


<p>UNIVERSITATEA DIN PITEȘTI</p>  <p>COMPARTIMENT GDPR</p>	<p>PROCEDURĂ OPERAȚIONAL PRIVIND ASIGURAREA SECURITĂȚII DATELOR CU CARACTER PERSONAL ÎN UNIVERSITATEA DIN PITEȘTI</p> <p>COD: PO-GDPR-01</p>	Ediția 1
		Revizia 0
		Nr. de ex.: 2
		Nr. pagini: 21
		Exemplar nr. 1

AVIZAT,
În edința Consiliului de Administrație
din data de 07.12.2022


APROBAT,
În edința Senatului
din data de 19.12.2022

RECTOR,
Conf. univ. dr. ing. Dumitru CHIRLEAN

PREȘEDINTELE SENATULUI,
Prof. univ. dr. Mihaela DIACONU

**PROCEDURĂ OPERAȚIONAL
PRIVIND
ASIGURAREA SECURITĂȚII DATELOR CU CARACTER PERSONAL ÎN
UNIVERSITATEA DIN PITEȘTI**

COD: PO-GDPR-01


	PROCEDURĂ OPERA IONAL PRIVIND ASIGURAREA SECURIT II DATELOR CU CARACTER PERSONAL ÎN UNIVERSITATEA DIN PITE TI	Edi ia 1
	COD: PO-GDPR-01	Revizia 0

1. LISTA RESPONSABILILOR CU ELABORAREA, VERIFICAREA I APROBAREA EDI IEI

Nr. crt.	Elemente privind responsabilit i/ opera iuni	Responsabili cu elaborarea/verificarea edi iei	Func ia	Data	Semn tura
1.	Elaborare	Petruta RIZEA	Responsabil cu protec ia datelor cu caracter personal	12.10.2022	
2.	Verificare	Prof.univ.dr. Ionela NICULESCU	Director CMCPU	12.10.2022	
3.	Aviz juridic	C.j. Elena MATEESCU	Director Dir. Juridic	12.10.2022	
4.	Avizat comisie monitorizare	Prof.univ.dr. ing. Viorel NICOLAE	Pre edintele Comisiei de monitorizare	12.10.2022	
5.	Avizat Comisia nr. 2 a Senatului	Conf. univ. dr. Monica POPESCU	Pre edintele Comisiei nr. 2 a Senatului	16.10.2022	
6.	Avizat Secretar General al Senatului	Lect. univ. dr. Ramona DUMINIC	Secretar General al Senatului	19.12.2022	

2. SITUAȚIA EDIȚIILOR I REVIZIILOR ÎN CADRUL EDIȚIILOR PROCEDURII

Nr. crt.	Revizia / Data aplic rii	Num rul capitolului i paginilor revizuite	Conținutul modific rii	Nume i prenume			
				Elaborat	Verificat	Avizat	Aprobat
1							
2							
3							

	PROCEDURĂ OPERAȚIONALĂ PRIVIND ASIGURAREA SECURITĂȚII DATELOR CU CARACTER PERSONAL ÎN UNIVERSITATEA DIN PITEȘTI	Ediția 1
	COD: PO-GDPR-01	Revizia 0

3. 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 din Pitești.

4. DOMENIUL DE APLICARE

Procedura se aplică de către tot personalul, titular sau asociat al Universității din Pitești, 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 din 18 iulie 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 din 17 noiembrie 2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice**
- **Decizii ale Autorității Naționale pentru Protecția datelor**
- **Legea Educației Naționale nr. 1/2011, cu modificările ulterioare**

5.2. Interne:


- **Carta Universității din Pitești**
- **Regulament de organizare și funcționare a Universității din Pitești**
- **Regulament intern al Universității din Pitești**

	PROCEDURĂ OPERAȚIONALĂ PRIVIND ASIGURAREA SECURITĂȚII DATELOR CU CARACTER PERSONAL ÎN UNIVERSITATEA DIN PITEȘTI COD: PO-GDPR-01	Ediția 1
		Revizia 0

6. DEFINIȚII ȘI ABREVIERI

6.1. Definiții

Nr. Crt.	Termenul	Definiția
1.	Date cu caracter personal	Orice informații privind o persoană fizică identificată sau identificabilă (persoană vizată).
2.	Încălcare a 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.
3.	Persoane vizate	Persoanele ale căror date cu caracter personal sunt colectate și prelucrate.
4.	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 combinarea, restricționarea, tergerea ori distrugerea.
5.	Operator	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 – în cazul de față Universitatea din Pitești.
6.	Persoană împuternicită de operator	Persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care prelucrează datele cu caracter personal în numele operatorului.
7.	Parte ter	Persoana fizică sau juridică, autorizată să prelucreze date cu caracter personal.

	<p style="text-align: center;">PROCEDURĂ OPERAȚIONALĂ PRIVIND ASIGURAREA SECURITĂȚII DATELOR CU CARACTER PERSONAL ÎN UNIVERSITATEA DIN PITEȘTI</p> <p style="text-align: center;">COD: PO-GDPR-01</p>	Ediția 1
		Revizia 0

Nr. Crt.	Termenul	Definiția
8.	Destinatar	Persoana fizică sau juridică, autoritatea publică, agenția sau alt organism creia (caruia) îi sunt transmise/divulgate datele cu caracter personal, indiferent dacă este sau nu o parte terță.
9.	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.


6.2. Abrevieri

Nr. Crt.	Abrevierea	Termenul abreviat
1.	UPIT	Universitatea din Pitești
2.	P.O.	Procedură operațională
3.	GDPR	Regulamentul 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 și de abrogare a Directivei 95/46 CE
4.	DPO	Responsabil cu protecția datelor cu caracter personal
5.	ANSPDCP	Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal

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).

	<p style="text-align: center;">PROCEDURĂ OPERA IONAL PRIVIND ASIGURAREA SECURIT II DATELOR CU CARACTER PERSONAL ÎN UNIVERSITATEA DIN PITE TI</p> <p style="text-align: center;">COD: PO-GDPR-01</p>	Edi ia 1
		Revizia 0

Procedura descrie condi iile i cerin ele obligatorii ce trebuie respectate în procesele institu ionale de prelucrare a datelor, în vederea asigurarii 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 a unei persoane sau categorii de persoane vizate, chiar dac aceasta presupune doar colectarea datelor în procesul de admitere sau de recrutare, stocarea datelor, utilizarea unui nou instrument on-line, dezvoltarea unei activit i de marketing direct din partea universit ii, un nou proiect, o conferin sau un eveniment organizat în cadrul universit ii sau orice alt nou proces de prelucrare a datelor cu caracter personal în cadrul UPIT, fiecare operator trebuie s își pun urm toarele întreb ri:


- ✓ Sigur este nevoie s fie colectat această informa ie?
- ✓ Exist o baz legal pentru prelucrare (cum ar fi consim mântul persoanei vizate, interesul legitim al universit ii pentru îndeplinirea unor clauze precontractuale sau în vederea derul rii unui contract deja existent, obliga ii legale ce îi revin universit ii)?
- ✓ Datele colectate pot fi anonimizate sau pseudonimizate?
- ✓ Datele personale vor fi prelucrate în condi ii de siguran ?
- ✓ Datele personale vor fi transmise c tre o alt parte pentru a fi prelucrate (c tre o persoan împuternicit de c tre UPIT)?
- ✓ Este planificat ca datele colectate s fie transferate c tre o ar non-UE? Dac da, exist un set adecvat de m suri de securitate implementat în ara respectiv ?
- ✓ Exist alt alternativ de îndeplinire a activit ii respective, f r a fi necesar prelucrarea sau transferarea datelor personale?

Dac în urma analizei punctelor de mai sus se constata necesitatea colectării acelor categorii de date cu caracter personal în structura respectiv a universit ii, în vederea prelucrării, atunci utilizatorul datelor cu caracter personal trebuie s se conformeze la prevederile Regulamentului 679/2016 (UE).

- Este important s se analizeze necesitatea unui studiu de impact de câte ori apar noi activit i de colectare a datelor în procesele existente sau sunt identificate noi procese ce presupun colectarea de date cu caracter personal.
- GDPR impune aplicarea unor m suri de confiden ialitate înc de la crearea acestor procese („by design”), dar i pe parcursul desf ur rii activit ilor („by default”).
- Colectarea datelor cu caracter personal este permis numai utilizatorilor autoriza i în acest sens, în îndeplinirea obliga iilor de serviciu prev zute prin fi a postului.

7.3. Prelucrarea datelor cu caracter personal


- Prin prelucrarea datelor se în elege, în mod sumar, orice opera iune efectuat asupra datelor cu caracter personal cum ar fi: colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, divulgarea prin transmitere, diseminarea sau punerea la dispozi ie în orice alt mod, alinierea sau combinarea, restric ionarea, tergerea ori distrugerea.

	PROCEDURĂ OPERAȚIONALĂ PRIVIND ASIGURAREA SECURITĂȚII DATELOR CU CARACTER PERSONAL ÎN UNIVERSITATEA DIN PITEȘTI	Ediția 1
	COD: PO-GDPR-01	Revizia 0

- Datele trebuie să fie prelucrate într-un mod care asigură securitatea adecvată a acestora, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luarea de măsuri tehnice și organizatorice corespunzătoare (principiul „integritate și confidențialitate”).
- Conducătorii tuturor structurilor din UPIT 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 funcția postului.
- La nivel de fiecare structură 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, de înregistrate sau create în timpul executării sarcinilor de serviciu.
- Datele cu caracter personal vor fi prelucrate exclusiv în scopul pentru care au fost colectate.
- Modificările necesare a fi aduse datelor cu caracter personal se fac doar de către personalul 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 indisponibil 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 poate să își reia activitatea, accesul persoanei de back-up să fie restricționat.
- În cazul în care se întrerupe sau se suspendă contractul individual de muncă cu universitatea sau angajatul este mutat într-un alt loc de muncă, unde atribuțiile de serviciu specificate în funcția postului nu mai presupun prelucrarea datelor cu caracter personal de la fostul loc, este obligatoriu să se revoce imediat accesul acestuia la bazele de date.

7.4. Protecția 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 "limitări 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 dacă au fost stocate electronic pe un server al instituției, pe PC-le personale,

	PROCEDURĂ OPERAȚIONALĂ PRIVIND ASIGURAREA SECURITĂȚII DATELOR CU CARACTER PERSONAL ÎN UNIVERSITATEA DIN PITEȘTI	Ediția 1
	COD: PO-GDPR-01	Revizia 0

echipamente mobile sau pe suport de hârtie. Înregistrările pe hârtie trebuie să fie fragmentate în de euri, iar înregistrările electronice trebuie terse definitiv.

- Fiecare structură organizatorică din cadrul Universității din Pitești este responsabil de stabilirea și asigurarea perioadelor corespunzătoare de păstrare a informațiilor cu caracter personal pe care le administrează, în condiții de siguranță în baza legislației de arhivare în vigoare, coroborat 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”.
- 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 Angajament de confidențialitate (Anexa nr. 1) trebuie semnat de către fiecare persoană (angajat/colaborator/voluntar UPIT) 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/zonelor în care sunt stocate sau arhivate documente ce conțin date cu caracter personal este strict permis doar persoanelor autorizate de către conducătorii structurilor din UPIT, 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 lăsararea documentelor neasigurate pe birouri, în imprimante, ci acestea trebuie depozitate în dulapuri încuiate, 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 din prisma sarcinilor de serviciu pentru care angajatul a fost autorizat.
- Este interzisă scoaterea din perimetrul UPIT 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, 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

	PROCEDURĂ OPERAȚIONALĂ PRIVIND ASIGURAREA SECURITĂȚII DATELOR CU CARACTER PERSONAL ÎN UNIVERSITATEA DIN PITEȘTI	Ediția 1
	COD: PO-GDPR-01	Revizia 0

utilizator și nu vor fi comunicate altor persoane neautorizate, 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 imprimeze 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. Este obligatorie setarea funcției de „screen-saver”, cu un interval de temporizare de maxim 5 minute. În același 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 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 UPIT, în calitate de utilizatori, trebuie să fie salvate în siguranță și să se creeze copii (back-up), iar intervalul de timp la care se execută acestea și locația unde vor fi salvate se va stabili de către conducătorii de structură, în funcție de importanța și volumul acestor informații. Controlul și responsabilitatea acestei acțiuni este în sarcina fiecărui conducător de structură, cu menținerea acestui interval 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 din Pitești (domeniul *upit.ro*).
- Nu este permisă trimiterea prin e-mail, către un cont extern de domeniul UPIT, 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 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 din Pitești sau care conțin date personale, folosind conturi de utilizator e-mail configurate pe servere care nu sunt proprietate UPIT (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 aliniatei anterioare, dacă universitatea, în calitate de persoană juridică sau un salariat al universității, obține în mod direct adresa de poștă

	PROCEDURĂ OPERA IONAL PRIVIND ASIGURAREA SECURIT II DATELOR CU CARACTER PERSONAL ÎN UNIVERSITATEA DIN PITE TI	Edi ia 1
	COD: PO-GDPR-01	Revizia 0

electronic a unui candidat/student/elev/angajat/colaborator/alt categorie de persoan vizat , de exemplu cu ocazia particip rii la un concurs/furniz rii serviciilor educa ionale/particip rii într-un proiect sau la un eveniment organizat de universitate, în conformitate cu prevederile GDPR, persoana fizic sau juridic în cauz poate utiliza adresa respectiv , în scopul efectu rii de comunic ri viitoare de marketing referitoare la servicii educa ionale/proiecte/evenimente similare, cu condi ia de a oferi în mod clar i expres persoanelor vizate posibilitatea de a se opune printr-un mijloc simplu i gratuit unei asemenea utiliz ri (de ex. prin trimiterea unui email), atât la ob inerea adresei de po t electronic , cât i cu ocazia fiec rui mesaj, în cazul în care clientul nu s-a opus ini ial.

7.5.3. Accesarea i administrarea înregistr rilor sistemelor de supraveghere video

- UPIT utilizeaz subsistemul de supraveghere video pentru asigurarea securit ii i 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 împreun un sistem integrat de securitate fizic . Astfel, subsistemele de supraveghere video funcționeaz în relație de colaborare cu celelalte subsisteme enumerate mai sus, asigurând elementul de monitorizare în timp real i posibilitatea de vizualizare post-eveniment precum i înregistrarea, afi area i transmisia video c tre diverse persoane desemnate ca utilizatori ai subsistemului de supraveghere.
- UPIT are obliga ia de a administra, în condi ii de siguran i numai pentru scopul specificat, datele personale colectate prin intermediul sistemelor de supraveghere video. UPIT nu va prelucra datele personale decât în m sura în care acest demers este necesar îndeplinirii scopului mai sus men ionat, cu respectarea m surilor legale de securitate i confiden ialitate a datelor.
- Durata de stocare a datelor ob inute prin intermediul sistemului de supraveghere video este de 30 de zile, cu excep ia situa iilor expres reglementate de lege sau a cazurilor temeinic justificate. La expirarea termenului, înregistr rile se distrug sau se terg.
- Personalul de paz /administrare/service a acestor Sisteme de supraveghere, sub atenta supraveghere a conduc torilor structurilor din cadrul Direc iei Generale Administrative/C.T.I.C.I. va verifica periodic i va r sponde de siguran a i confiden ialitatea datelor personale stocate în sistemul de supraveghere/monitorizare video. Angajamentul de confiden ialitate (Anexa nr. 1) va fi semnat de c tre fiecare salariat/colaborator/operator ce intr în contact cu sistemele de supraveghere video, prin prisma sarcinilor de serviciu, ca m sur ce demonstreaz instruirea i respectarea confiden ialit ii datelor cu caracter personal.
- Operatorii autoriza i ai sistemelor de supraveghere video trebuie s se asigure c nu permit accesul în spa iile de vizualizare sau stocare a imaginilor/înregistr rilor video niciunei persoane neautorizate i c nu vor comunica în mod accidental sau inten ionat înregistr ri c tre al i destinatari, f r acordul conduc torului ierarhic i un temei legal bine stabilit.
- O eviden clar a disponerii sistemului de supraveghere video i a personalului care opereaz /acceseaz înregistr rile trebuie s fie p strat la nivelul Direc iei Generale Administrative i comunicat c tre Responsabilul cu protec ia datelor cu caracter personal al universit ii (DPO). Orice modificare adus sistemului de supraveghere video

	<p style="text-align: center;">PROCEDURĂ OPERAȚIONALĂ PRIVIND ASIGURAREA SECURITĂȚII DATELOR CU CARACTER PERSONAL ÎN UNIVERSITATEA DIN PITEȘTI</p> <p style="text-align: center;">COD: PO-GDPR-01</p>	Ediția 1
		Revizia 0

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

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

7.6.1. Conștientizarea personalului UPIT 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 UPIT are dreptul la informare și trebuie să cunoască politicile și procedurile interne ale UPIT în acest domeniu, măsurile tehnice și organizatorice ce trebuie adoptate în activitatea profesională, în vederea conformării la prevederile GDPR.


7.6.2. Instruirea personalului UPIT privind obligativitatea conformării la prevederile GDPR

7.6.2.1. Planificarea instruirii

- Instruirea se realizează în scopul ridicării nivelului de cunoștințe, de 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 constat, resursele umane și financiare disponibile, obiectivele propuse, grupul țintă la care se adresează.

7.6.2.2. Procesul de instruire

- *Instruirea internă* –se realizează de către furnizori, angajații universității (cum ar fi DPO, reprezentant al centrului T.I.C.I., 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 derulat la locul de muncă al angajatului, în timpul perioadei de desfășurare a activității profesionale.
- *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 pusă la dispoziție de către

	PROCEDURĂ OPERAȚIONALĂ PRIVIND ASIGURAREA SECURITĂȚII DATELOR CU CARACTER PERSONAL ÎN UNIVERSITATEA DIN PITEȘTI	Ediția 1
	COD: PO-GDPR-01	Revizia 0

universitate: legislație, metodologii, regulamente, proceduri operaționale, ghiduri de conformare la prevederile GDPR.

- *Instruirea extern* –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 fixarea informațiilor furnizate în cadrul sesiunii de instruire.
- Monitorizarea rezultatelor instruirii se realizează pe tot parcursul activității angajatului, prin verificarea conformității la prevederile GDPR și intră în sarcina directoarelor 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 din Pitești, 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 din Pitești;
- urmărește eficienta măsurilor de securizare a datelor cu caracter personal implementate în universitate, în cazul în care sunt constatate riscuri sau vulnerabilități, solicitând măsuri corective și participând, 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;
- 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;
- instruiște personalul universității care, prin atribuțiile postului, prelucrează date cu caracter personal, dar și reprezentanții conducerii, cu privire la obligația legală

	PROCEDURĂ OPERA IONALĂ PRIVIND ASIGURAREA SECURITĂȚII DATELOR CU CARACTER PERSONAL ÎN UNIVERSITATEA DIN PITEȘTI	Ediția 1
	COD: PO-GDPR-01	Revizia 0

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 colectarea 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 UPIT 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 cunoștință a 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. Centrul T.I.C.I. –cu atribuții în domeniul tehnologiei și securizării informației

- propune și stabilește tipurile de acces pentru fiecare utilizator al sistemelor informatice din UPIT, 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, ters sau divulgat accidental sau intenționat date cu caracter personal în sistemele electronice ale universității;
- 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. Direcția 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.

	PROCEDURĂ OPERAȚIONALĂ PRIVIND ASIGURAREA SECURITĂȚII DATELOR CU CARACTER PERSONAL ÎN UNIVERSITATEA DIN PITEȘTI	Ediția 1
	COD: PO-GDPR-01	Revizia 0

- aplică și respectă prevederile prezentei proceduri.

8.5. Decanul facultății/Directorul de departament/Conducătorul de structură administrativă de resort/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 pstrarea 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/accesează 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 pstreze confidențialitatea datelor cu caracter personal cu care într în contact în îndeplinirea sarcinilor de serviciu, așa cum este prevăzut în Angajamentul de confidențialitate (Anexa nr. 1);
- să cunoască și să aplice prevederile legale din domeniul prelucrării datelor cu caracter personal, puse la dispoziție de către Universitatea din Pitești;
- 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;
- aplică și respectă prevederile prezentei proceduri.

9. DATE DE CONTACT ALE DPO

- **Nume:** Rizea Petru a Mihaela
- **Adresă corespondență:** Universitatea din Pitești, str. Târgu din Vale nr.1, Rectorat
- **Număr de telefon:** 0348/453121
- **Adresă de email:** responsabil.gdpr@upit.ro

10. ANEXE ȘI FORMULARE

- Anexa 1 - F01-PO-GDPR-01- Angajamentul de confidențialitate și conformare la prevederile GDPR al salariatului/voluntarului Universității din Pitești.
- Anexa 2 - Diagrama procesului.

	<p style="text-align: center;">PROCEDURĂ OPERA IONAL PRIVIND ASIGURAREA SECURIT II DATELOR CU CARACTER PERSONAL ÎN UNIVERSITATEA DIN PITE TI</p> <p style="text-align: center;">COD: PO-GDPR-01</p>	Edi ia 1
		Revizia 0

F01-PO-GDPR-01

Anexa nr. 1



MINISTERUL EDUCA IEI
UNIVERSITATEA DIN PITE TI
Str. Târgul din Vale, Nr. 1, Cod po tal 110040 - Pite ti, Jud. Arge
Tel./ Fax: +40 348 453 100/123, www.upit.ro



ANGAJAMENTUL DE CONFIDEN IALITATE I CONFORMARE LA PREVEDERILE GDPR AL SALARIATULUI/VOLUNTARULUI UNIVERSIT II DIN PITE TI

Domnul/doamna....., domiciliat/domiciliat în localitatea....., str. nr., jude ul....., posesor/poseoare al/a buletinului/c r ii de identitate/pa aportului seria, nr., eliberat/eliberat de, la data de....., C.N.P....., **în calitate de salariat/voluntar la UNIVERSITATEA DIN PITE TI** (denumit în continuare **operator** de date cu caracter personal), CUI 4122183, cu sediul în str. Târgu din Vale, nr. 1, Pite ti, Departamentul/Serviciul....., în conformitate cu Regulamentul general privind protec ia datelor cu caracter personal 679/2016 (UE), se oblig s respecte prevederile acestui **angajament**.

I. OBIECTUL ANGAJAMENTULUI


1.1 Informa iile i documentele, pe care le ob ine sau la care are acces salariatul/voluntarul, ca efect al execut rii contractului de munc , sunt strict confiden iale.

1.2. În conformitate cu Regulamentul general privind protec ia datelor cu caracter personal 2016/679 (UE), art. 32, alin. (4), datele personale, la care salariatul/voluntarul are acces, pot fi prelucrate numai dac exist un acord în acest sens, prin atribu iile ce îi revin din fi a postului sau la cererea operatorului, cu excep ia cazului în care exist o obliga ie legal care s -i permit o astfel de prelucrare, în temeiul dreptului Uniunii sau al dreptului intern,

II. OBLIGA II

2.1. În contextul paragrafului 1.1., salariatul/voluntarul are urm toarele obliga ii:

- S nu prelucreze date cu caracter personal cu care intr în contact decât în condi iile precizate la paragraful 1.2.;
- S abordeze toate informa iile i documentele la care are acces, prin prisma atribu iilor din fi a postului sau contractului individual de munc , în condi ii de strict confiden ialitate;
- S nu divulge sub nici o form (sau s permit divulgarea de c tre orice alt persoan) informa ii cu caracter confiden ial sau documente cu caracter confiden ial c tre ter i, cât vreme declara iile privind opera iunile individuale nu sunt autorizate oficial;
- S nu utilizeze sau s permit utilizarea de c tre orice alt persoan a informa iilor cu caracter confiden ial sau a oric rui document cu caracter confiden ial pentru alte scopuri decât cele legate de atribu iile sale în cadrul activit ii în Universitatea din Pite ti;

	PROCEDURĂ OPERAȚIONALĂ PRIVIND ASIGURAREA SECURITĂȚII DATELOR CU CARACTER PERSONAL ÎN UNIVERSITATEA DIN PITEȘTI	Ediția 1
	COD: PO-GDPR-01	Revizia 0

- 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 din Pitești 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 (denumit 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 identificator 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 ia cunoștință, direct sau indirect, ca rezultat al participării sale la activitățile Universității din Pitești 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 din Pitești.

În plus, toate înregistrările sau însemnările efectuate de salariat/voluntar 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 din Pitești.

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.

În funcție de natura încălcării, se pot impune amenzi de până la 10 sau 20 milioane de euro, sau de până la 4% din cifra totală anuală de afaceri a operatorului.

4.2. Următoarele situații exonerează de răspundere salariatul/voluntarul:

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

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

	PROCEDURĂ OPERAȚIONALĂ PRIVIND ASIGURAREA SECURITĂȚII DATELOR CU CARACTER PERSONAL ÎN UNIVERSITATEA DIN PITEȘTI COD: PO-GDPR-01	Ediția 1
		Revizia 0

Semnătura salariatului/voluntarului,

.....

Data,

.....



**PROCEDURĂ OPERAȚIONALĂ
PRIVIND
ASIGURAREA SECURITĂȚII DATELOR CU
CARACTER PERSONAL ÎN UNIVERSITATEA
DIN PITEȘTI**

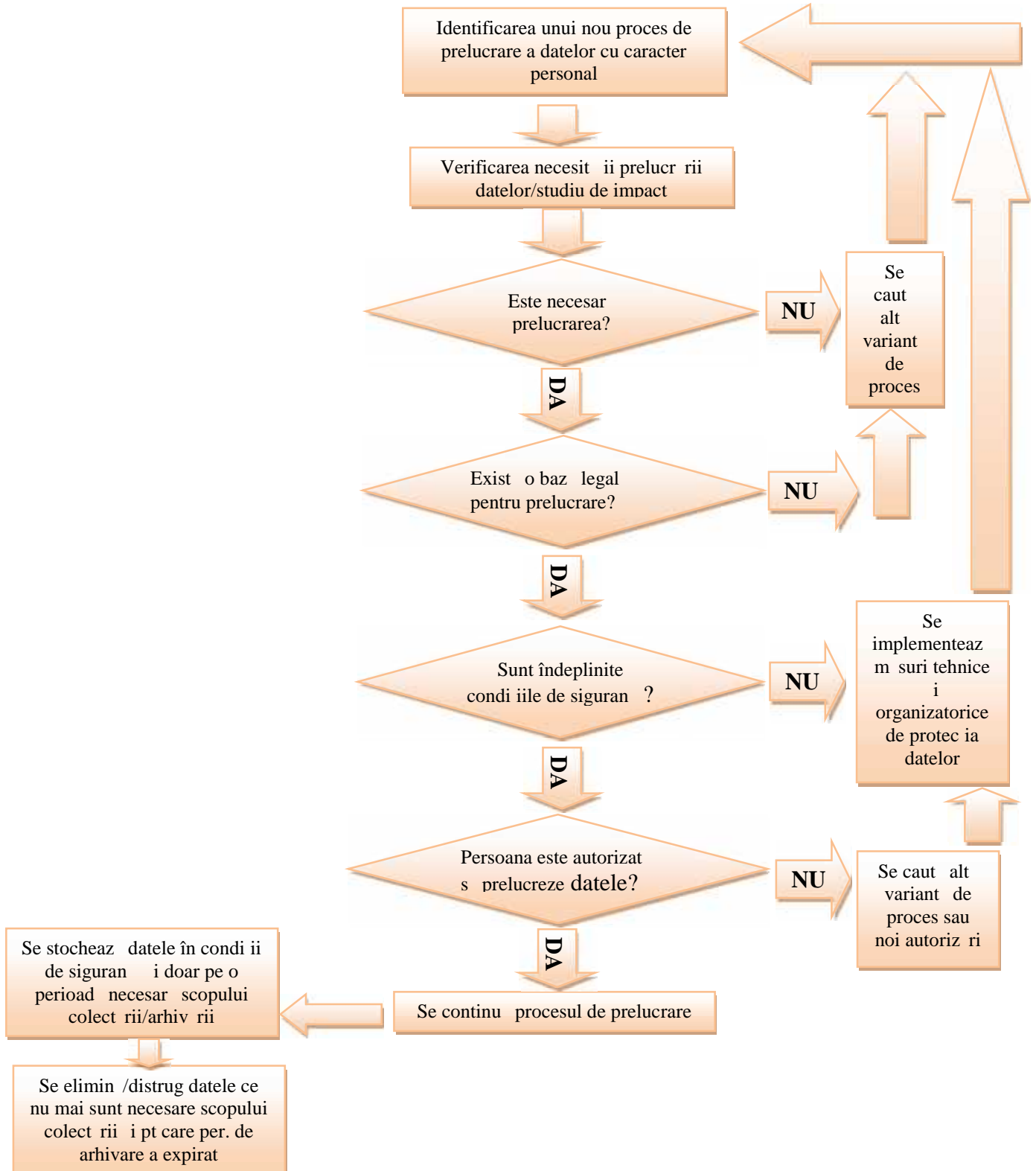
COD: PO-GDPR-01


Ediția 1

Revizia 0

Diagrama procesului


Anexa nr. 2




	PROCEDURĂ OPERA IONAL PRIVIND ASIGURAREA SECURIT II DATELOR CU CARACTER PERSONAL ÎN UNIVERSITATEA DIN PITE TI	Edi ia 1
	COD: PO-GDPR-01	Revizia 0

11. LISTA DE DIFUZARE

Nr. crt.	Structur	Nume i prenume	Data primirii	Semn tur	Data retragerii	Semn tur
1.	Senatul universit ții					
2.	CMCPU					
3.	Direc ia Resurse Umane					
4.	Centrul de Marketing Universitar					
5.	Facultatea de Științe, Educație Fizic i Informatic					
6.	Facultatea de Mecanic i Tehnologie					
7.	Facultatea de Electronic , Comunicații i Calculatoare					
8.	Facultatea de Științe Economice i Drept					
9.	Facultatea de Științe ale Educației, Științe Sociale i Psihologie					
10.	Facultatea de Teologie, Litere, Istorie i Arte					
11.	Colegiul Ter iar Nonuniversitar					
12.	Compartiment Studii Doctorale i Postdoctorale					
13.	CTICI					
14.	Centrul R.I.					
15.	Centrul IFR					
16.	Centrul de Formare Muntenia					
17.	Direc ia Secretariat General					
18.	BTS CA					

	PROCEDURĂ OPERAȚIONALĂ PRIVIND ASIGURAREA SECURITĂȚII DATELOR CU CARACTER PERSONAL ÎN UNIVERSITATEA DIN PITEȘTI	Ediția 1
		Revizia 0
COD: PO-GDPR-01		

19.	Direcția Generală Administrativă					
20.	Direcția Economică					
21.	Direcția Juridică					
22.	Compartimentul Audit public intern					
23.	Centrul pentru Consiliere și Orientare în Carieră					
24.	Serviciul Bibliotecă					
25.	Secretariatul tehnic al Comisiei de monitorizare					

	<p style="text-align: center;">PROCEDURĂ OPERAȚIONALĂ PRIVIND ASIGURAREA SECURITĂȚII DATELOR CU CARACTER PERSONAL ÎN UNIVERSITATEA DIN PITEȘTI</p> <p style="text-align: center;">COD: PO-GDPR-01</p>	Ediția 1
		Revizia 0

12. CUPRINS

Numărul componentei în cadrul procedurii	Denumirea componentei din cadrul procedurii	Pagina
	PAGINA DE GARD	1
1	LISTA RESPONSABILILOR CU ELABORAREA, VERIFICAREA ȘI APROBAREA EDIȚIEI/REVIZIEI	2
2	SITUAȚIA EDIȚIILOR ȘI REVIZIILOR ÎN CADRUL EDIȚIILOR PROCEDURII	2
3	SCOPUL PROCEDURII	3
4	DOMENIU DE APLICARE	3
5	DOCUMENTE DE REFERINȚĂ	3
6	DEFINIȚII ȘI ABREVIERI	4
7	DESCRIERE PROCEDURĂ	5
8	RESPONSABILITĂȚI	12
9	DATE DE CONTACT ALE DPO	14
10	ANEXE ȘI FORMULARE	14
11	LISTA DE DIFUZARE	19
12	CUPRINS	21