UVT-GDPR-01</b>	<b>Ediția I</b>
		<b>Pagina 13 din 26</b>

sau personalului care operează/accesează acest sistem trebuie actualizată automat și de asemenea comunicată către DPO.

## 7.6. Conștientizarea și instruirea personalului UVT ce prelucrează date cu caracter personal

### 7.6.1. Conștientizarea personalului UVT privind importanța respectării GDPR

- Creșterea nivelului de conștientizare a fiecărui angajat/colaborator/voluntar din universitate (în calitate de prelucrător de date cu caracter personal), referitor la importanța implementării și respectării prevederilor GDPR în ceea ce privește protecția datelor cu caracter personal, constituie un principiu de bază în creșterea calității serviciilor oferite, precum și în desfășurarea activității profesionale în condiții de siguranță și confidențialitate.
- Acest proces se realizează ca urmare a identificării necesității de informare și instruire a personalului referitor la legislația în vigoare privind protecția datelor cu caracter personal.
- Fiecare angajat/colaborator/voluntar UVT are dreptul la informare și trebuie să cunoască politicile și procedurile interne ale UVT în acest domeniu, măsurile tehnice și organizatorice ce trebuie adoptate în activitatea profesională, în vederea conformării la prevederile GDPR.

### 7.6.2. Instruirea personalului UVT privind obligativitatea conformării la prevederile GDPR


#### 7.6.2.1. Planificarea instruirii

- Instruirea se realizează în scopul ridicării nivelului de cunoștințe și conștientizare privind obligativitatea implementării normelor GDPR în activitatea de prelucrare a datelor cu caracter personal.
- Planificarea instruirii se face de comun acord cu fiecare conducător de structură în parte, luând în considerare constrângerile ce se impun privind obligativitatea legală a instruirii, termenele, disponibilitatea și motivația fiecărei persoane care urmează să fie instruită.
- Metodele de instruire (instruirea internă, consilierea la locul de muncă, instruirea externă, autoinstruirea) se vor alege în funcție de necesarul constatat, resursele umane și financiare disponibile, obiectivele propuse și grupul țintă căruia se adresează.

#### 7.6.2.2. Procesul de instruire

- Instruirea internă – se realizează de către furnizori, angajați ai universității (cum ar fi DPO, angajați ai Direcției IT&C, conducătorul de structură în baza unei documentații primite etc.), într-o locație și cu un program bine stabilit anterior.
- Instruirea la locul de muncă – se realizează de către unul dintre furnizorii de instruire internă, dar are loc la cerere sau în funcție de necesitățile/neconformitățile punctuale constatate în urma etapelor de audit sau de către superiorul direct și este derulată la locul de muncă al angajatului, în timpul perioadei de desfășurare a activității profesionale.



 <b>Universitatea de Vest din Timișoara</b>  <b>Serviciul de Consultanță și Avizare Juridică</b>	<b>Procedura operațională Privind asigurarea securității datelor cu caracter personal în Universitatea de Vest din Timișoara</b>  <b>Cod: PO.UVT-GDPR-01</b>	<b>Ediția I</b>
		<b>Pagina 14 din 26</b>

- Autoinstruirea – se realizează în mod direct, de către fiecare angajat al universității, cu sprijinul DPO sau al conducătorului direct, dacă este cazul, și în baza documentației necesare în domeniul protecției datelor cu caracter personal puse la dispoziție de către universitate: legislație, metodologii, regulamente, proceduri operaționale, ghiduri de conformare la prevederile GDPR.
- Instruirea externă – se realizează de către furnizori de servicii externe, urmând ca astfel de sesiuni să fie planificate în urma constatării necesității și identificării resurselor financiare, numai cu aprobarea prealabilă a conducerii universității.

#### 7.6.2.3. Evaluarea, monitorizarea și îmbunătățirea procesului de instruire

- Scopul principal al evaluării și monitorizării este să se asigure că procesul de instruire și-a atins obiectivele propuse, privind conștientizarea angajatului referitor la obligativitatea implementării și respectării prevederilor GDPR în activitatea profesională.
- Evaluarea se face la finalul fiecărei instruirii, prin etapa de sumarizare și fixare a informațiilor furnizate în cadrul sesiunii de instruire.
- Monitorizarea rezultatelor instruirii se realizează pe tot parcursul activității angajatului, prin verificarea conformării la prevederile GDPR și intră în sarcina directă a conducătorilor de structură.
- Monitorizarea rezultatelor instruirii și a nivelului de pregătire în domeniul GDPR se realizează și prin procesul de audit intern periodic organizat de DPO, urmând ca fiecare neconformitate constatată să fie analizată și să fie luate măsuri corective, prin actualizarea informațiilor conținute în instruirile viitoare.

### 8. Responsabilități


#### 8.1. Rectorul Universității de Vest din Timișoara, în calitate de reprezentant legal al operatorului

- asigură implementarea și respectarea procedurii;
- identifică și alocă resursele necesare desfășurării în condiții de legalitate și siguranță a proceselor ce presupun colectarea și prelucrarea de date cu caracter personal în Universitatea de Vest din Timișoara;
- urmărește eficiența măsurilor de securizare a datelor cu caracter personal implementate în universitate și, în cazul în care sunt constatate riscuri sau vulnerabilități, solicită măsuri corective și participă, alături de ceilalți factori de decizie implicați, la implementarea acestora.

#### 8.2. Responsabilul DPO

- inițiază și execută procesul de constatare a situației curente din punct de vedere al stadiului respectării protecției datelor cu caracter personal în universitate, prin interviuri, întâlniri de lucru cu personalul din departamentele relevante;




 <b>Universitatea de Vest din Timișoara</b>  <b>Serviciul de Consultanță și Avizare Juridică</b>	<b>Procedura operațională Privind asigurarea securității datelor cu caracter personal în Universitatea de Vest din Timișoara</b>  <b>Cod: PO.UVT-GDPR-01</b>	<b>Ediția I</b>
		<b>Pagina 15 din 26</b>

- identifică procesele instituționale în care au loc activități de colectare și prelucrare a datelor cu caracter personal și sprijină structurile unde se derulează aceste procese în proiectarea și implementarea de măsuri tehnice și organizatorice de asigurare a protecției și confidențialității acestor tipuri de date;
- elaborează documente interne specifice GDPR (politici, proceduri, ghiduri de conformare) și actualizează, cu clauze privind securizarea datelor cu caracter personal, metodologii, regulamente, proceduri ale universității care interferează cu activități de colectare și prelucrare a datelor cu caracter personal;
- instruește personalul universității care, prin atribuțiile postului, prelucerează date cu caracter personal, dar și reprezentanții conducerii, cu privire la obligația legală a securizării datelor cu caracter personal ale tuturor categoriilor de persoane vizate, cu care intră în contact prin prisma proceselor instituționale;
- consiliază în mod constant conducerea universității cu privire la obligațiile ce îi revin în aplicarea prevederilor GDPR în cadrul fiecărui proces ce presupune colectare și prelucrare de date cu caracter personal;
- monitorizează și evaluează periodic, dar și în timpul activității curente a fiecărui angajat, implementarea și respectarea prevederilor GDPR privind asigurarea securității datelor cu caracter personal;
- informează conducerea UVT privind vulnerabilitățile și riscurile constatate cu privire la securizarea datelor cu caracter personal în universitate și propune măsuri tehnice și organizatorice pentru înlăturarea acestora;
- aduce la cunoștința conducerii universității orice posibilă breșă de securitate constatată, ce ar putea conduce la afectarea drepturilor și libertăților persoanelor vizate, în vederea identificării cauzelor și a minimizării riscurilor și limitării efectelor de diseminare neautorizată a datelor personale;
- elaborează și propune revizuirea acestei proceduri ori de câte ori se constată că este necesar.

### 8.3. Direcția IT&C - cu atribuții în domeniul tehnologiei și securizării informației

- propune și stabilește tipurile de acces pentru fiecare utilizator al sistemelor informatice din UVT, în concordanță cu atribuțiile ce îi revin prin fișa postului;
- asigură măsurile tehnice necesare pentru protejarea datelor cu caracter personal colectate și prelucrate în sistemele informatice ale universității, împotriva accesării, copierii sau divulgării neautorizate;
- actualizează și supraveghează, din punctul de vedere al securității, site-urile universității;
- identifică și informează factorii de conducere ai universității și DPO-ul cu privire la orice posibil risc ce ar conduce la o breșă de securitate a datelor cu caracter personal prelucrate în sistemele electronice ale universității și propune măsuri/resurse necesare remedierii;
- asigură măsurile necesare pentru identificarea rapidă a utilizatorului care a introdus, a actualizat, a modificat, șters sau divulgat accidental sau intenționat date cu caracter personal în sistemele electronice ale universității;



 <b>Universitatea de Vest din Timișoara</b> <b>Serviciul de Consultanță și Avizare Juridică</b>	<b>Procedura operațională Privind asigurarea securității datelor cu caracter personal în Universitatea de Vest din Timișoara</b> <b>Cod: PO.UVT-GDPR-01</b>	<b>Ediția I</b>
		<b>Pagina 16 din 26</b>

- este responsabil, alături de DPO, de instruirea pe partea tehnică a personalului universității care, prin atribuțiile postului, prelucrează date cu caracter personal, cu privire la obligația legală a securizării datelor cu caracter personal cu care intră în contact prin prisma atribuțiilor postului;
- aplică și respectă prevederile prezentei proceduri.

#### 8.4. Serviciul Consultanță și Avizare Juridică

- este responsabil în ceea ce privește asigurarea aplicării prevederilor GDPR în toate procesele cu care interacționează prin prisma avizului juridic (ex. contracte, acte adiționale, acorduri de colaborare, proceduri, metodologii, regulamente, fișe de post etc.) sau a activității specifice, cât și în orice documente ale universității ce presupun prelucrare de date cu caracter personal;
- informează DPO-ul privind orice neconformități constatate referitoare la protecția datelor cu caracter personal, în vederea identificării măsurilor necesare remedierii acestora.


#### 8.5. Decanul facultății/Directorul de departament/Conducătorul de structură administrativă de resort/Șeful de serviciu administrativ//Responsabilul de proces sau proiect

- răspunde pentru implementarea și respectarea prevederilor GDPR în activitatea structurii pe care o coordonează;
- asigură măsuri tehnice și organizatorice pentru respectarea confidențialității datelor cu caracter personal prelucrate la nivel de structură, cum ar fi: numirea unui responsabil, la nivel de structură, cu atribuții în păstrarea unei evidențe clare a tuturor prelucrărilor de date cu caracter personal la nivel de structură, semnarea Angajamentului de confidențialitate de către fiecare membru al personalului din structură ce colectează/prelucrează/accesază date cu caracter personal în îndeplinirea obligațiilor de serviciu, stocarea în condiții de siguranță a tuturor documentelor și înregistrărilor ce conțin date cu caracter personal, acordarea de permisiuni de acces la informații cu caracter personal doar personalului autorizat în îndeplinirea sarcinilor de serviciu etc.;
- informează DPO-ul privind orice neconformități constatate referitoare la protecția datelor cu caracter personal, în vederea identificării măsurilor necesare remedierii acestora;
- solicită instruirea personalului din subordine, ori de câte ori se constată necesitatea, în vederea respectării prevederilor GDPR;
- aplică și respectă prevederile prezentei proceduri.

#### 8.6. Utilizatori autorizați

- să păstreze confidențialitatea datelor cu caracter personal cu care intră în contact în îndeplinirea sarcinilor de serviciu, așa cum este prevăzut în Angajamentul de confidențialitate (Anexa nr. 1);




 <b>Universitatea de Vest din Timișoara</b> <b>Serviciul de Consultanță și Avizare Juridică</b>	<b>Procedura operațională Privind asigurarea securității datelor cu caracter personal în Universitatea de Vest din Timișoara</b>  <b>Cod: PO.UVT-GDPR-01</b>	<b>Ediția I</b>
		<b>Pagina 17 din 26</b>

- să cunoască și să aplice prevederile legale din domeniul prelucrării datelor cu caracter personal, puse la dispoziție de către Universitatea de Vest din Timișoara;
- să solicite superiorului ierarhic/DPO-ului informații/instruire în domeniul protecției datelor cu caracter personal ori de câte ori consideră necesar;
- să informeze superiorul direct/DPO-ul de fiecare dată când identifică un posibil risc asupra prelucrărilor de date cu caracter personal, ce ar putea conduce la o breșă de securitate, în vederea stabilirii cauzelor și a limitării efectelor de diseminare neautorizată;
- să aplice și să respecte prevederile prezentei proceduri.

## 9. Drepturile persoanelor vizate

- **Dreptul la transparența informațiilor, a comunicărilor și a modalităților de exercitare a drepturilor persoanei vizat.**
- **Dreptul de a fi informat cu privire la datele cu caracter personal proprii sau pentru care se justifică un interes.**
- **Dreptul de acces:** Persoana vizată are dreptul de a obține din partea UVT o confirmare că se prelucrează sau nu date cu caracter personal care o privesc și, în caz afirmativ, acces la datele respective.
- **Dreptul de rectificare:** Persoana vizată are dreptul de a obține de la UVT, fără întârzieri nejustificate, rectificarea datelor cu caracter personal inexacte care o privesc.
- **Dreptul la ștergerea datelor ("dreptul de a fi uitat"):** Persoana vizată are dreptul de a obține din partea UVT ștergerea datelor cu caracter personal care o privesc, fără întârzieri nejustificate.
- **Dreptul la restricționarea prelucrării:** Persoana vizată are dreptul de a obține din partea UVT restricționarea prelucrării în cazurile prevăzute de art. 18 RGPD. UVT comunică orice rectificare sau ștergere a datelor cu caracter personal sau restricționarea prelucrării.
- **Dreptul la portabilitatea datelor:** Persoana vizată are dreptul de a transmite către un alt operator datele furnizate către UVT.
- **Dreptul la opoziție:** Persoana vizată are dreptul să se opună prelucrării datelor cu caracter personal, în limita legislației în vigoare.
- **Dreptul de a nu face obiectul unei decizii bazate exclusiv pe prelucrarea automată** care produce efecte juridice care privesc persoana vizată sau o afectează în mod similar într-o măsură semnificativă.
- **Dreptul de a depune o plângere la Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal.**

 <b>Universitatea de Vest din Timișoara</b> <b>Serviciul de Consultanță și Avizare Juridică</b>	<b>Procedura operațională Privind asigurarea securității datelor cu caracter personal în Universitatea de Vest din Timișoara</b> <b>Cod: PO.UVT-GDPR-01</b>	<b>Ediția I</b>
		<b>Pagina 18 din 26</b>


#### 10. Date de contact ale DPO

- **E-mail:** gdpr@e-uvt.ro
- **Telefon:** +40757693806
- **Adresa:** Bulevardul Vasile Pârvan 4, Timișoara 300223, et. 1, cam. 119

#### 11. Anexe, înregistrări, arhivări

Nr. anexă	Denumirea anexei
0	1
1	Model Acord de confidențialitate și conformare la prevederile RGPD
2	Diagrama procesului de prelucrare a datelor cu caracter personal



 <p><b>Universitatea de Vest din Timișoara</b></p> <p><b>Serviciul de Consultanță și Avizare Juridică</b></p>	<p><b>Procedura operațională Privind asigurarea securității caracter personal în Universitatea de Vest din Timișoara</b></p> <p><b>Cod: PO.UVT-GDPR-01</b></p>	<p><b>Pagina 19 din 26</b></p>
--	--	--------------------------------

**Anexa nr. 1**

## **ACORD DE CONFIDENȚIALITATE ȘI CONFORMARE LA PREVEDERILE RGPD AL SALARIATULUI/COLABORATORULUI/VOLUNTARULUI UNIVERSITĂȚII DE VEST DIN TIMIȘOARA**

Domnul/doamna ....., domiciliat/domiciliată în localitatea ....., str. ...., nr. ...., județul ....., posesor/posesoare al/a cărții de identitate/pașaportului seria ....., nr. ...., eliberat/eliberată de ....., la data de ....., C.N.P. ...., în calitate de salariat/voluntar/colaborator la UNIVERSITATEA DE VEST DIN TIMIȘOARA (denumită în continuare operator de date cu caracter personal), CUI 4250670, cu sediul în Timișoara, Bld. Vasile Pârvan, nr. 4, Facultatea/Departamentul/Direcția/Serviciul ....., în conformitate cu Regulamentul general privind protecția datelor cu caracter personal 679/2016 (UE), se obligă să respecte prevederile acestui angajament.

### **I. OBIECTUL ANGAJAMENTULUI**


1.1. Informațiile și documentele, pe care le obține sau la care are acces salariatul/voluntarul/colaboratorul, ca efect al executării contractului de muncă, sunt strict confidențiale.

1.2. În conformitate cu Regulamentul general privind protecția datelor cu caracter personal 2016/679 (UE), art. 32, alin. (4), datele personale, la care salariatul/voluntarul/colaboratorul are acces, pot fi prelucrate numai dacă există un acord în acest sens, prin atribuțiile ce îi revin din fișa postului sau la cererea operatorului, cu excepția cazului în care există o obligație legală care să-i permită o astfel de prelucrare, în temeiul dreptului Uniunii sau al dreptului intern.

### **II. OBLIGAȚII**

2.1. În contextul paragrafului 1.1., salariatul/colaboratorul/voluntarul/colaboratorul are următoarele obligații:

- Să nu prelucreze date cu caracter personal cu care intră în contact decât în condițiile precizate la paragraful 1.2.;
- Să abordeze toate informațiile și documentele la care are acces, prin prisma atribuțiilor din fișa postului sau contractului individual de muncă, în condiții de strictă confidențialitate;
- Să nu divulge sub nicio formă (sau să permită divulgarea de către orice altă persoană) informații cu caracter confidențial sau documente cu caracter confidențial către terți, câtă vreme declarațiile privind operațiunile individuale nu sunt autorizate oficial;

 <b>Universitatea de Vest din Timișoara</b> <b>Serviciul de Consultanță și Avizare Juridică</b>	<b>Procedura operațională Privind asigurarea securității datelor cu caracter personal în Universitatea de Vest din Timișoara</b>  <b>Cod: PO.UVT-GDPR-01</b>	<b>Ediția I</b>
		<b>Pagina 20 din 26</b>

- Să nu utilizeze sau să permită utilizarea de către orice altă persoană a informațiilor cu caracter confidențial sau a oricărui document cu caracter confidențial pentru alte scopuri decât cele legate de atribuțiile sale în cadrul activității în Universitatea de Vest din Timișoara;
- Să distrugă documentele cu caracter confidențial care nu mai sunt folosite în activitatea profesională sau în scopuri de arhivare, în conformitate cu procedurile specifice ale Universității de Vest din Timișoara privind distrugerea materialelor confidențiale.

## 2.2. În înțelesul prezentului document, termenii folosiți au următoarele semnificații:


- Date cu caracter personal se referă la orice informații privind o persoană fizică identificată sau identificabilă (denumită generic „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 identifiant online, sau la unul sau mai multe elemente specifice, proprii identității sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale.
- Informațiile cu caracter confidențial se referă la toate informațiile, datele cu caracter personal și orice alte date/aspecte de care salariatul/voluntarul/colaboratorul ia cunoștință, direct sau indirect, ca rezultat al participării sale la activitățile Universității de Vest din Timișoara și care nu se încadrează în categoria informațiilor de interes public, așa cum sunt ele definite în Legea nr. 544/2001 privind liberul acces la informațiile de interes public.
- Documentele cu caracter confidențial se referă la toate documentele pe suport de hârtie sau în format electronic și orice alte materiale cu caracter pregătitor, împreună cu toate informațiile conținute în acestea, la care salariatul/voluntarul are acces, direct sau indirect, ca rezultat al participării sale la activitățile din cadrul Universității de Vest din Timișoara.

În plus, toate înregistrările sau însemnările efectuate de salariat/voluntar/colaborator referitoare la informațiile cu caracter confidențial sau la documentele cu caracter confidențial vor fi de asemenea considerate documente cu caracter confidențial.

## III. DURATA ANGAJAMENTULUI

3.1. Prezentul angajament de confidențialitate se aplică pe întreaga perioadă contractuală, cu precizarea că obligațiile de păstrare a confidențialității continuă și după încetarea perioadei contractuale/a raporturilor de muncă dintre semnatar și Universitatea de Vest din Timișoara.



 <p><b>Universitatea de Vest din Timișoara</b></p> <p><b>Serviciul de Consultanță și Avizare Juridică</b></p>	<p><b>Procedura operațională Privind asigurarea securității datelor cu caracter personal în Universitatea de Vest din Timișoara</b></p> <p><b>Cod: PO.UVT-GDPR-01</b></p>	<p><b>Ediția I</b></p> <hr/> <p><b>Pagina 21 din 26</b></p>
--	---	---

#### IV. RĂSPUNDEREA CONTRACTUALĂ

4.1. Încălcarea prevederilor privind confidențialitatea se pedepsește conform art. 83, alin.(4) și (5) din GDPR și ale altor dispoziții legale în vigoare. Orice persoană care a suferit daune materiale sau morale în urma încălcării confidențialității datelor are dreptul să solicite daune de la persoana responsabilă de încălcarea acestui drept sau de la operatorul sau persoana împuternicită care a executat operațiunea.

4.2. Următoarele situații exonerează de răspundere salariatul/voluntarul/colaboratorul:

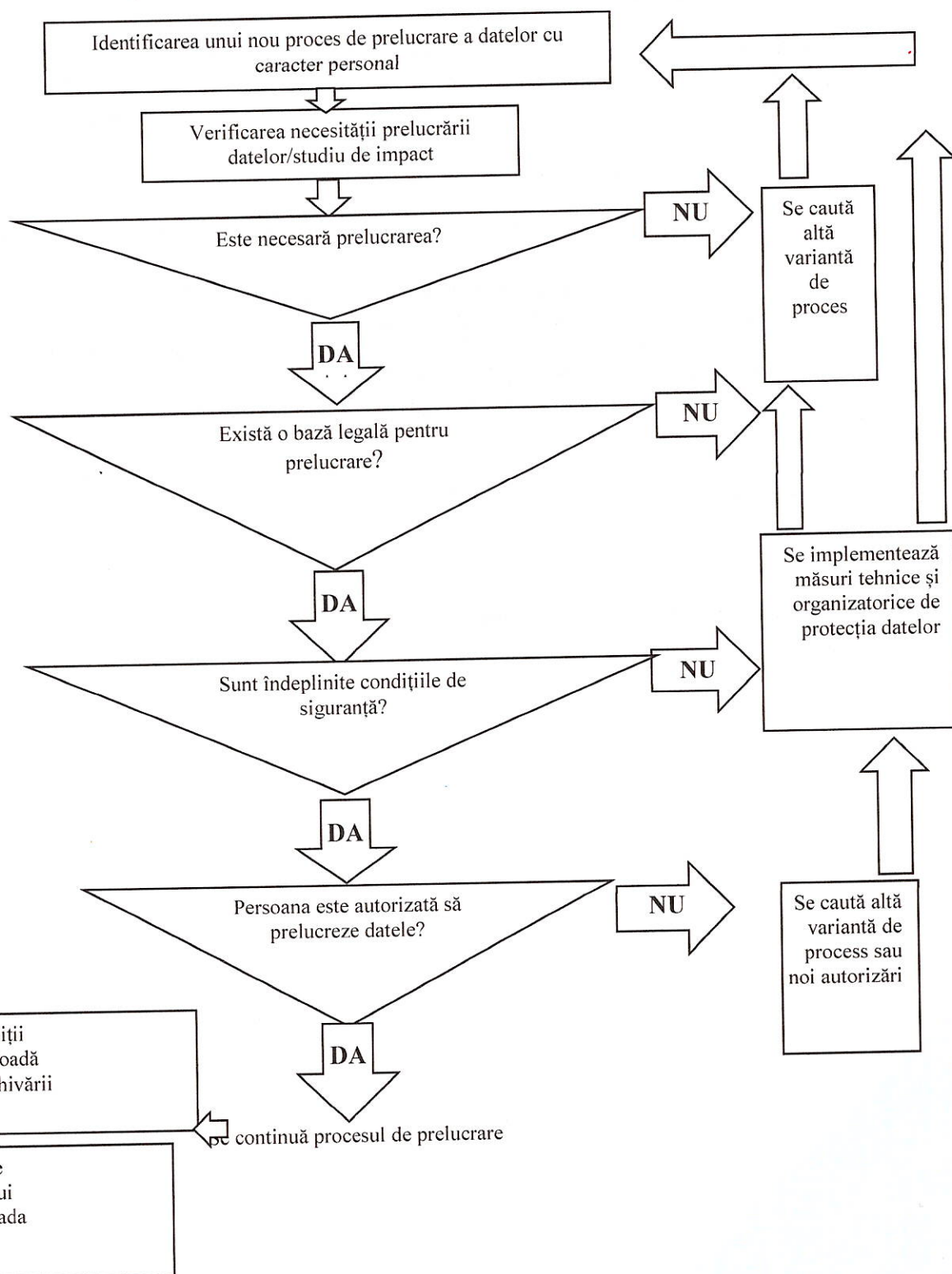
- informațiile erau cunoscute înainte de a fi obținute de la angajator;
- informația provine dintr-o sursă neconfidențială;
- dezvăluirea informației s-a făcut după primirea acordului scris pentru aceasta;
- informația era publică la data dezvăluirii ei;
- salariatul/voluntarul/colaboratorul a fost obligat în mod legal să dezvăluie informația.

Subsemnatul/ă ....., confirm că am luat la cunoștință și voi respecta prevederile prezentului Angajament de confidențialitate și conformare GDPR.


Semnătura salariatului/voluntarului,  
Data,

**Diagrama procesului**

Anexa 2






 <b>Serviciul de Consultanță și Avizare Juridică</b>	<b>Procedura operațională Privind asigurarea securității datelor cu caracter personal în Universitatea de Vest din Timișoara</b>  <b>Cod: PO.UVT-GDPR-01</b>	<b>Ediția I</b>
		<b>Pagina 23 din 26</b>

## 12. Lista de difuzare

Nr. Crt.	Structură	Nume și prenume	Data primirii	Semnatura	Data retragerii	Semnatura
1	Cabinet Rector					
2	Cancelaria Rectorului					
3	Compartimentul Audit Public Intern					
4	Consiliul de Studii Universitare de Doctorat					
5	Departamentul pt. Pregătire a Personalului					
5	Didactic					
6	Direcția Comunicare, Imagine și Marketing					
6	Instituțional					
7	Direcția Digitalizare și Analiza Date					
8	Direcția Economico-Financiar					
9	Direcția Evidența patrimoniu, achiziții și monitorizare investiții					
10	Direcția General Administrativă					
11	Direcția IT&C					
12	Direcția Management Educațional					
13	Direcția Managementul Activităților CDI					
14	Direcția Parteneriate Instituționale și Finanțări					
14	Nerambursabile					
15	Direcția Relații Internaționale					
16	Direcția Resurse Umane					
17	Direcția Secretariat General					
18	Facultatea de Arte și Design					
19	Serviciul Administrare și Gestiune Cămine					
20	Serviciul Administrativ					
21	Serviciul Consultanță și Avizare Juridică					
22	Serviciul Corp de Control Intern					
23	Serviciul Tipografie					
24	Facultatea de Chimie, Biologie, Geografie					
20	Facultatea de Drept					
21	Facultatea de Economie și de Administrare a Afacerilor					
22	Facultatea de Educație Fizică și Sport					


- |    |   |
|----|---|
| 23 | Facultatea de Fizică                          |
|    | Facultatea de Litere, Istorie, Filosofie și   |
| 24 | Teologie                                      |
| 25 | Facultatea de Matematică și Informatică       |
| 26 | Facultatea de Muzică și Teatru                |
| 27 | Facultatea de Sociologie și Psihologie        |
|    | Facultatea de Științe ale Guvernării și       |
| 28 | Comunicării                                   |
|    | Institutul pentru Cercetări Avansate de Mediu |
| 29 | (ICAM)  |



 <b>Serviciul de Consultanță și Avizare Juridică</b>	<b>Procedura operațională Privind asigurarea securității datelor cu caracter personal în Universitatea de Vest din Timișoara</b>  <b>Cod: PO.UVT-GDPR-01</b>	<b>Ediția I</b>
		<b>Pagina 25 din 26</b>

### 13. Cuprins

1. Lista responsabililor cu elaborarea, verificarea și aprobarea ediției sau, după caz, a reviziei în cadrul ediției procedurii operaționale .....	2
2. Formular de evidență a modificărilor .....	3
3. Scopul procedurii .....	3
4. Domeniul de aplicare .....	4
5. Documente de referință.....	5
5.1. Externe:.....	5
5.2. Interne: .....	5
6. Definiții și abrevieri.....	5
6.1. Definiții .....	5
6.2. Abrevieri .....	6
7. Descriere procedură .....	7
7.1. Prevederi generale .....	7
7.2. Colectarea datelor cu caracter personal .....	7
7.3. Prelucrarea datelor cu caracter personal .....	8
7.4. Păstrarea datelor cu caracter personal.....	9
7.5. Accesarea și administrarea înregistrărilor și bazelor de date cu caracter personal.....	9
7.5.1. Accesul și administrarea documentelor ce conțin date cu caracter personal, stocate/arhivate în format fizic .....	10
7.5.2. Accesul și administrarea datelor cu caracter personal/bazelor de date stocate electronic.....	10
7.5.3. Accesarea și administrarea înregistrărilor sistemelor de supraveghere video .....	12
7.6. Conștientizarea și instruirea personalului UVT ce prelucrează date cu caracter personal .....	13
7.6.1. Conștientizarea personalului UVT privind importanța respectării GDPR .....	13
7.6.2. Instruirea personalului UVT privind obligativitatea conformării la prevederile GDPR ....	13
7.6.2.1. Planificarea instruirii .....	13
7.6.2.2. Procesul de instruire .....	13
7.6.2.3. Evaluarea, monitorizarea și îmbunătățirea procesului de instruire.....	14
8. Responsabilități.....	14

 <b>Universitatea de Vest din Timișoara</b> <b>Serviciul de Consultanță și Avizare Juridică</b>	<b>Procedura operațională Privind asigurarea securității datelor cu caracter personal în Universitatea de Vest din Timișoara</b> <b>Cod: PO.UVT-GDPR-01</b>	<b>Ediția I</b>
		<b>Pagina 26 din 26</b>

8.1. Rectorul Universității de Vest din Timișoara, în calitate de reprezentant legal al operatorului.....	14
8.2. Responsabilul DPO.....	14
8.3. Direcția IT&C - cu atribuții în domeniul tehnologiei și securizării informației.....	15
8.4. Serviciul Consultanță și Avizare Juridică.....	16
8.5. Decanul facultății/Directorul de departament/Conducătorul de structură administrativă de resort/Șeful de serviciu administrativ//Responsabilul de proces sau proiect.....	16
8.6. Utilizatori autorizați.....	16
9. Drepturile persoanelor vizate.....	17
10. Date de contact DPO .....	18
10. Anexe și formulare .....	19-22
11. Lista de difuzare .....	23
12. Cuprins.....	26