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

UNIVERSITATEA DIN PITEȘTI
SENAT
Nr. 635
an 2022 luna 12 zi 09

UNIVERSITATEA DIN PITEȘTI
RECTORAT
Nr. 16567
2022 luna 12 zi 07

AVIZAT,
În şedinţa Consiliului de Administraţie
din data de 07.12.2022

APROBAT,
În şedinţa Senatului
din data de 19.12.2022

RECTOR,
Conf. univ. ing. Dumitru CHIRLEȘAN

PREȘEDINTELE SENATULUI,
Prof. univ. dr. Mihaela-DIACONU

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

COD: PO-GDPR-01

1. LISTA RESPONSABILILOR CU ELABORAREA, VERIFICAREA ŞI APROBAREA EDIŢIEI

Nr. crt.	Elemente privind responsabilităţi/ operaţiuni	Responsabili cu elaborarea/verificarea ediţiei	Funcţia	Data	Semnătura
1.	Elaborare	Petruta RIZEA	Responsabil cu protecţia 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. Juridică	12.10.2022	
4.	Avizat comisie monitorizare	Prof.univ.dr. ing. Viorel NICOLAE	Preşedintele Comisiei de monitorizare	12.10.2022	
5.	Avizat Comisia nr. 2 a Senatului	Conf. univ. dr. Monica POPESCU	Preşedintele Comisiei nr. 2 a Senatului	16.10.2022	
6.	Avizat Secretar General al Senatului	Lect. univ. dr. Ramona DUMINICĂ	Secretar General al Senatului	19.12.2022	

2. SITUAȚIA EDIȚIILOR ȘI REVIZIILOR ÎN CADRUL EDIȚIILOR PROCEDURII

Nr. crt.	Revizia / Data aplicării	Numărul capitolului şi paginilor revizuite	Conținutul modificării	Nume şi prenume			
				Elaborat	Verificat	Avizat	Aprobat
1							
2							
3							

3. SCOPUL PROCEDURII

Prezenta procedură reglementează cadrul legal, măsurile tehnice şi organizatorice, cât şi modul unitar de desfăşurare în condiţii de siguranţă a activităţilor privind procesul de colectare şi prelucrare a datelor cu caracter personal, atât automat/în sistem informatic, cât şi prin intermediul altor mijloace, în cadrul Universităţii din Piteşti.

4. DOMENIUL DE APLICARE

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

5. DOCUMENTE DE REFERINȚĂ

5.1. Externe:

- **Regulamentul (UE) 2016/679 al Parlamentului European şi al Consiliului din 27 aprilie 2016** privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE (**Regulamentul general privind protectia datelor**).
- **Legea nr. 190 din 18 iulie 2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679** al Parlamentului European şi al Consiliului din 27 aprilie 2016 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE (Regulamentul general privind protecţia datelor)
- **Legea nr. 506 din 17 noiembrie 2004 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul comunicaţiilor electronice**
- **Decizii ale Autorităţii Naţionale pentru Protecţia datelor**
- **Legea Educaţiei Naţionale nr. 1/2011**, cu modificările ulterioare

5.2. Interne:

- **Carta Universităţii din Piteşti**
- **Regulament de organizare şi funcţionare a Universităţii din Piteşti**
- **Regulament intern al Universităţii din Piteşti**

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.	**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.
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, ștergerea ori distrugerea.
5.	**Operator**	Persoana 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 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 terță**	Persoana fizică sau juridică, autorizată să prelucreze date cu caracter personal.

Nr. Crt.	Termenul	Definiția
8.	**Destinatar**	Persoana fizică sau juridică, autoritatea publică, agenția sau alt organism căreia (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).

Procedura descrie condiţiile şi cerinţele obligatorii ce trebuie respectate în procesele instituţionale 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 a 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 on-line, dezvoltarea unei activităţi de marketing direct din partea universităţii, un nou proiect, o conferinţă sau un eveniment organizat în cadrul universităţii sau orice alt nou proces de prelucrare a datelor cu caracter personal în cadrul UPIT, fiecare operator trebuie să îsi pună următoarele întrebări:

  - ✓ Sigur este nevoie să fie colectată această informaţie?
  - ✓ Există o bază legală pentru prelucrare (cum ar fi consimţământul persoanei vizate, interesul legitim al universităţii pentru îndeplinirea unor clauze precontractuale sau în vederea derulării unui contract deja existent, obligaţii legale ce îi revin universităţii)?
  - ✓ Datele colectate pot fi anonimizate sau pseudonimizate?
  - ✓ Datele personale vor fi prelucrate în condiţii de siguranţă?
  - ✓ Datele personale vor fi transmise către o altă parte pentru a fi prelucrate (către o persoană împuternicită de către UPIT)?
  - ✓ Este planificat ca datele colectate să fie transferate către o ţară non-UE? Dacă da, există un set adecvat de măsuri de securitate implementat în ţara respectivă?
  - ✓ Există altă alternativă de îndeplinire a activităţii 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 universităţii, în vederea prelucrării, atunci utilizatorul datelor cu caracter personal trebuie să se conformeze la prevederile Regulamentului 679/2016 (UE).

- Este important să se analizeze necesitatea unui studiu de impact de câte ori apar noi activităţi de colectare a datelor în procesele existente sau sunt identificate noi procese ce presupun colectarea de date cu caracter personal.
- GDPR impune aplicarea unor măsuri de confidenţialitate încă de la crearea acestor procese („by design"), dar şi pe parcursul desfăşurării activităţilor („by default").
- Colectarea datelor cu caracter personal este permisă numai utilizatorilor autorizaţi în acest sens, în indeplinirea obligaţiilor de serviciu prevăzute prin fişa postului.

7.3. Prelucrarea datelor cu caracter personal

- Prin prelucrarea datelor se înţelege, în mod sumar, orice operaţiune efectuată 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 dispoziţie în orice alt mod, alinierea sau combinarea, restricţionarea, ştergerea ori distrugerea.

- 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 fișa postului.
- La nivel de fiecare structură trebuie implementate măsuri care să permită identificarea facilă a utilizatorului care a creat o inregistrare, a actualizat datele sau a modificat accidental inregistrarea (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.
- Modificările necesar 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 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 fișa 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. 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 "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 că au fost stocate electronic pe un server al instituției, pe PC-le personale,

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

- Fiecare structură organizatorică din cadrul Universităţii din Piteşti este responsabilă de stabilirea şi asigurarea perioadelor corespunzătoare de păstrare a informaţiilor cu caracter personal pe care le administrează, în condiţii de siguranţă şi în baza legislaţiei de arhivare în vigoare, coroborată cu nomenclatorul arhivistic specific şi procedurile interne ale universităţii.

7.5. Accesarea şi administrarea înregistrărilor şi bazelor de date cu caracter personal

- Accesul neautorizat, accidental sau intenţionat, la documente sau informaţii cu caracter personal, care poate duce la distrugerea, pierderea, modificarea sau divulgarea acestora, constituie o „încălcare a securităţii datelor cu caracter personal".
- Conducătorul de structură este responsabil, alături de persoanele din subordine care operează date cu caracter personal, de respectarea obligaţiei păstrării confidenţialităţii informaţiilor pe care le procesează. Un Angajament de confidenţialitate (Anexa nr. 1) trebuie semnat de către fiecare persoană (angajat/colaborator/voluntar UPIT) care, prin atribuţiile locului de muncă, are acces la/prelucrează date cu caracter personal, acest document însoţind fişa postului.

7.5.1. Accesul şi admistrarea documentelor ce conţin date cu caracter personal, stocate/arhivate în format fizic

- Accesul în încăperile/zonele în care sunt stocate sau arhivate documente ce conţin date cu caracter personal este strict permis doar persoanelor autorizate de către conducătorii structurilor din UPIT, în funţie de atribuţiile de serviciu ce le revin prin fişa postului.
- În cazul în care zona de lucru este de tip „open-space" şi nu pot fi implementate măsuri stricte de acces, angajaţii ce prelucrează date cu caracter personal au obligaţia de a se asigura că informaţiile nu pot fi vizualizate de către ceilalţi angajaţi sau de către vizitatori. Nu este permisă lăsarea 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 îşi părăsească biroul.
- Utilizatorii autorizaţi să acceseze sau să prelucreze date cu caracter personal sunt obligaţi să asigure confidenţialitatea acestora şi nu vor permite accesul la documente altor persoane, neautorizate.
- Este strict interzisă copierea fizică sau pe echipamente de stocare mobilă a informaţiilor confidenţiale 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 informaţie confidenţială sau de înregistrări ce conţin date cu caracter personal, fără o autorizare prealabilă de la conducătorul ierarhic.

7.5.2. Accesul şi 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 universităţii, accesul la sistem va fi permis doar în baza unor parole/conturi de acces, a căror confidenţialitate strictă va fi asigurată de către

utilizator şi nu vor fi comunicate altor persoane neautorizate, în mod conştient sau accidental.

- Utilizatorii autorizaţi nu au voie să copieze pe un mediu de stocare mobil (Stick USB, CD, DVD, Hard disk extern) sau să printeze documente ce conţin date cu caracter personal, în vederea comunicării către o terţă parte, fără o autorizare în acest sens.
- Utilizatorii nu vor permite, intenţionat sau accidental, accesul altor utilizatori neautorizaţi pe calculatorul propriu. Monitoarele calculatoarelor vor fi poziţionate în aşa fel încât datele să nu poată fi vizualizate decât exclusiv de către utilizatorul autorizat. Este obligatorie setarea funcţiei de „screen-saver", cu un interval de temporizare de maxim 5 minute. În acelaşi timp, utilizatorul are obligaţia de a se asigura că închide în condiţii de siguranţă orice fişier, bază de date sau sesiune de lucru, imediat ce nu mai operează.
- Indiferent dacă este vorba de proiectarea, întreţinerea, actualizarea datelor sau softului specifice unei baze de date, accesul unei terţe părţi este permis strict în aria de lucru, în prezenţa utilizatorului autorizat. În cazul în care suportul tehnic este asigurat de o firmă externă (persoană împuternicită de universitate), accesul reprezentanţilor acesteia este permis doar pe durata derulării contractului şi numai în baza unui acord de confidenţialitate ce va însoţi în mod obligatoriu contractul.
- Înregistrările şi bazele de date cu caracter personal create sau actualizate de către angajaţii UPIT, în calitate de utilizatori, trebuie să fie salvate în siguranţă şi să li se creeze copii (back-up), iar intervalul de timp la care se execută acestea şi locaţia unde vor fi salvate se va stabili de către conducătorii de structuri, în funcţie de importanţa şi volumul acestor informaţii. Controlul şi responsabilitatea acestei acţiuni este în sarcina fiecărui conducător de structură, cu menţiunea că intervalul de timp între două operaţiuni de creare a back-up-ului pentru acelaşi fişier sau bază de date nu trebuie să depaşească 3 luni. O evidenţă a acestor operaţiuni va trebui menţinută la nivelul fiecărei structuri.
- În exercitarea atribuţiilor de serviciu, tot personalul universităţii va utiliza adresele de e-mail instituţionale, configurate pe serverul Universităţii din Piteşti (domeniul *upit.ro*).
- Nu este permisă trimiterea prin e-mail, către un cont extern de domeniul UPIT, a unor documente sau informaţii ce conţin date cu caracter personal, decât în baza unui temei legal (ex. obligaţie legală ce îi revine universităţii, la solicitarea directă şi în baza consimţământului persoanei vizate, pentru derularea unui contract ce presupune şi un acord de confidenţialitate etc.) şi cu respectarea măsurilor de securitate, cum ar fi parolarea sau criptarea informaţiei.
- Personalul instituţiei nu trebuie să transmită sau să primească informaţii confidenţiale ce privesc Universitatea din Piteşti sau care conţin 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 şi comunicare care nu necesită intervenţia unui operator uman, prin fax ori prin poştă electronică sau prin orice altă metodă care foloseşte serviciile de comunicaţii electronice destinate publicului, cu excepţia cazului în care abonatul sau utilizatorul vizat şi-a exprimat în prealabil consimţământul expres pentru a primi asemenea comunicări (ex. prin intermediul abonării la newsletter).
- Fără a aduce atingere prevederilor aliniatului anterior, dacă universitatea, în calitate de persoană juridică sau un salariat al universităţii, obţin în mod direct adresa de poştă

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 servicii educaționale/proiecte/evenimente similare, cu condiția de a oferi în 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

- UPIT 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.
- UPIT are obligația de a administra, în condiții de siguranță și numai pentru scopul specificat, datele personale colectate prin intermediul sistemelor de supraveghere video. UPIT nu va prelucra datele personale decât în măsura în care acest demers este necesar îndeplinirii 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/C.T.I.C.I. va verifica periodic și va răspunde de siguranța și confidențialitatea datelor personale stocate în sistemul de supraveghere/monitorizare video. Angajamentul de confidențialitate (Anexa nr. 1) 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

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

7.6. Conştientizarea şi instruirea personalului UPIT ce prelucreaza date cu caracter personal

7.6.1. Conştientizarea personalului UPIT privind importanţa respectării GDPR

- Creşterea nivelului de conştientizare a fiecărui angajat/colaborator/voluntar din universitate (în calitate de prelucrător de date cu caracter personal), referitor la importanţa implementării şi respectării prevederilor GDPR în ceea ce priveşte protecţia datelor cu caracter personal, constituie un principiu de bază în creşterea calităţii serviciilor oferite, precum şi în desfăşurarea activităţii profesionale în condiţii de siguranţă şi confidenţialitate.
- Acest proces se realizează ca urmare a identificarii necesităţii de informare şi instruire a personalului referitor la legislaţia în vigoare privind protecţia datelor cu caracter personal.
- Fiecare angajat/colaborator/voluntar UPIT are dreptul la informare şi trebuie să cunoască politicile şi procedurile interne ale UPIT în acest domeniu, măsurile tehnice şi 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 cunoştinţe, de conştientizare privind obligativitatea implementarii 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 şi motivaţia fiecărei persoane care urmează să fie instruită.
- Metodele de instruire (instruirea internă, consilierea la locul de muncă, instruirea externă, autoinstruirea) se vor alege în funcţie de necesarul constatat, resursele umane şi financiare disponibile, obiectivele propuse, grupul ţintă căruia se adresează.

7.6.2.2. Procesul de instruire

- *Instruirea internă* -se realizează de către furnizori, angajaţi ai universităţii (cum ar fi DPO, reprezentant al centrului T.I.C.I., conducătorul de structură în baza unei documentaţii primite etc.), într-o locaţie şi 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 funcţie de necesităţile/neconformităţilor punctuale constatate în urma etapelor de audit sau de către superiorul direct şi este derulată la locul de muncă al angajatului, în timpul perioadei de desfăşurare a activităţii profesionale.
- *Autoinstruirea* –se realizează în mod direct, de către fiecare angajat al universităţii, cu sprijinul DPO sau al conducătorului direct, dacă este cazul, şi în baza documentaţiei necesare în domeniul protecţiei datelor cu caracter personal pusă la dispoziţie de către

universitate: legislaţie, metodologii, regulamente, proceduri operaţionale, ghiduri de conformare la prevederile GDPR.

- *Instruirea externă* –se realizează de către furnizori de servicii externi, urmând ca astfel de sesiuni să fie planificate în urma constatării necesităţii şi identificării resurselor financiare, numai cu aprobarea prealabilă a conducerii universităţii.

7.6.2.3. Evaluarea, monitorizarea şi îmbunătăţirea procesului de instruire

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

8. RESPONSABILITĂȚI

8.1. Rectorul Universităţii din Piteşti, în calitate de reprezentant legal al operatorului

- asigură implementarea şi respectarea procedurii;
- identifică şi alocă resursele necesare desfăşurării în condiţii de legalitate şi siguranţă a proceselor ce presupun colectarea şi prelucrarea de date cu caracter personal în Universitatea din Piteşti;
- urmăreşte eficienţa măsurilor de securizare a datelor cu caracter personal implementate în universitate şi, în cazul în care sunt constatate riscuri sau vulnerabilităţi, solicită măsuri corective şi participă, alături de ceilalţi factori de decizie implicaţi, la implementarea acestora.

8.2. Responsabilul DPO

- iniţiază şi execută procesul de constatare a situaţiei curente din punct de vedere al stadiului respectării protecţiei datelor cu caracter personal în universitate, prin interviuri, întâlniri de lucru cu personalul din departamentele relevante;
- identifică procesele instituţionale în care au loc activităţi de colectare şi prelucrare a datelor cu caracter personal şi sprijină structurile unde se derulează aceste procese în proiectarea şi implementarea de măsuri tehnice şi organizatorice de asigurare a protecţiei şi confidenţialităţii acestor tipuri de date;
- elaborează documente interne specifice GDPR (politici, proceduri, ghiduri de conformare) şi actualizează, cu clauze privind securizarea datelor cu caracter personal, metodologii, regulamente, proceduri ale universităţii care interferează cu activităţi de colectare şi prelucrare a datelor cu caracter personal;
- instruieşte personalul universităţii care, prin atribuţiile postului, prelucrează date cu caracter personal, dar şi reprezentanţii conducerii, cu privire la obligaţia legală a

securizării datelor cu caracter personal ale tuturor categoriilor de persoane vizate, cu care intră în contact prin prisma proceselor instituţionale;
- consiliază în mod constant conducerea universităţii cu privire la obligaţiile ce îi revin în aplicarea prevederilor GDPR în cadrul fiecărui proces ce presupune colectare şi prelucrare de date cu caracter personal;
- monitorizează şi evaluează periodic, dar şi în timpul activităţii curente a fiecărui angajat, implementarea şi respectarea prevederilor GDPR privind asigurarea securităţii datelor cu caracter personal;
- informează conducerea UPIT privind vulnerabilităţile şi riscurile constate cu privirea la securizarea datelor cu caracter personal în universitate şi propune măsuri tehnice şi organizatorice pentru înlăturarea acestora;
- aduce la cunoştinţa conducerii universităţii orice posibilă breşă de securitate constatată, ce ar putea conduce la afectarea drepturilor şi libertăţilor persoanelor vizate, în vederea identificării cauzelor şi a minimizării riscurilor şi limitării efectelor de diseminare neautorizată a datelor personale;
- elaborează şi propune revizuirea acestei proceduri ori de câte ori se constată că este necesar.

8.3. Centrul T.I.C.I. –cu atribuţii în domeniul tehnologiei şi securizării informaţiei
- propune şi stabileşte tipurile de acces pentru fiecare utilizator al sistemelor informatice din UPIT, în concordanţă cu atribuţiile ce îi revin prin fişa postului;
- asigură măsurile tehnice necesare pentru protejarea datelor cu caracter personal colectate şi prelucrate în sistemele informatice ale universităţii, împotriva accesării, copierii sau divulgării neautorizate;
- actualizează şi supraveghează, din punctul de vedere al securităţii, site-urile universităţii.
- identifică şi informează factorii de conducere ai universităţii şi DPO-ul cu privire la orice posibil risc ce ar conduce la o breşă de securitate a datelor cu caracter personal prelucrate în sistemele electronice ale universităţii şi propune măsuri/resurse necesare remedierii.
- asigură măsurile necesare pentru identificarea rapidă a utilizatorului care a introdus, a actualizat, a modificat, şters sau divulgat accidental sau intenţionat date cu caracter personal în sistemele electronice ale universităţii;
- este responsabil, alături de DPO, de instruirea pe partea tehnică a personalului universităţii care, prin atribuţiile postului, prelucrează date cu caracter personal, cu privire la obligaţia legală a securizării datelor cu caracter personal cu care intră în contact prin prisma atribuţiilor postului;
- aplică şi respectă prevederile prezentei proceduri.

8.4. Direcţia juridică
- este responsabilă în ceea ce priveşte asigurarea aplicării prevederilor GDPR în toate procesele cu care interacţionează prin prisma avizului juridic (ex. contracte, acte adiţionale, acorduri de colaborare, proceduri, metodologii, regulamente, fişe de post, etc.) sau a activităţii specifice, cât şi în orice documente ale universităţii ce presupun prelucrare de date cu caracter personal;
- informează DPO-ul privind orice neconformităţi constatate referitoare la protecţia datelor cu caracter personal, în vederea identificării măsurilor necesare remedierii acestora.

- 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 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/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 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);
- 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 Petruța Mihaela
- **Adresă corespondență:** Universitatea din Pitești, str. Târgu din Vale nr.1, Rectorat
- **Numar de telefon:** 0348/453121
- **Adresă de email:** responsabil.gdpr@upit.ro

10. ANEXE SI 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.

F01-PO-GDPR-01

Anexa nr. 1

MINISTERUL EDUCAȚIEI
UNIVERSITATEA DIN PITEȘTI
Str. Târgul din Vale, Nr. 1, Cod poștal 110040 - Pitești, Jud. Argeș
Tel./ Fax: +40 348 453 100/123, www.upit.ro

UNIVERSITATEA DIN PITEȘTI

ANGAJAMENTUL DE CONFIDENȚIALITATE ȘI CONFORMARE LA PREVEDERILE GDPR AL SALARIATULUI/VOLUNTARULUI UNIVERSITĂȚII DIN PITEȘTI

Domnul/doamna....., domiciliat/domiciliată în localitatea....., str. ..... nr. ....., județul....., posesor/posesoare al/a buletinului/cărții de identitate/pașaportului seria ....., nr. ....., eliberat/eliberată de ....., la data de....., C.N.P....., **în calitate de salariat/voluntar la UNIVERSITATEA DIN PITEȘTI** (denumită în continuare **operator** de date cu caracter personal), CUI 4122183, cu sediul în str. Târgu din Vale, nr. 1, Pitești, Departamentul/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, 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 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/voluntarul 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 nici o 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;
- 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 din Pitești;

- Să distrugă documentele cu caracter confidențial care nu mai sunt folositoare 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 (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 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 d**ocumente 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;
- dezvăluirea informației s-a făcut după primirea acordului scris pentru aceasta;
- informația era publică la data dezvăluirii ei;
- salariatul/voluntarul a fost obligat în mod legal să dezvaluie informația.

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

Semnătura salariatului/voluntarului,

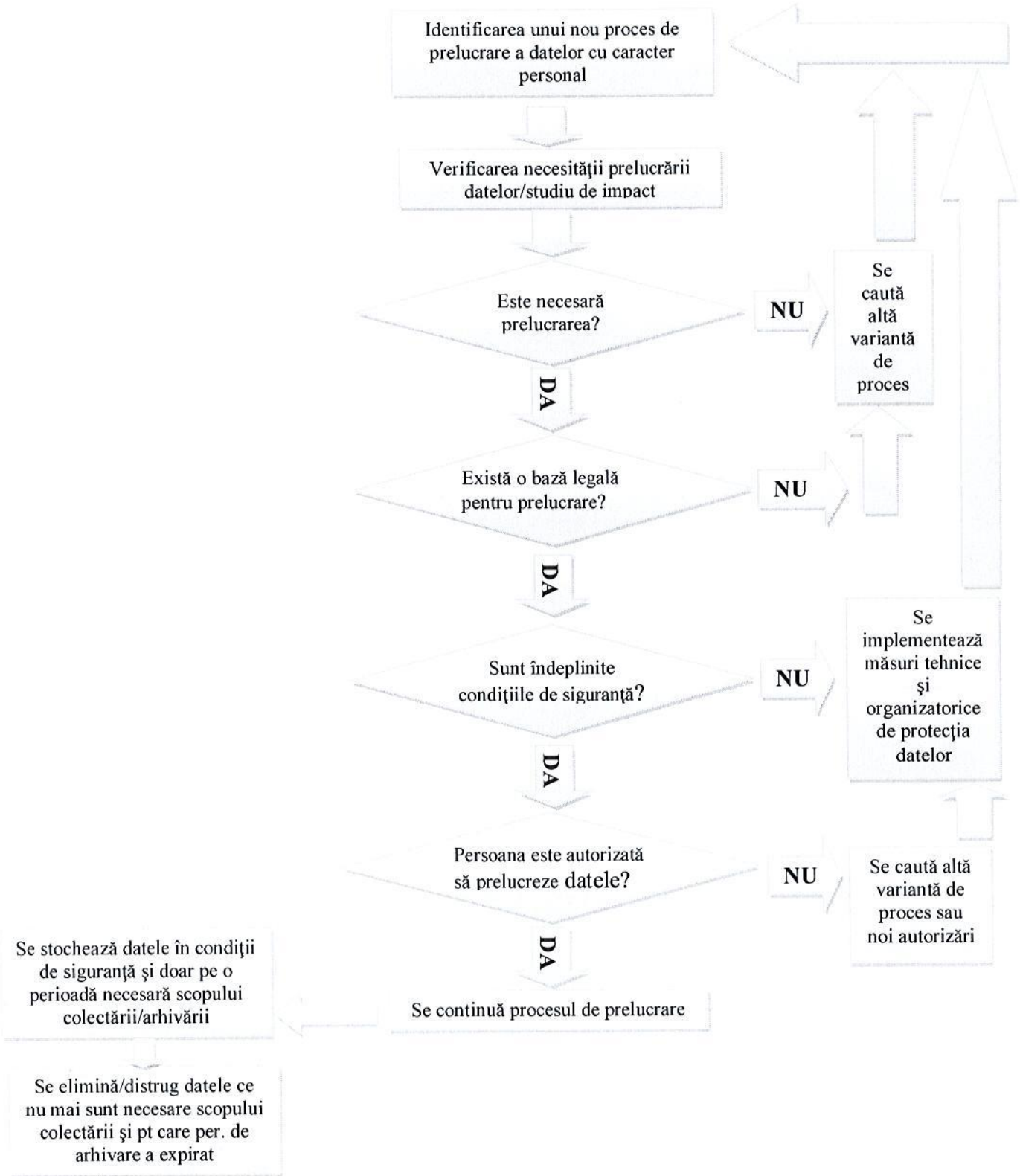
.....

Data,

.....

Diagrama procesului

Anexa nr. 2



11. LISTA DE DIFUZARE

Nr. crt.	Structură	Nume și prenume	Data primirii	Semnătură	Data retragerii	Semnătură
1.	Senatul universității					
2.	CMCPU					
3.	Direcţia Resurse Umane					
4.	Centrul de Marketing Universitar					
5.	Facultatea de Științe, Educație Fizică și Informatică					
6.	Facultatea de Mecanică și Tehnologie					
7.	Facultatea de Electronică, Comunicații și Calculatoare					
8.	Facultatea de Științe Economice și Drept					
9.	Facultatea de Științe ale Educației, Științe Sociale și Psihologie					
10.	Facultatea de Teologie, Litere, Istorie și Arte					
11.	Colegiul Terţiar Nonuniversitar					
12.	Compartiment Studii Doctorale și Postdoctorale					
13.	CTICI					
14.	Centrul R.I.					
15.	Centrul IFR					
16.	Centrul de Formare Muntenia					
17.	Direcţia Secretariat General					
18.	BTS CA					

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

12. CUPRINS