PROCEDURA OPERAȚIONALĂ PRIVIND PROTECȚIA PERSOANELOR FIZICE ÎN CEEA CE PRIVEȘTE PRELUCRAREA DATELOR CU CARACTER PERSONAL ȘI LIBERA CIRCULAȚIE A ACESTOR DATE

CUPRINS:

1) Ce este GPDR şi transpunerea acestuia în Procedură Operațională la nivelul UNEFS

1.1.General Data Protection Regulation (GDPR) este Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) și este aplicabil începând cu data de 25 mai 2018.

1.2. Astfel, GDPR este un regulament general privind protecția persoanelor fizice în legatură cu prelucrarea datelor cu caracter personal prin care se stabilește un set unic de reguli care se va aplica în toate statele membre ale Uniunii Europene.

1.3 În conformitate cu procedurile aprobate la nivelul Universității de Educație Fizică și Sport, Regulamentul (UE) 2016/679 va fi transpus prin intermediul prezentei proceduri, denumită Procedura operațională privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date, denumită în continuare **Procedura**.

2) Scopul și domeniul de aplicare a Procedurii

2.1 Scopul prezentei Proceduri este acela de a proteja și garanta drepturile și libertățile fundamentale ale persoanelor fizice în conformitate cu reglementările prevăzute în cadrul Regulamentului 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 privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor).

2.2 Procedura urmărește trei scopuri fundamentale:

a) să constituie un instrument de clarificare și interpretare a prevederilor Regulamentului;
b) să garanteze și să protejeze drepturile și libertățile fundamentale ale persoanelor fizice cu privire la prelucrarea datelor cu caracter personal;
c) să propună o serie de bune practici menite să asigure aplicarea adecvată și unitară a normelor comunitare care guvernează prelucrarea datelor cu caracter personal în activitatea instituțiilor și departamentelor/serviciilor care fac parte din cadrul Universității Naționale de Educație Fizică și Sport;

2.3.Prezenta Procedură se aplică în mod unitar în cadrul Universității Naționale de Educație Fizică și Sport din București (denumită în continuare "***UNEFS***"), colectării și prelucrării datelor cu caracter personal, efectuate, în tot sau în parte, prin mijloace automate precum și colectării și prelucrării prin alte mijloace decât cele automate a datelor cu caracter personal care fac parte dintr-un sistem de evidență și care sunt destinate să fie incluse într-un asemenea sistem.

2.4.Procedura vizează activitățile de colectare și prelucrare a datelor cu caracter personal efectuate de către instituțiile, structurile și departamentele din cadrul UNEFS, astfel cum acestea sunt prezentate în cadrul organigramei afişate pe site-ul instituției.

2.5. Facultățile, departamentele și serviciile care fac parte integrantă din cadrul UNEFS, denumite în continuare în prezenta Procedură "***structuri UNEFS***", sunt următoarele:

a) ***Facultatea de Educatie Fizica si Sport***, cu sediul în Bucuresti, Str. Constantin Noica, Nr. 140, Sector 6, C.P.060057, telefon: +40/21 3164107, +40/21 3164108, fax: + 40/21 3120400, E-mail**:** rector@unefs.ro, secretariat@unefs.ro;

b) ***Facultatea de Kinetoterapie***, cu sediul în București, Str. Constantin Noica, Nr. 140, Sector 6, C.P.060057, telefon: +40/21 3164107, +40/21 3164108, fax: + 40/21 3120400, e-mail: decanatkt@unefs.ro;

c) ***Școala Doctorală***, cu sediul în București, Str. Constantin Noica, Nr. 140, Sector 6, C.P.060057, telefon: +40/21 3164107, +40/21 3164108, Fax: + 40/21 3120400, E-mail**:** secretariat_doctorat@unefs.ro;

d) ***Centru de Formare și Dezvoltare Profesională*** cu sediul în Str. Constantin Noica, nr. 140, sector 6, Bucureşti, telefon: +40/21 3164106, fax**:** + 40/21 3120400 ***e-mail:*** **cfdp.unefs@yahoo.com**

e) ***Departamentul de Comunicare și Relații Externe*** cu sediul în Str. Constantin Noica, nr. 140, sector 6, Bucureşti, telefon: **0**21 3164107/int. 231, fax: + 40/21 3120400**, E-mail: dcre@unefs.ro**

f) ***Centrul de Consiliere și Orientare în Carieră*** cu sediul în Str. Constantin Noica, nr. 140, sector 6, Bucureşti, telefon: +40/21 3164107**;** interior 213; fax +40.21) 312.04.00 E-mail: **ccocp@unefs.ro**

g) ***Centrul de Cercetări Interdisciplinare "dr. Alexandru Parthensis"*** cu sediul în Str. Constantin Noica, nr. 140, sector 6, Bucureşti, telefon: +40/21 3164107**;** interior 213; E-mail: **cercetare@unefs.ro**

h) ***Serviciul Secretariat*** cu sediul în București, Str. Constantin Noica, Nr. 140, Sector 6, C.P.060057, telefon: +40/21 3164107, +40/21 3164108, interior 201, fax: + 40/21 3120400, E-mail**:** secretariat_rectorat@unefs.ro; secretariat@unefs.ro

i) ***Serviciul Organizare Resurse Umane şi Salarizare*** cu sediul în București, Str. Constantin Noica, Nr. 140, Sector 6, C.P.060057, telefon: +40/21 3164107, interior 212, fax: + 40/21 3120400, E-mail**:** resurseumane_unefs@yahoo.com

j) ***Serviciul Financiar Contabilitate*** cu sediul în București, Str. Constantin Noica, Nr. 140, Sector 6, C.P.060057, telefon: +40/21 3164107, interior 227, ax: + 40/21 3120400, E-mail**:** resurseumane_unefs@yahoo.com

k) ***Biblioteca***, cu sediul în București, Str. Constantin Noica, Nr. 140, Sector 6, C.P.060057, telefon: +40/21 3164107, fax: + 40/21 3120400, interior 242, E-mail**:** u.biblioteca@yahoo.com

3) DOCUMENTE DE REFERINȚĂ

- 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 Educaţiei Naţionale nr. 1/2011, cu modificările şi completările ulterioare;
- Legea nr. 128/12.07.1997 privind Statutul Personalului Didactic, cu modificările și

completările ulterioare.

4) DEFINIȚIA TERMENILOR

4.1 Date cu caracter personal - înseamnă orice informații privind o persoană fizică identificată sau identificabilă („persoana vizată"); o persoană fizică identificabilă este o persoană care poate fi identificată, direct sau indirect, în special prin referire la un element de identificare, cum ar fi un nume, un număr de identificare, date de localizare, un identificator online, sau la unul sau mai multe elemente specifice, proprii identităţii sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale.

A)„Orice Informații"

- **Din punctul de vedere al naturii Informațiilor**, conceptul de date cu caracter personal cuprinde orice afirmație referitoare la o persoană. Acesta acoperă Informațiile „obiective", precum prezența unei anumite substanțe în sângele unei persoane. De asemenea, conceptul se poate referi la Informații „subiective", sub forma opiniilor sau evaluărilor.

- **Din punctul de vedere al conținutului Informațiilor**, conceptul de date cu caracter personal cuprinde datele care furnizeaza orice fel de Informații, datele personale putând fi împărțite în:

a. **date cu caracter personal generale**, precum nume și prenume, data și locul nașterii, adresa, numărul de telefon, adresa de e-mail; date referitoare la contul bancar.
b. **date cu caracter personal cu caracter special**: acele date care dezvăluie originea rasială sau etnică, opiniile politice, confesiunea religioasă sau convingerile filozofice sau apartenența la sindicate și prelucrarea de date genetice, de date biometrice pentru identificarea unică a unei persoane fizice, de date privind sănătatea sau de date privind viața sexuală sau orientarea sexuală ale unei persoane fizice;
c. date cu caracter personal referitoare la condamnări penale și infracțiuni;

- **Din punct de vedere al suportului sau formatului** pe care sunt stocate Informațiile, datele cu caracter personal cuprind Informațiile disponibile în orice formă, indiferent că aceasta este, de exemplu, alfabetică, numerică, grafică, fotografică sau acustică. Datele personale cuprind Informațiile scrise pe hârtie, precum și Informațiile stocate în memoria unui calculator cu ajutorul unui cod binar sau stocate, de exemplu, pe o casetă video.

B) „Privind" [o persoană fizică]

Informațiile pot fi considerate că „privesc" o persoană atunci când acestea sunt despre persoana respectivă. Informațiile se referă la o persoană atunci când acestea au în vedere identitatea, caracteristicile sau comportamentul unei persoane sau atunci când asemenea Informații sunt utilizate pentru a determina sau influența modul în care persoana respectivă este tratată sau evaluată.

C) [Persoana fizică] „identificată sau identificabilă"

- O persoană fizică poate fi considerată ca fiind „**identificată**" atunci când, în cadrul unui grup de persoane, aceasta **se distinge** de ceilalți membri ai grupului. În consecință,

persoana fizică este „identificabilă” atunci când, cu toate că persoana nu a fost încă identificată, este posibil să se realizeze acest lucru.

- O nouă clarificare este cuprinsă în definiția datelor cu caracter personal din cuprinsul Regulamentului, în sensul că „*o persoana 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*”.
- **În ceea ce privește persoanele *„identificate direct”***, numele persoanei reprezintă identificatorul cel mai obișnuit, iar, în principiu, noțiunea de „persoană identificată” implică, cel mai adesea, o referire la numele persoanei. Pentru a stabili această identitate, numele persoanei trebuie, uneori, coroborat cu alte Informații (data nașterii, numele părinților, adresa sau fotografia cu fața persoanei) pentru a preveni confuzia dintre persoana respectivă și posibili omonimi.
- ***În ceea ce privește persoanele „identificate indirect”,*** aceasta categorie de persoane are legatură cu fenomenul „combinațiilor unice”, indiferent că acestea sunt mari sau mici. Un exemplu de astfel de caracteristici care pot determina identificarea fără dificultate a persoanei în cauza îl constituie *elementele specifice, proprii identității sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale* (de exemplu „actualul prim ministru al Spaniei”).
- Gradul în care anumite informații sunt suficiente pentru a realiza identificarea depinde de contextul situației specifice. Un nume de familie foarte obișnuit nu este suficient pentru a identifica o persoană - cu alte cuvinte, pentru a individualiza pe cineva - din ansamblul populației unei țări. În schimb, este posibil să se realizeze identificarea unui copil într-o clasă de elevi.

C) „[Orice Informații privind] o persoană fizică”

Datele cu caracter personal sunt date referitoare la persoanele în viață identificate sau identificabile.

Informațiile privind persoanele decedate nu trebuie considerate drept date cu caracter personal în temeiul Regulamentului.

IMPORTANT: Conceptul de date cu caracter personal include identificatorii online furnizaţi de dispozitivele, aplicaţiile, instrumentele şi protocoalele lor, cum ar fi adresele IP, identificatorii cookie sau alţi identificatori precum etichetele de identificare prin frecvenţe radio şi datele despre locaţie.

Regulamentul introduce termenul de “date pseudonime”, adică acele date personale care au fost supuse unor modalităţi de prelucrare a datelor astfel încât să nu mai poată identifica direct o persoană fără a utiliza informaţii suplimentare. Datele pseudonime sunt considerate date cu caracter personal şi, prin urmare, se supun cerinţelor GDPR.

4.2. Prelucrare de date cu caracter personal - înseamnă orice operațiune care se efectuează asupra datelor cu caracter personal, prin mijloace automate sau neautomate în cadrul unor operațiuni ori seturi de operațiuni, fără a fi limitate la acestea, cum ar fi colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea,

divulgarea prin transmitere, diseminarea sau punerea la dispoziție în orice alt mod, alinierea sau combinarea, restricționarea, ștergerea sau distrugerea.

- ***Colectarea*** presupune acțiunea de a strânge, a aduna, a primi date cu caracter personal de la persoanele vizate prin intermediul structurilor UNEFS.
- ***Înregistrare*** presupune consemnarea datelor cu caracter personal într-un sistem de evidențiere automată ori neautomată, care poate fi registru, fișier automat, baza de date sau orice altă formă de evidență organizată, structurată ori ad-hoc sau într-un text, înșiruire de date ori document, indiferent de modalitatea în care se înscriu datele.
- ***Organizarea*** presupune ordonarea, structurarea sau sistematizarea datelor cu caracter personal, conform unor criterii prestabilite, potrivit atribuțiilor legale ale operatorului, în scopul eficientizării/optimizării activităților de prelucrare a acestora.
- ***Stocarea*** presupune păstrarea pe orice fel de suport a datelor cu caracter personal culese, inclusiv prin efectuarea unor copii de siguranță.
- ***Adaptarea*** presupune transformarea datelor cu caracter personal colectate inițial, conform criteriilor prestabilite și scopurilor pentru care au fost colectate.
- ***Modificarea*** presupune actualizarea, completarea, schimbarea, corectarea ori refacerea datelor cu caracter personal, în scopul menținerii caracteristicilor de exactitate, realitate și actualitate;
- ***Extragerea*** presupune scoaterea unei părți din categoria specifică de date cu caracter personal, în scopul utilizării acesteia, separat și distinct de prelucrarea inițială.
- ***Consultarea*** presupune examinarea, vizualizarea, interogarea ori cercetarea datelor cu caracter personal fără a fi limitate la acestea, în scopul efectuării unei operațiuni sau set de operațiuni de prelucrare ulterioară.
- ***Utilizarea*** presupune folosirea datelor cu caracter personal, în tot sau în parte, de către și în interiorul operatorului, împuterniciților operatorului sau destinatarului, după caz, inclusiv prin tipărire, copiere, multiplicare, scanare sau alte procedee similare;
- ***Dezvăluirea*** presupune acțiunea de a face disponibile datele cu caracter personal către terți prin comunicare, transmitere, diseminare sau în orice alt mod;
- ***Alăturarea*** presupune acțiunea de a adăuga, alipirea sau anexarea unor date cu caracter personal la cele deja existente, pe care nu le modifică;
- ***Combinarea*** presupune îmbinarea, unirea sau asamblarea unor date cu caracter personal separate inițial, într-o formă nouă, pe baza unor criterii prestabilite, pentru scopuri anume determinate;
- ***Restricționarea*** presupune limitarea accesului la datele cu caracter personal pentru o perioadă determinată, pentru scopuri anume determinate;
- ***Ștergerea*** presupune eliminarea sau înlăturarea, în tot sau în parte, a datelor cu caracter personal din evidențe sau înregistrări, prin împlinirea termenului de păstrare, la atingerea scopului pentru care au fost introduse, caducitatea, inexistența ori inexactitatea acestora;
- ***Transformarea*** presupune operațiunea efectuată asupra datelor cu caracter personal având ca scop anonimizarea ori utilizarea în scopuri exclusiv statistice;
- ***Distrugerea*** presupune aducerea la stare de neîntrebuințare, în condițiile legii, definitivă și irecuperabilă, prin mijloace mecanice sau termice, a suportului fizic pe care au fost prelucrate date cu caracter personal.

4.3 Operator și Persoana împuternicită de operator

Operatorul este persoana care decide cum și pentru ce sunt prelucrate datele cu caracter personal, adică determină scopul și mijloacele prelucrării datelor.

Nu este considerată operator de date, persoana care prelucrează date cu caracter personal în numele și pe seama unui operator și care nu determină individual care este scopul și modul de prelucrare a datelor obținute, ci este considerată **persoana împuternicită de operator**.
Persoana împuternicită de operator este persoana fizică sau juridică de drept privat ori de drept public, inclusiv autoritățile publice, instituțiile şi structurile teritoriale ale acestora care prelucrează date cu caracter personal pe seama operatorului.

4.4. Persoana vizată înseamnă orice persoană ale cărui date sunt prelucrate, devenind astfel persoană fizică identificată sau identificabilă, acestea fiind precizate în concret la art. 5.1 din prezenta Procedură.

4.5. Destinatar înseamnă persoană fizică sau juridică, autoritatea publică, agenția sau alt organism căreia (căruia) îi sunt divulgate datele cu caracter personal, indiferent dacă este sau nu o parte terță. Cu toate acestea, autoritățile publice cărora li se pot comunica date cu caracter personal în cadrul unei anumite anchete în conformitate cu dreptul Uniunii sau cu dreptul intern nu sunt considerate destinatari; prelucrarea acestor date de către autoritățile publice respective respectă normele aplicabile în materie de protecție a datelor, în conformitate cu scopurile prelucrării.
În categoria destinatarilor pot intra autoritățile publice față de care UNEFS face *raportari și situații*, respectiv Ministerul Educației Naționale, Ministerul Cercetării Științifice, ITM, Agenția Națională de Administrare Fiscală, Colegiul Medicilor, Inspectoratul General al Poliție, Institutul Național de Statistică, Agenția Națională de Asigurarea Calității în Învățământul Superior, Serviciul Emigrări, ambasade, organizații similare din străinătate; inclusiv autorități fiscale; asociații din domeniul învățământului, dacă legislația prevede acest lucru; prestatori implicați în mod direct/indirect în procesul de învățământ (ex. contracte de voluntariat;contracte de parteneriat) și/sau în procesul de gestionare a monitorizării și securizării persoanelor și a bunurilor publice ori private aflate în patrimoniul ori în administrarea UNEFS (ex: contractele de servicii de pază).

4.6. Parte terță înseamnă o persoana fizică sau juridică, autoritate publică, agenție sau organism altul decât persoana vizată, operatorul, persoana împuternicită de operator și persoanele care, sub directa autoritate a operatorului sau a persoanei împuternicite de operator, sunt autorizate să prelucreze date cu caracter personal.

4.7 Consimțământ al persoanei vizate înseamnă orice manifestare de voință liberă, specifică, informată și lipsită de ambiguitate a persoanei vizate prin care aceasta acceptă, printr-o declarație sau printr-o acțiune fără echivoc, ca datele cu caracter personal care o privesc să fie prelucrate.

4.8.Încălcarea securității datelor cu caracter personal înseamnă o încalcare 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.

4.9. Reprezentant înseamnă o persoana fizică sau juridică stabilită în Uniune, desemnată în scris de către operator sau persoana împuternicită de operator în temeiul articolului 27 din GPDR, care reprezintă operatorul sau persoana împuternicită în ceea ce privește obligațiile lor respective care le revin in temeiul GDPR.

4.10. Reguli corporatiste obligatorii înseamnă politicile în materie de protecție a datelor cu caracter personal care trebuie respectate de un operator sau de o persoană împuternicită de operator stabilită pe teritoriul unui stat membru, în ceea ce privește transferurile sau seturile de transferuri de date cu caracter personal către un operator sau o persoană împuternicită de operator în una sau mai multe țări terțe în cadrul unui grup de întreprinderi sau al unui grup de întreprinderi implicate într-o activitate economică comună.

4.11. Încălcare a securității datelor cu caracter personal
înseamnă o încălcăre 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.

a) ***Distrugerea*** se referă la situația în care datele nu mai există ori nu mai există într-o formă care să le facă utilizabile de către operatori;
b) ***Pierderea*** are în vedere situația în care datele pot să existe, însă operatorul a pierdut controlul sau accesul la date;
c) ***modificarea*** desemnează situația în care datele sunt corupte sau modificate în alt mod, astfel încât ele nu mai sunt complete;
d) ***divulgarea neautorizată*** are în vedere situația în care datele au fost transmise către ori accesate de către persoane neautorizate să primească sau să acceseze datele personale.

DESCRIEREA ACTIVITĂȚII

5) *Categorii de persoane vizate. Scop prelucrare. Temei prelucrare date. Părțile care au acces la datele cu caracter personal*

5.1 Categorii de persoane vizate

5.1.1 UNEFS are calitate de operator de date cu caracter personal care colectează și prelucrează datele cu caracter personal următoarelor categorii de persoane fizice, în funcție de scopul prevăzut în prezenta procedură, respectiv:

a) Studenți, doctoranzi, masteranzi, cursanți, părinți ai acestora, reprezentanți legali ai acestora, alți membri ai familiei, candidați la concursurile de admitere; personal didactic, personal didactic auxiliar și personal administrativ, candidați la concursurile de ocupare a posturilor didactice, de cercetare, didactice auxiliare și administrative din învățământul superior, vizitatori, orice persoană care intră într-o clădire aparținând UNEFS ori administrate de UNEFS (în acest caz, ne referim la situațiile bazelor didactice Parâng și Eforie Nord) indiferent dacă sunt sau nu dotate cu sistem de supraveghere video.

b) Orice persoană fizică sau juridică ce are raporturi de natură comercială sau contractuală cu UNEFS.

c) Orice referire în prezenta Procedură la categoriile de persoane vizate indicate mai sus se va face prin folosirea sintagmei "*persoană vizată*".

5.2. Scopul și motivația colectării prelucrării datelor cu caracter personal

5.2.1 UNEFS are obligația de a administra în condiții de siguranță și numai pentru scopurile specificate, datele cu caracter personal ale categoriilor de persoane prevăzute la art. 5.1.

5.2.2 Scopul colectării datelor este:

a) Pentru persoanele prevăzute la 5.1.1 lit.a):

- prestări de servicii ale UNEFS pentru realizarea activităților de educație, cultură și cercetare științifică**.** De asemenea, informațiile colectate de către universitate prin intermediul structurilor UNEFS sunt folosite pentru analize și prelucrări statistice necesare pentru fundamentarea deciziilor manageriale;
- monitorizarea/ securitatea persoanelor, spațiilor și/ sau bunurilor publice/ private ori a bunurilor publice aflate în administrarea UNEFS (ex. Bazele didactice_Parâng si Eforie Nord);

b) Pentru persoanele fizice prevăzute la 5.1.1 lit. b): gestiune economico-financiară și administrativă; servicii hoteliere și de turism, aplicabile în mod specific pentru bazele didactice Parâng si Eforie Nord; servicii de comunicații electronice, dacă este cazul.

5.2.3 (a) Motivația pentru care UNEFS colectează date cu caracter personal ține de prelucrări ale informațiilor pe baza cărora să se poată lua decizii coerente și corecte în managementul universității.

(b) Pentru persoanele de la 5.1 lit. a) este necesară furnizarea de către persoane a unor date obligatorii (informații despre identitatea persoanei precum și a părinților sau reprezentanților legali, acceptul asupra monitorizării video perimetrale și de interior pentru sporirea securității în sistemul educațional etc.), acestea fiind necesare în vederea derulării/ inițierii de raporturi juridice cu UNEFS, cu respectarea prevederilor legale (exemplu: cele privind relația cu angajații sau cele privind înscrierea la studii sau cele privind evidența rezultatelor școlare sau a actelor de studii). În situația refuzului de a furniza aceste date, UNEFS poate refuza inițierea de raporturi juridice, întrucât poate fi pusă în imposibilitatea de a respecta cerințele reglementărilor speciale în domeniul educației, iar în cazul angajaților, a prevederilor dreptului muncii și dreptului fiscal.
(3) UNEFS colectează inclusiv informații care nu au caracter obligatoriu (de exemplu: adresa de e-mail, telefon etc.) în vederea îmbunătățirii modului de comunicare cu studenții, doctoranzii, masteranzii, cursanții sau reprezentanții legali ai acestora precum și pentru realizarea ulterioară de sondaje statistice utilizând comunicarea prin sistemul poștei electronice. În situația în care se refuză furnizarea și/sau prelucrarea datelor informațiilor opționale poate duce la imposibilitatea ca UNEFS să transmită informații despre serviciile sale.
(4) În situațiile prevazute la 5.1 lit. b), datele cu caracter personal se colectează și prelucrează pentru a respecta prevederile legale relativ la înregistrarea operațiunilor financiar-contabile. Furnizarea datelor de către persoanele din această categorie este obligatorie, refuzul de a le furniza duce la imposibilitatea de a demara relații juridice între UNEFS și respectivele persoane.

5.3 Temeiul prelucrării datelor cu caracter personal

5.3.1 UNEFS poate prelucra date cu caracter personal atunci când se află în cel puțin unul dintre următoarele cazuri:

a) persoana vizată și-a dat consimțământul pentru prelucrarea datelor sale cu caracter personal

Consimțământul persoanei vizate este:

- ***Oferit în mod liber***

Elementul „liber" implică o alegere reală și un control real din partea persoanelor vizate. Ca regulă generală, în situația în care persoana vizată nu beneficiază de o alegere reala, se simte obligată sau va suferi consecințe negative dacă nu exprimă consimțământul, consimțământul acesteia nu va fi unul valabil exprimat. Dacă consimțământul este încadrat ca o parte ce nu poate fi negociată în cadrul unor termeni și condiții, se prezumă că acesta nu este exprimat în mod liber. Astfel, consimțământul nu va fi considerat ca fiind în mod liber exprimat dacă persoana vizată se afla în imposibilitatea de a refuza sau a-l retrage fără a suferi un prejudiciu.

- ***Specific***

Acordarea consimțământului de către persoana vizată trebuie să fie facută în raport cu ,,unul sau mai multe scopuri specifice". Pentru a respecta elementul ,,specific", trebuie să aplice:
(i) specificarea scopului ca garanție împotriva denaturării funcției,
(ii) separarea clară a informațiilor legate de obținerea consimțământului pentru prelucrarea datelor față de informațiile referitoare la alte aspecte.
Consimțământul trebuie solicitat (i) în mod separat de termeni și condiții ori alte documente de informare și prezentare și (ii) în mod specific pentru fiecare scop pentru care se face prelucrare pe acest temei juridic.

- ***În cunoștință de cauză***

Furnizarea de informații persoanei vizate înainte de obținerea consimțământului este esențială pentru a-i permite să ia decizii în cunoștință de cauză, să înțeleagă cu ce este de acord și, de exemplu, să își exercite dreptul de a-și retrage consimțământul. Dacă operatorul/persoana împuternicită nu furnizează informații accesibile, controlul pe care îl are persoana vizată devine iluzoriu, iar consimțământul va fi un temei nevalabil pentru prelucrare.

Exemplu: persoanei vizate i se aduce la cunoștință scopul specific pentru care i se solicită datele, respectiv pentru ca acestea să fie folosite, respectiv pentru a i se include datele în sistemul de evidență (pentru persoanele care urmează să acceadă la concursul de admitere) iar pentru vizitatori, acestora li se comunică scopul prelucrării, respectiv vizita în cadrul clădirii 1 a UNEFS.

- ***Exprimare 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.***

Consimțământul necesită o declarație din partea persoanei vizate sau un act afirmativ clar ceea ce înseamnă că trebuie să fie dat întotdeauna printr-o manifestare activă de voință sau printr-o declarație. Trebuie să fie evident ca persoană vizată și-a dat consimțământul pentru o anumită prelucrare. Un „act afirmativ clar" înseamnă că persoană vizată trebuie să fi luat o acțiune deliberată pentru consimțirea la aceea prelucrare specifică. Consimțământul poate fi obținut printr-o declarație scrisă sau o declarație orală (înregistrată), inclusiv prin mijloace electronice. Acesta ar putea include bifarea unei căsuțe atunci când persoana vizitează un site, alegerea parametrilor tehnici pentru serviciile societății informaționale sau orice altă declarație sau acțiune care indică în mod clar în acest context acceptarea de către persoană vizată a prelucrării

propuse a datelor sale cu caracter personal. Prin urmare, absența unui răspuns, căsuțele bifate în prealabil, absența unei acțiuni sau simpla continuare a utilizării unui serviciu nu constituie consimțământ.

Exemplu: UNEFS stabilește consimțământul ca temei juridic al prelucrării datelor persoanei vizate, în funcție de scopul specific declarat. În acest scop, la începutul colaborării, în proiectul de contract de studiu inserează o fereastră de consimțământ expres (cerința solicitării separate a consimțământului), prin care persoanele vizate sunt invitate să valideze / bifeze acordul lor pentru prelucrarea datelor lor personale (consimțământ expres), o dată cu semnarea contractului de studiu.

b) prelucrarea este necesară pentru executarea unui contract la care persoana vizată este parte sau pentru a face demersuri la cererea persoanei vizate înainte de încheierea unui contract

b.1) Există un contract valabil, pentru a cărui executare este necesară prelucrarea de date cu caracter personal; sau
b.2) În fază pre-contractuală, la solicitarea persoanei vizate, este nevoie de prelucrarea anumitor date cu caracter personal în vederea încheierii contractului.
Exemplul 1: UNEFS urmează să primească viitori studenți, masteranzi ori doctoranzi, în limita locurilor alocate și după ce au promovat examenul de admitere. În atare situație, operatorul se afla în faza pre contractuală, situație în care se pot prelucra numele și prenumele, datele de identificare și celelalte date cu caracter personal furnizate de potențialul candidat (date cu caracter medical care reies din adeverința depusă, cazier judiciar etc...) depuse la dosarul de candidat.
Exemplul 2: În cadrul contractelor individuale de muncă, angajatul trebuie să prezinte datele cu caracter personal pentru a se efectua formalitățile de angajare.

b.3) În mod contrar, prelucrarea nu se poate baza pe temeiul încheierii /executării contractului dacă:

a) Trebuie prelucrate datele unei persoane, alta decât cea cu care se încheie contractul;

Exemplu: situația prelucrării datelor unui reprezentant legal al unui student, care intră să facă o vizită în căminul studențesc. Prelucrarea datelor acestei persoane nu se poate întemeia pe contractul de studiu încheiat cu studentul. În acest caz, trebuie ales un alt temei al prelucrării, în cazul de față administrarea bunului public care se efectuează de către UNEFS.

b) Inițiativa încheierii contractului aparține operatorului sau unei terțe persoane;

Exemplu: Abordarea unui cadru didactic, persoană fizică, de către UNEFS, pentru o anumită activitatea de cercetare fără o manifestare de interes din partea primului nu se poate întemeia pe un eventual și viitor contract cu persoană fizică. Eventual, o asemenea abordare ar fi legală dacă se utilizează ca și alt temei al prelucrării, activitatea de cercetare științifică.

c) Cerința necesității prelucrării pentru încheierea sau executarea unui contract nu înseamnă întotdeauna ca prelucrarea este esențială în acest scop, totuși aceasta trebuie să fie limitată la și proporțională cu scopul urmărit.

Exemplu: Prelucrarea de către UNEFS a datelor de contact ale unui nou angajat sunt necesare pentru încheierea contractului de muncă. Spre diferență, prelucrarea datelor privind parcursul profesional/performanța angajatului (e.g. evaluări periodice) nu vor avea ca temei juridic executarea contractului (nu este necesară derulării acestuia), ci eventual, un alt temei, interesul legitim.

c) prelucrarea este necesară în vederea îndeplinirii unei obligații legale care îi revine operatorului

Prelucrarea datelor cu caracter personal pe temeiul necesității conformării unei obligații legale presupune existența unei norme legale imperative aplicabile operatorului. De asemenea, prelucrarea impusă printr-o decizie administrativă / hotărâre judecatorească (ele însele, luate în temeiul unei abilitări legale) poate fi justificată tot prin necesitatea conformării unei obligații legale.

Exemplul 1: În vederea desfășurării obiectului său de activitate, UNEFS prelucrează datele cu caracter personal al candidaților la concursul de admitere, studenți, cursanți, candidați la concursurile de ocupare a posturilor de cercetare si didactice.
Exemplul 2: În vederea respectării dispozițiilor legale în materie de securitate socială, operatorul poate furniza autorității relevante date cu caracter personal privind angajații săi.
Exemplul 3: Pentru ca personalul didactic să acceadă la funcții de conducere, este necesară prelucrarea datelor cu caracter personal pentru prezentarea la concurs și apoi pentru efectuarea tuturor formalităților pentru a se încheia actul adițional în care se consemnează noua funcție.

d) prelucrarea este necesară pentru a proteja interesele vitale ale persoanei vizate sau ale altei persoane fizice

Exemplu: Un spital tratează un pacient după un accident rutier grav; spitalul nu are nevoie de consimțământul acestuia pentru a-i cauta actul de identitate și a verifica dacă persoana respectivă se află în baza sa de date, pentru a-i găsi fișa medicală sau a-i contacta rudele cele mai apropiate.

e) prelucrarea este necesară pentru îndeplinirea unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice cu care este investit operatorul

Exemplu: situația în care în cadrul campusului universitar se întâmplă un incident între studenți care necesită intervenția poliției ori a serviciului de urgență

f) prelucrarea este necesară în scopul intereselor legitime urmărite de operator sau de o parte terță

5.3.2. Interesul legitim este cel mai flexibil temei juridic de prelucrare a datelor cu caracter personal și, de aceea, utilizarea sa trebuie calibrată în mod adecvat. În mod tipic, poate fi folosit doar în cazurile în care prelucrarea are un impact minimal asupra persoanelor vizate. Pentru o judicioasă întemeiere pe interesul legitim, prelucrarea datelor cu caracter personal trebuie să îndeplinească trei tipuri de caracteristici:
a) Testul scopului legitim. Operatorul trebuie să urmărească un interes legitim al său ori al unui terț. Interesul legitim poate fi un interes comercial, profesional sau un scop mai larg, de exemplu un interes social.
b) Testul necesității. Prelucrarea trebuie să fie proporțională și limitată pentru atingerea interesului legitim urmărit. Dacă respectivul interes poate fi atins printr-o prelucrare mai puțin intruzivă / cuprinzătoare, nu poate fi utilizat acest temei.
c) Testul raportării la interesele persoanei vizate. Ca principiu, prelucrarea trebuie să fie previzibilă pentru persoană vizată și să nu creeze un prejudiciu / inconvenient nenecesar persoanei vizate. ***Important:*** ***nu întotdeauna interesele persoanei vizate trebuie aliniate cu cele ale operatorului. Pot exista situații în care interesele operatorului pot prevala asupra celor ale persoanei vizate în cadrul unei prelucrări legitime***.

5.4. Părțile care au acces la datele cu caracter personal

5.4.1 Datele cu caracter personal colectate sunt destinate utilizării de către structurile UNEFS, în calitate de operator, și sunt comunicate numai următorilor destinatari: persoana vizată, reprezentanții legali ai persoanei vizate, angajați cu drept de acces ai operatorului, împuternicitul operatorului (dacă există), alte persoane fizice / juridice care prelucrează datele personale în numele operatorului, autorități publice, poliția, organe de cercetare și urmărire penală și alte instituții abilitate de lege să solicite informații și să primească date cu caracter personal.

5.4.2. Au calitatea de operator structurile din cadrul UNEFS, dacă stabilesc scopul și mijloacele de prelucrare a datelor cu caracter personal.

5.4.2 Are calitatea de utilizator al datelor cu caracter personal, denumit în continuare utilizator, personalul operatorului sau al împuternicitului acestuia ale cărui atribuții de serviciu presupun operațiuni de prelucrare a datelor cu caracter personal.

5.4.3 UNEFS, în calitate de operator, are în principal următoarele obligații:

a) să asigure informarea persoanei vizate și să respecte drepturile acestora;
b) să ia măsurile necesare pentru a asigura securitatea prelucrării datelor cu caracter personal;
c) să respecte prezenta procedură privind măsurile de protecție a persoanelor cu privire la prelucrarea datelor cu caracter personal.

6) Prelucrarea de categorii speciale de date sau referitoare la condamnări penale şi infracțiuni

6.1 Categorii speciale de date

(1) Regulamentul definește categoriile speciale de date ca fiind date cu caracter personal care dezvăluie originea rasială sau etnică, opiniile politice, confesiunea religioasă sau convingerile filozofice sau apartenența la sindicate și prelucrarea de date genetice, de date biometrice pentru identificarea unică a unei persoane fizice, de date privind sănătatea sau de date privind viața sexuală sau orientarea sexuală ale unei persoane fizice.

(2) Aceste categorii de date sunt considerate sensibile și se impune un standard de protecție superior**.** Concret, pentru prelucrarea adecvată a acestor categorii de date se impune îndeplinirea uneia dintre condițiile reglementate de Art. 9 alin. (2) din Regulament.

(3) În această categorie de date se includ datele de sănătate și cele biometrice care sunt necesare în mod special la UNEFS, în particular la Facultatea de Educație Fizică şi Sport și Facultatea de Kinetoterapie. Cu privire la acest tip de date Regulamentul prevede, în cadrul art. 9 alin. (2) lit. g) si/sau j) împrejurarea că operatorul poate prelucra acest tip de date în virtutea interesului public major ori cel al scopului de educație și cercetare științifică, o astfel de derogare decurgând din chiar specificul UNEFS.

6.2 Date referitoare la condamnări speciale şi infracţiuni

(1) Similar prelucrării categoriilor speciale de date, prelucrarea datelor referitoare la condamnări penale și infracțiuni presupune: (i) un temei juridic de prelucrare potrivit Art. 6 din Regulament; și (ii) competență legală (proprie autorităților publice) sau o autorizare legală.

(2) În cazul de față, prelucrarea datelor referitoare la condamnări speciale și infracțiuni înscrise în cazierul judiciar se prelucrează integrat în cadrul datelor din dosarele de personal, în situația candidaților la concursurile de ocuparea funcției didactice ori de angajarea personalui didactic auxiliar ori administrativ, temeiul în acest caz fiind dat de art. 6 lit. e) „prelucrarea este necesară pentru îndeplinirea unei sarcini care servește unui interes public sau în exercitarea autorității publice cu care este investit operatorul” din Regulament.

7) Principiile prelucrării datelor cu caracter personal

7.1 Legalitate, echitate şi transparenţă	Datele cu caracter personal vor fi prelucrate în mod legal, echitabil și transparent față de persoana vizată
7.2 Limitări legate de scop	Datele cu caracter personal vor fi colectate în scopuri determinate, explicite și legitime și nu sunt prelucrate ulterior într-un mod incompatibil cu aceste scopuri
7.3 Reducerea la minimum a datelor	Datele cu caracter personal vor fi adecvate, relevante și limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate
7.4 Exactitate	Datele cu caracter personal vor fi exacte și, în cazul în care este necesar, actualizate
7.5 Limitări legate de stocare	Datele cu caracter personal vor fi păstrate într-o formă care permite identificarea persoanei vizate pe o perioadă care nu depășește perioada necesară îndeplinirii scopurilor în care sunt prelucrate datele
7.6 Integritate și confidențialitate	Datele cu caracter personal vor fi prelucrate

	într-un mod care asigura securitatea adecvată a datelor cu caracter personal, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luarea de măsuri tehnice sau organizatorice corespunzătoare
7.7 Responsabilitate	Operatorul este responsabil și va trebui să demonstreze conformitatatea cu reglementările europene privind protecția datelor cu caracter personal

În virtutea respectării principiului legalității, echității și transparenței, operatorul are obligația de a furniza persoanei vizate o serie de informații.

7.8 Cum se face informarea persoanei vizate

(1) Informarea trebuie oferită într-o formă concisă, transparentă, inteligibilă și ușor accesibilă, utilizând un limbaj clar si simplu.
(2) Documentul de informare este pus la dispoziția persoanei vizate în forme diferite, depinzând de scopurile prelucrării și de sursa datelor (persoană vizată sau altă sursă): de exemplu, politica de confidențialitate a unui website, anexa la contractul încheiat cu persoana fizică, nota de informare inserată într-un formular de aplicație pentru o poziție în cadrul operatorului, etc.
(3) Ca principiu, nota de informare se livrează în scris inclusiv, atunci când este oportun, în format electronic.
(4) Pot exista și informări verbale, la solicitarea persoanei vizate, cu condiţia ca identitatea persoanei vizate sa fie dovedită prin alte mijloace.

7.9 Ce informații trebuie furnizate persoanelor vizate

Tip de informație	Date obținute de la persoană vizată	Date obținute din alte surse
identitatea şi datele de contact ale operatorului și, după caz, ale reprezentantului acestuia;	✓	✓
datele de contact ale responsabilului cu protecția datelor, după caz;	✓	✓
scopurile în care sunt prelucrate datele cu caracter personal, precum și temeiul juridic al prelucrării;	✓	✓
în cazul în care prelucrarea se face în baza temeiului legitim, interesele legitime urmărite;	✓	✓
categoriile de date cu caracter personal vizate;		✓

destinatarii sau categoriile de destinatari ai datelor cu caracter personal;	✓	✓
dacă este cazul, intenția operatorului de a transfera date cu caracter personal către o țară terță sau o organizație internațională si existența sau absența unei decizii a Comisiei privind caracterul adecvat;	✓	✓
perioada pentru care vor fi stocate datele cu caracter personal sau, dacă acest lucru nu este posibil, criteriile utilizate pentru a stabili această perioadă;	✓	✓
existența dreptului de a solicita operatorului, în ceea ce privește datele cu caracter personal referitoare la persoană vizată, accesul la acestea, rectificarea sau ștergerea acestora sau restricționarea prelucrării sau a dreptului de a se opune prelucrării, precum și a dreptului la portabilitatea datelor;	✓	✓
atunci când prelucrarea se bazează pe consimțământul persoanei vizate, existența dreptului de a retrage consimțământul în orice moment, fără a afecta legalitatea prelucrării efectuate pe baza consimțământului înainte de retragerea acestuia;	✓	✓
dreptul de a depune o plângere în fața unei autorități de supraveghere;	✓	✓
dacă furnizarea de date cu caracter personal reprezintă o obligație legală sau contractuală sau o obligație necesară pentru încheierea unui contract, precum și dacă persoană vizată este obligată să furnizeze aceste date cu caracter personal și care sunt eventualele consecințe ale nerespectării acestei obligații;	✓	
existența unui proces decizional automatizat incluzând crearea de profiluri, precum și, cel puțin în cazurile prevăzute în Regulament, informații pertinente privind logica utilizată și privind importanța și consecințele preconizate ale unei astfel de prelucrări pentru persoana vizată;	✓	✓
sursa din care provin datele cu caracter personal și, dacă este cazul, dacă acestea provin din surse disponibile public;		✓

7.10 Când se face informarea

(1) În cazul datelor cu caracter personal colectate direct de la persoana vizată, informarea se face în momentul obținerii datelor.
(2) În cazul datelor cu caracter personal colectate din alte surse, informarea se face:
a) într-un termen rezonabil după obtinerea datelor cu caracter personal, dar nu mai mare de o lună, ținându-se seama de circumstanțele specifice în care sunt prelucrate datele cu caracter personal;
b) dacă datele cu caracter personal urmează să fie utilizate pentru comunicarea cu persoană vizată, cel târziu în momentul primei comunicari către persoană vizată respectivă; sau
c) dacă se intenționează divulgarea datelor cu caracter personal către un alt destinatar, cel mai târziu la data la care acestea sunt divulgate pentru prima oară.

7.11 Excepții de la obligația de informare

(1) Indiferent dacă datele cu caracter personal sunt obținute de la persoană vizată sau din alte surse, informarea nu este necesară dacă și în măsura în care persoană vizată deține deja informațiile respective.
(2) În plus, pentru cazul particular al prelucrărilor de date cu caracter personal obținute din alte surse realizate de FEPARH, alte excepţii de la obligaţia de informare pot deveni incidente:

a) furnizarea acestor informații se dovedește a fi imposibilă sau ar implica eforturi disproporționate;
b) obținerea sau divulgarea datelor este prevăzută în mod expres de dreptul Uniunii sau de dreptul intern și care prevede măsuri adecvate pentru a proteja interesele legitime ale persoanei vizate;
c) în cazul în care datele cu caracter personal trebuie să rămână confidențiale în temeiul unei obligații statutare de secret profesional reglementate de dreptul Uniunii sau de dreptul intern, inclusiv al unei obligații legale de a păstra secretul.

8) *Drepturile persoanei vizate*

8.1 Regulamentul prevede 8 drepturi specifice în materie de prelucrare a datelor cu caracter personal
a) Dreptul de acces la date;
b) Dreptul la rectificarea datelor;
c) Dreptul la ștergerea datelor;
d) Dreptul la restricționarea prelucrării;
e) Dreptul la portabilitatea datelor;
f) Dreptul de opoziție la prelucrarea datelor;
g) Dreptul de a nu fi supus unor decizi automatizate, inclusiv profilarea;

h) Dreptul la notificarea destinatarilor privind rectificarea, ștergerea ori restricționarea datelor cu caracter personal.

A) Dreptul de acces la date

8.2 Atunci când acționează în calitate de operator, UNEFS are obligația, la cererea transmisă pe orice canal de către persoana vizată (studenți, cursanți, angajati, alte persoane fizice), de a confirma acesteia ce date prelucrează și în ce condiții.
8.3 În cazul în care se solicită accesul la datele cu caracter personal, soluționarea unei astfel de solicitări presupune:
a) Confirmarea cu privire la operațiunea prelucrării de date (dacă se prelucrează sau nu);
b) Informații cu privire la:
• Scopurile prelucrării;
• Categoriile de date personale vizate;
• Destinatarii cărora datele personale au fost sau vor fi divulgate (în special destinatari din țări terțe sau organizații internaționale);
• Perioada de stocare a datelor personale (dacă este posibil);
• Existența dreptului la ștergere, rectificare sau restricționare precum și dreptul de a se opune prelucrării;
• Dreptul de a depune plângere în fața unei autorități de supraveghere;
• Existența unui proces decizional automatizat, inclusiv crearea de profiluri si informații privind logica utilizată și consecințele prelucrării;
c) Informații cu privire la garanțiile adecvate (când datele sunt transferate către o țară terță sau o organizație internațională);
d) Copie a datelor care fac obiectul prelucrării. Pentru orice alte copii solicitate de persoană vizată, se poate percepe o taxa rezonabilă, bazată pe costurile administrative, dacă este cazul. În cazul în care persoană vizată introduce cererea în format electronic și cu excepția cazului în care persoană vizată solicită un alt format, informațiile sunt furnizate într-un format electronic utilizat în mod curent.

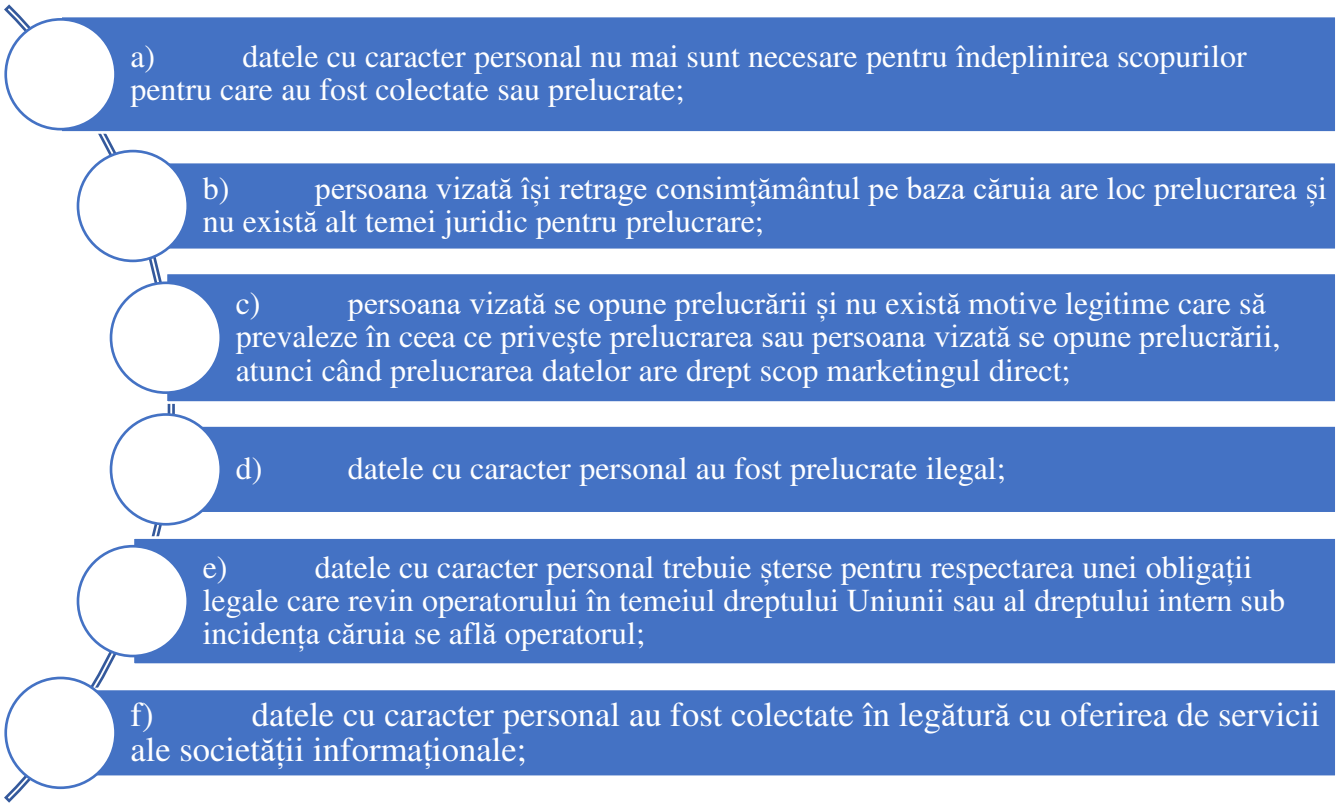
B) Dreptul la rectificarea datelor

8.4 Când acționează ca operator, UNEFS are obligația de a asigura respectarea drepturilor persoanei vizate de a obține fără întârziere rectificarea oricăror date inexacte (eronate sau incomplete) care le privesc.
Exemplu: la solicitarea uneia dintre persoanele vizate de la art. 5.1.1 de actualizare a datelor sale de contact / identificare, UNEFS trebuie să aibă implementate mijloace corespunzătoare pentru a introduce imediat în sistem astfel de modificări (ex. dacă vorbim despre un număr ridicat de persoane (ne raportăm la studenți/cursanți/doctoranzi, masteranzi), ar trebui să aibă o persoană cu atribuții specifice pentru tratarea unor asemenea solicitari venite din partea acestora).

C) Dreptul la ștergerea datelor

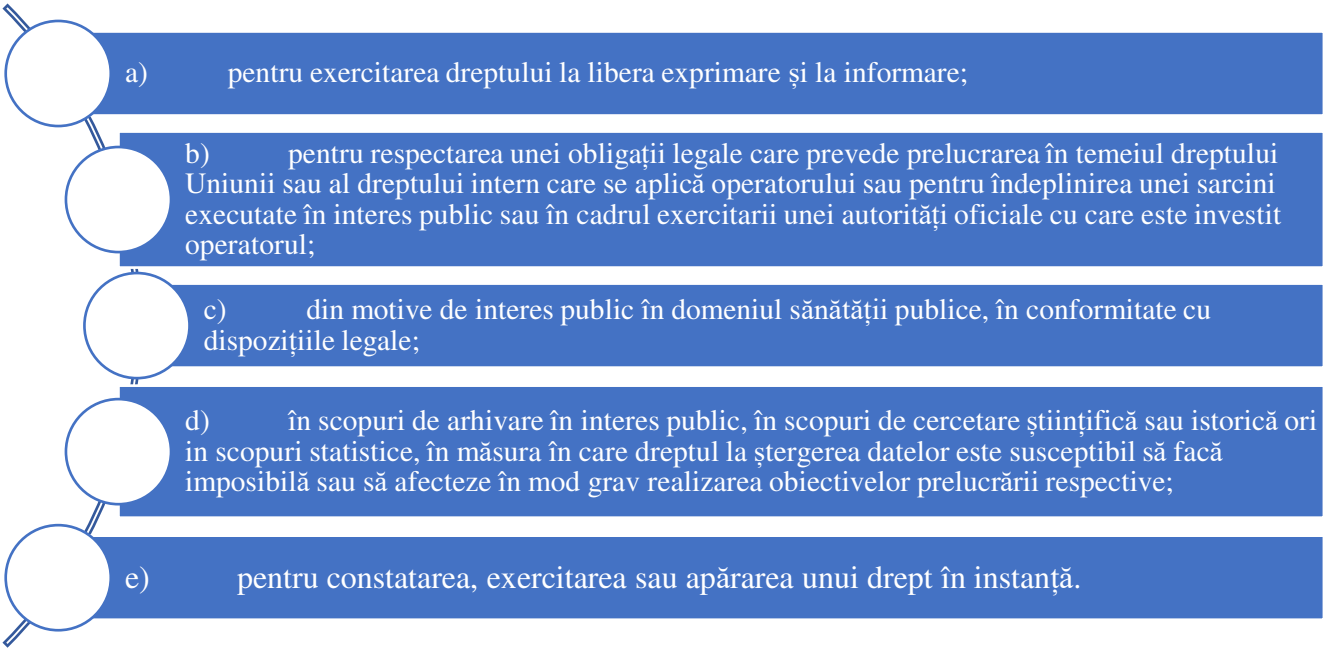
8.5 În cazul în care persoana vizată solicită ștergerea datelor cu caracter personal care o privesc, se va transmite acesteia o declarație în care să se menționeze că toate datele au fost șterse (inclusiv copii sau reproduceri).
8.6 În cazul în care UNEFS a făcut publice datele cu caracter personal și este obligat să le șteargă, ținând seama de tehnologia disponibilă și de costul implementării, UNEFS ia măsuri rezonabile, inclusiv măsuri tehnice, pentru a informa operatorii care prelucrează datele cu caracter personal că persoana vizată a solicitat ștergerea de către acești operatori a oricăror linkuri către datele respective sau a oricăror copii sau reproduceri ale acestor date cu caracter personal.

8.7 Când se poate solicita ștergerea datelor



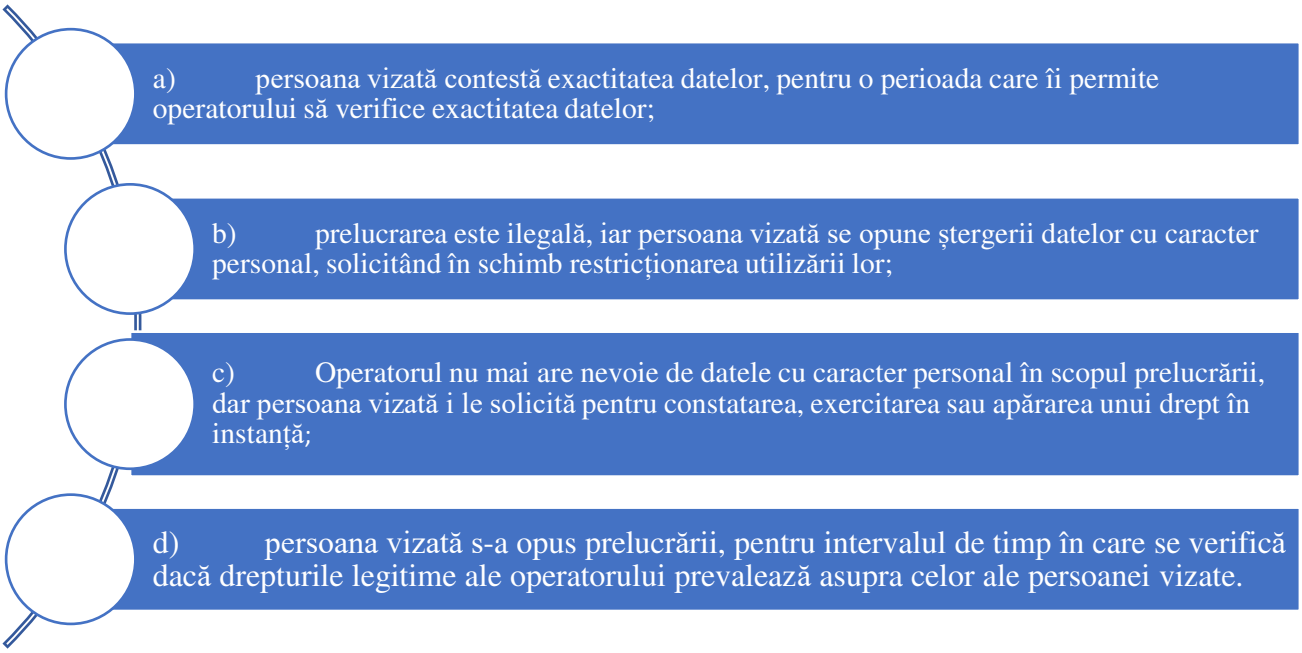
Exemplul 1: În situația în care un student/cursant se retrage din cadrul UNEFS, acestea nu mai sunt necesare pentru îndeplinirea scopurilor pentru care au fost colectate ori prelucrate.
Exemplul 2: În situația în care se organizează tabere în cadrul unor bazelor sportive ale UNEFS (de exemplu, bazele didactice Parâng și Eforie Nord), datele personale ale acestuia, asupra cărora există acordul părintelui/reprezentantului legal/tutorelui pentru prelucrare, nu mai sunt necesare pentru îndeplinirea scopurilor pentru care au fost inițial colectate și prelucrate.
Exemplul 3: Părintele/reprezentantul legal al unui student/cursant intră o singură dată în clădirile UNEFS, fără a mai reveni, iar la plecare solicită să i se șteargă datele cu caracter personal, datele de identificare întrucât colectarea acestora, respectiv pentru vizita în clădirile UNEFS, și-au atins scopul.

8.8 Ștergerea datelor nu este obligatorie în cazul în care prelucrarea este necesară:



D) Dreptul la restricționarea prelucrării

8.9 În cazul în care se solicită restricționarea prelucrării datelor cu caracter personal, trebuie avut în vedere că persoana vizată are dreptul de a obține din partea operatorului restricționarea prelucrării în cazul în care se aplică unul din următoarele cazuri:



Exemplul 1: Situația în care un fost student/ cursant/ doctorand/ masterand solicită foaia matricolă ori alte rezultate școlare mai detaliate pentru constatarea unor drepturi.

Exemplul 2: Situația în care un fost angajat al UNEFS solicită adeverință pentru calculul vechimii în muncă și al grupei (constatarea unor drepturi).
Exemplul 3: UNEFS, asemeni altor universități, se promovează atât pe plan intern cât și pe plan internațional. Există însă posibilitatea ca anumiți cursanți/studenţi cu rezultate foarte bune să solicite restricționarea datelor cu caracter personal pentru promovarea UNEFS.

E) Dreptul la portabilitatea datelor

8.10 Dreptul la portabilitatea datelor implică obligația UNEFS, atunci când acționează ca operator, de a asigura (i) furnizarea datelor primite de la persoană vizată într-un format accesibil la cererea acesteia și (ii) transmiterea unor astfel de date către alți operatori la cererea persoanei vizate, incidentă când următoarele condiții cumulative sunt îndeplinite:
• privește datele furnizate de persoană vizată;
• prelucrarea se bazează pe consimțământ sau este necesară pentru executarea unui contract (inclusiv faza precontractuala);
• este efectuată prin mijloace automate;
Exemplu:
1) prima latură (furnizarea datelor/documentelor ce le conțin persoanei vizate): la solicitarea persoanei vizate înainte de încetarea colaborării de a preda toate documentele furnizate precum și copiile efectuate după acestea în format electronic, UNEFS are obligația de a se conforma cu o asemenea cerere.
(2) portarea datelor către o altă universitate, în situație de transfer – dacă la încetarea colaborării persoana vizată solicita transmiterea datelor deținute în formă electronică către noua universitate, conform dreptului la portabilitate, dacă este tehnic posibil, solicitarea sa ar trebui să primească un răspuns pozitiv.

F) Dreptul de opoziție la prelucrarea datelor

8.11 Persoana vizată se poate opune oricând la prelucrarea datelor sale cu caracter personal:
a) din motive legate de situația particulară în care se află, operațiunilor de prelucrare desfășurate în temeiul necesității prelucrării pentru îndeplinirea unei sarcini care servește unui interes public cu care este investită UNEFS; și/ sau prelucrărilor efectuate în temeiul intereselor legitime urmărite de UNEFS sau de o parte terță a datelor cu caracter personal, inclusiv creării de profiluri.
b) fără motive și justificare, în cazul prelucrării datelor în scopuri de marketing direct (ex. pentru promovarea serviciilor UNEFS).

8.12 UNEFS nu mai poate prelucra datele cu caracter personal în cazul opunerii, cu excepția cazului în care demonstrează că are motive legitime și imperioase care justifică prelucrarea și care prevalează asupra intereselor, drepturilor și libertăților persoanei vizate sau ca scopul prelucrării este constatarea, exercitarea sau apărarea unui drept în instanță.

Exemplu: prelucrarea datelor cu caracter personal pentru eliberarea adeverințelor cerute de autorități pentru calculul pensiei și al vechimii în muncă. În atare situație, scopul este unul legitim, întrucât vizează constatarea unor drepturi în instanță ori în fața Casei Naționale de Pensii Publice.

G) Dreptul de a nu fi supus unor decizii automatizate, inclusiv profilarea

8.13 În general, persoana vizată are dreptul de a nu face obiectul unei decizii bazate exclusiv pe prelucrarea automată, inclusiv crearea de profiluri, care produce efecte juridice care privesc persoana vizată sau o afectează în mod similar într-o măsură semnificativă.
8.14 Prelucrarea datelor pentru luarea de decizii automatizate este permisă când:
(a) este necesară pentru încheierea sau executarea unui contract între persoana vizată și operatorul de date;
(b) este autorizată prin dreptul Uniunii sau dreptul intern care prevede, de asemenea, măsuri corespunzăoare pentru protejarea drepturilor, libertăților și intereselor legitime ale persoanei vizate;
(c) are la bază consimțământul explicit al persoanei vizate.
Exemplu: situația in care unui student/cursant/doctorand/masterand i se creează un profil automatizat ori i se dă un spațiu pe intranet cu o parolă de acces, pentru verificarea situației rezultatelor școlare, asigurându-se astfel operatorul ca persoana vizată este singura care are acces la acele date/informații.

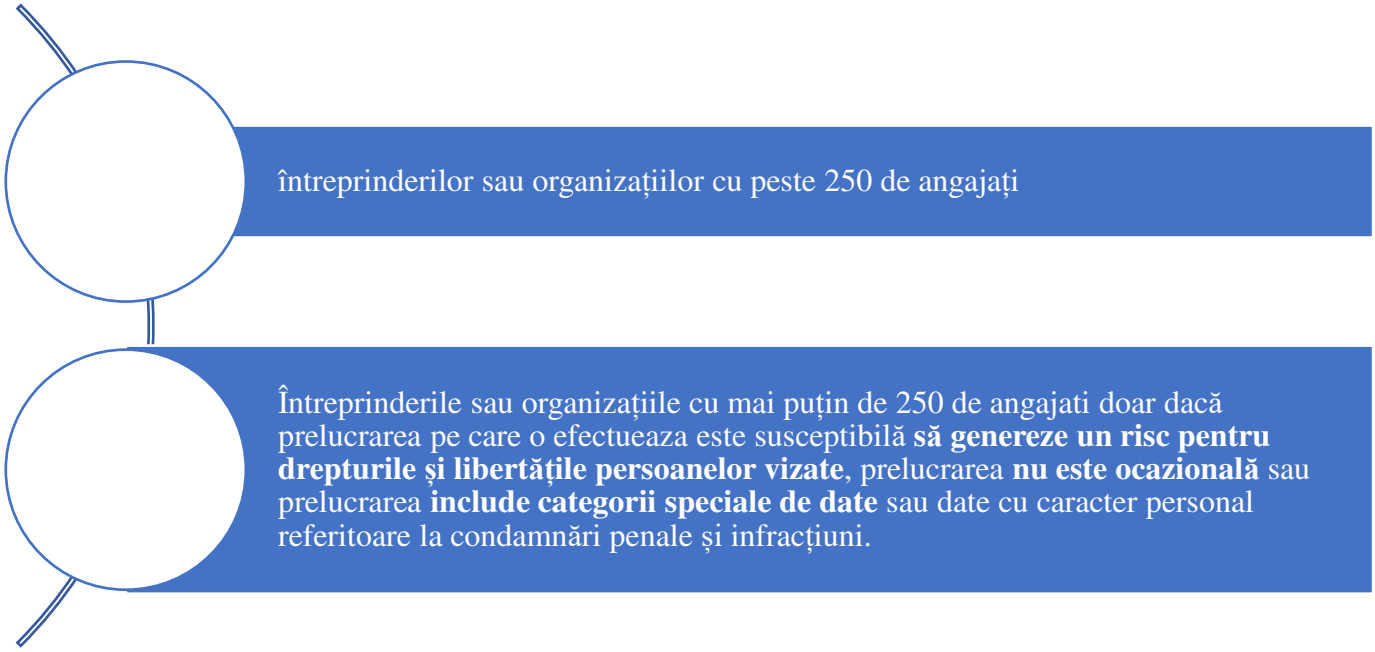
9) Mecanisme de răspuns la cererile de exercitare a drepturilor persoanelor vizate

9.1 Pentru a asigura tratarea cu celeritate a cererilor persoanei vizate pentru exercitarea drepturilor specifice, respectiv a cererilor altor entități (pentru cazurile în care UNEFS acționează în calitate de persoana imputernicită, dacă este cazul), următoarele mecanisme pot fi avute în vedere:
a) Alocarea unei / unor persoane care să se ocupe de tratarea în timp util a cererilor persoanelor vizate, care să răspundă în scris la asemenea solicitări;
b) Redactarea unor formulare de exercitare a drepturilor / răspuns tipizate care să fie utilizate atunci când persoana vizată își exercită drepturile specifice;
c) Dacă cererile sunt transmise prin mijloace electronice, răspunsul trebuie transmis prin aceleași mijloace, dacă persoanele vizate nu solicită altfel;
d) Implementarea unor secțiuni specifice pentru exercitarea drepturilor persoanei vizate online, în special în cazurile în care colectarea datelor se realizează online;
e) Pentru formele de exercitare cu personal numeros, conceperea unei proceduri specifice cu reguli clare de urmat în cazul primirii unor astfel de cereri, inclusiv cu principiile de avut in vedere în contextul conceperii răspunsurilor la cererile specifice.
9.2 În cazul în care există îndoieli întemeiate cu privire la identitatea persoanei fizice care înaintează cererea pentru exercitarea drepturilor specifice, operatorul poate solicita furnizarea de informații suplimentare necesare pentru a confirma identitatea persoanei vizate.
9.3 (1) Soluționarea cererilor se va realiza fără întârzieri nejustificate, în termen de cel mult 1 lună de la data recepționării acestora.
(2) Perioada de soluționare a cererilor poate fi prelungită cu două luni atunci când este necesar, ținându-se seama de complexitatea și numărul cererilor. În acest caz, persoana vizată trebuie să fie informată cu privire la orice astfel de prelungire, în termen de o lună de la primirea cererii, prezentând și motivele întârzierii. În cazul în care persoana vizată introduce o cerere în format electronic, informațiile sunt furnizate în format electronic acolo unde este posibil, cu excepția cazului în care persoană vizată solicită un alt format.

(3) Dacă nu se iau măsuri cu privire la cererea persoanei vizate, persoană vizată este informată, fără întârziere şi în termen de cel mult o lună de la primirea cererii, cu privire la motivele pentru care nu ia masuri şi la posibilitatea de a depune o plângere în faţa autorității de supraveghere şi de a introduce o cale de atac judiciară.
9.4 (1) Informațiile furnizate în temeiul solicitărilor persoanei vizate în exercitarea drepturilor specifice, orice comunicare și orice măsuri luate în temeiul acestora sunt oferite gratuit. În cazul în care cererile din partea unei persoane vizate sunt în mod vădit nefondate sau excesive, în special din cauza caracterului lor repetitiv, operatorul poate:
(a) fie să perceapă o taxă rezonabilă ținând cont de costurile administrative pentru furnizarea informațiilor sau a comunicării sau pentru luarea măsurilor solicitate;
(b) fie să refuze să dea curs cererii.
(2) În aceste cazuri, operatorului îi revine sarcina de a demonstra caracterul vădit nefondat sau excesiv al cererii.
9.5 UNEFS păstrează evidențe clare ale răspunsurilor date în contextul cererilor persoanei vizate de exercitare a drepturilor specifice în materie de prelucrare a datelor cu caracter personal, atât când acționează ca operator cât și ca persoana împuternicită, astfel:
a) UNEFS operator trebuie să aibă dovezi clare scrise (conținând inclusiv răspunsurile și data transmiterii acestora) care să ateste îndeplinirea obligațiilor specifice în materie; în atare condiții, păstrarea evidenței se va realiza pe două paliere: solicitări primite cu toate informațiile aferente cu evidențierea datei primirii acestora și respectiv răspunsuri transmise, cu evidențierea datei transmiterii răspunsurilor, iar unde este cazul de prelungire a termenului de răspuns după o lună, cu indicarea clară a motivului prelungirii.
b) UNEFS persoană împuternicită trebuie să aibă dovezi scrise care să susțină transmiterea în termen util a informațiilor solicitate respectiv implementarea în mod rezonabil a măsurilor necesare pentru conformarea cu drepturile specifice ale persoanei vizatea operatorilor care le solicită informații / luarea de măsuri specifice.
c) De principiu, UNEFS păstrează dovezile în formă scrisă. Cu toate acestea, dacă persoana vizată solicită anumite informații oral, este admisibilă și păstrarea unor dovezi ale înregistrărilor care să ateste răspunsul acordat unor asemenea solicitari.

10) Evidențele operațiunilor de prelucrare

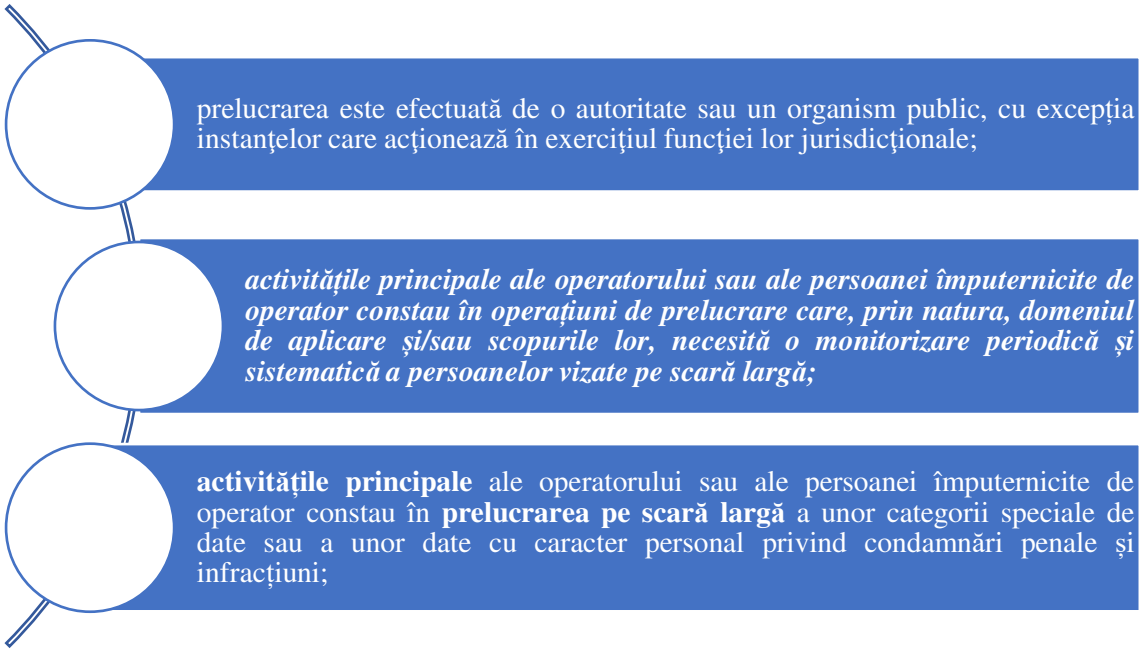
incumbă:



10.1 Evidența menținută de operator și, după caz, de reprezentanții acestuia trebuie să cuprindă următoarele informații:
(a) numele și datele de contact ale operatorului și, după caz, ale operatorului asociat, ale reprezentantului operatorului și ale responsabilului cu protecția datelor;
(b) scopurile prelucrării;
(c) o descriere a categoriilor de persoane vizate și a categoriilor de date cu caracter personal;
(d) categoriile de destinatari cărora le-au fost sau le vor fi divulgate datele cu caracter personal, inclusiv destinatarii din țări terțe sau organizații internaționale;
(e) dacă este cazul, transferurile de date cu caracter personal către o țară terță sau o organizație internațională;
(f) acolo unde este posibil, termenele-limită preconizate pentru ștergerea diferitelor categorii de date;
(g) acolo unde este posibil, o descriere generală a măsurilor tehnice și organizatorice de securitate.
10.2 Fiecare operator și, după caz, persoana împuternicită de operator păstrează o evidență a tuturor categoriilor de activități de prelucrare desfășurate în numele operatorului, care cuprind:
(a) numele și datele de contact ale persoanei sau persoanelor împuternicite de operator și ale fiecărui operator în numele căruia acționează această persoană (aceste persoane), precum și ale reprezentantului operatorului sau al persoanei împuternicite de operator, după caz;
(b) categoriile de activități de prelucrare desfășurate în numele fiecărui operator;
(c) dacă este cazul, transferurile de date cu caracter personal către o țară terță sau o organizație internațională;
(d) acolo unde este posibil, o descriere generală a măsurilor tehnice și organizatorice de securitate.

11) Responsabilul pentru protecția datelor cu caracter personal - DPO

11.1 Când este obligatoriu ca UNEFS să numească un DPO



11.2 ***Activități principale -*** înseamnă operațiuni-cheie pentru atingerea scopurilor operatorului / persoanei împuternicite, fără a exclude însă activitățile în care prelucrarea datelor cu caracter personal este o parte integrantă a activității operatorului / persoanei împuternicite.
Exemplu: Activitatea principală a UNEFS este de a oferi educație școlară și activitate didactico-științifică și de cercetare în educație fizică, sport și kinetoterapie. Însă, UNEFS nu poate oferi activitățile respective în condiții de siguranță și în mod eficient fără prelucrarea datelor privind starea de sănătate si situația școlară a acestora, toate regăsindu-se în dosarele studenților/cursanților/doctoranzilor/masteranzilor. Prin urmare, prelucrarea acestor date ar trebui să fie considerată a fi una dintre activitățile principale în unitate de învățământ și, prin urmare, UNEFS trebuie să desemneze un DPO.
În egală măsură, UNEFS efectuează la rândul său anumite activități, spre exemplu, plata angajaților lor sau deținerea de activități standard de suport IT. Acestea sunt exemple de funcții de sprijin necesare pentru activitatea de bază sau principală a organizației. Chiar dacă aceste activități sunt necesare sau esențiale, acestea sunt de obicei considerate mai degrabă funcții auxiliare decât activitate principală, însa presupun prelucrare de date cu caracter personal și necesită un DPO.

11.3 ***Prelucrare pe scară largă***
GDPR nu oferă criterii precise pentru a valida acest element. O serie de criterii orientative de care trebuie ţinut cont în calificarea unei prelucrări ca fiind „pe scară largă”: numărul de persoane vizate / proporția din populația relevantă, volumul și varietatea datelor personale prelucrate, durata prelucrării, întinderea geografică.
Exemple de prelucrări pe scara largă includ:

- prelucrarea datelor studenților/cursanților în activitatea regulată a structurilor UNEFS;
- prelucrarea datelor personalului didactic, didactic auxiliar și al administrativ;

11.4 ***Monitorizare periodică și sistematică***

i. monitorizare înseamnă orice formă de urmărire și profilare în mediu online, dar nu sunt excluse și forme de monitorizare „clasică”;
ii. „periodic” înseamnă una sau mai multe din următoarele: în curs de desfășurare sau care apare la anumite intervale într-o anumită perioadă; recurente sau repetate la perioade fixe; constante sau care au loc periodic;
iii. „sistematic” înseamnă una sau mai multe din următoarele: apărut conform sistemului; prearanjat, organizat sau metodic; luând loc ca parte a unui plan general de colectare a datelor; efectuat ca parte a unei strategii;
iv. Exemple de activități care pot constitui o monitorizare periodică și sistematică a persoanei vizate: operarea unei rețele de telecomunicații; furnizarea de servicii de telecomunicații; operarea bazelor de date ale studenților/cursanților/doctoranzilor ori masteranzilor; e-mail de direcționare repetată; profilare și scoring în scopul evaluării riscurilor (de exemplu, în scopul de credit scoring, stabilirea primelor de asigurare, de prevenire a fraudelor, detectarea spălării banilor); urmărirea locației, spre exemplu, prin aplicații mobile; programe de loialitate; publicitate comportamentală; monitorizarea wellness, fitness și a datelor de sănătate prin intermediul dispozitivelor portabile; televiziune cu circuit inchis; dispozitive conectate spre exemplu, contoare inteligente, mașini inteligente, etc.

11.5 Obligația de numire a unui DPO se aplică atât operatorului cât și persoanelor împuternicite de operator. În funcție de cine îndeplinește criteriile de desemnare obligatorie, în unele cazuri numai operatorul sau numai persoana împuternicită de operator, iar în alte cazuri atât operatorul, cât și persoana împuternicită de operator sunt obligați să numească un DPO.
11.6 DPO desemnat de o persoană împuternicită supraveghează, de asemenea, activitățile desfășurate de persoana împuternicită atunci când aceasta acționează în calitate de operator (spre exemplu resurse umane, IT, logistică, administrativ).

12) Principalele sarcini ale unui DPO

12.1 Responsabilul cu protecția datelor are cel puțin următoarele sarcini:
(a) informarea și consilierea operatorului sau a persoanei împuternicite de operator, precum și a angajaților care se ocupă de prelucrare cu privire la obligațiile care le revin în temeiul prezentului regulament și al altor dispoziții de drept al Uniunii sau drept intern referitoare la protecția datelor;
(b) monitorizarea respectării prezentului regulament, a altor dispoziții de drept al Uniunii sau de drept intern referitoare la protecția datelor și a politicilor operatorului sau ale persoanei împuternicite de operator în ceea ce privește protecția datelor cu caracter personal, inclusiv alocarea responsabilităților și actiunile de sensibilizare și de formare a personalului implicat în operațiunile de prelucrare, precum și auditurile aferente;
(c) furnizarea de consiliere la cerere în ceea ce privește evaluarea impactului asupra protecției datelor și monitorizarea funcționării acesteia;
(d) cooperarea cu autoritatea de supraveghere;

(e) asumarea rolului de punct de contact pentru autoritatea de supraveghere privind aspectele legate de prelucrare, inclusiv consultarea prealabilă, precum şi, dacă este cazul, consultarea cu privire la orice altă chestiune.

12.2. Regulamentul impune o serie de garanții pe care UNEFS trebuie să le ofere DPO în vederea îndeplinirii sarcinilor și rolului acestuia stabilite prin Regulament.

Este implicat în mod corespunzător și în timp util în toate aspectele legate de protecția datelor cu caracter personal	• DPO este invitat să participe în mod regulat la sedințele conducerii la nivel inalt și la nivel mediu. • Prezența DPO este recomandată în cazul în care se iau decizii cu implicații asupra protecției datelor. Toate informațiile relevante trebuie să fie transmise DPO în timp util pentru a permite ca acesta să ofere o consiliere corespunzătoare. • Avizului DPO trebuie să i se acorde întotdeauna o importanță deosebită. În caz de dezacord, ca bună practică, documentarea motivelor pentru care nu a fost urmat avizul DPO. • DPO trebuie să fie consultat cu promptitudine imediat ce a avut loc o încălcare a securității datelor sau un alt incident.
I se asigură resursele necesare pentru executarea sarcinilor ce îi revin, precum și accesarea datelor cu caracter personal și a operațiunilor de prelucrare, și pentru menținerea cunostințelor sale de specialitate	• Sprijin activ al funcţiei DPO din partea managementului superior (cum ar fi la nivelul conducerii structurilor din cadrul UNEFS). • Timp suficient pentru DPO în vederea îndeplinirii atribuțiilor sale. • Sprijin corespunzător în ceea ce privește resursele financiare, infrastructură (sediu, facilitati, echipament) și personal, după caz. • Comunicare oficială către toți angajații cu privire la desemnarea DPO astfel încât să se asigure că este cunoscută existența şi funcţionarea DPO. • Accesul necesar la alte servicii precum resurse umane, juridic, IT, securitate etc. astfel încât DPO să beneficieze de un sprijin esențial, reacții și informații din partea altor servicii. • Pregătire continuă. DPO trebuie să aibă posibilitatea de a rămâne la curent cu evoluțiile în domeniul protecției datelor.
DPO nu primește niciun fel de instrucțiuni în ceea ce privește îndeplinirea sarcinilor sale	• În îndeplinirea sarcinilor ce îi revin, DPO nu trebuie să fie instruit cum să se ocupe de o problemă.

	• Acesta nu trebuie să fie instruit să adopte o anumită perspectivă a problemei legată de legislația privind protecția datelor, de exemplu, o anumită interpretare a legii. • DPO răspunde direct în fața celui mai înalt nivel al conducerii operatorului sau persoanei împuternicite de operator
Demiterea sau sancționarea DPO	• DPO nu poate să fie demis sau sancționat de operator sau persoana împuternicită de operator pentru îndeplinirea sarcinilor sale. • Sancțiunile sunt interzise potrivit GDPR numai în cazul în care acestea sunt impuse ca urmare a îndeplinirii sarcinilor DPO în calitate de DPO. De exemplu, un DPO nu poate fi demis pentru oferirea unei opinii privind prelucrarea datelor personale. • Un DPO ar putea fi totuși demis, în mod legal, din alte motive decât cele privind îndeplinirea sarcinilor sale în calitate de DPO.
Poziția de DPO nu trebuie să genereze un conflict de interese	În principiu, DPO nu poate exercita o funcție care îi permite să determine scopurile sau mijloacele unei prelucrari. DPO incompatibil cu o poziție de conducere / de decizie sau în situația în care un DPO extern este rugat să reprezinte oporatorul sau persoana împuternicită de operator în instanță, în cazurile care implică probleme de protecție a datelor. Bune practici pentru UNEFS: - să identifice funcțiile ce ar fi incompatibile cu funcția de DPO; - să elaboreze norme interne pentru a evita conflictele de interese; - să realizeze o declarație în sensul că DPO nu are niciun conflict de interese în ceea ce privește funcția sa; - să includă garanții în normele interne ale UNEFS și să se asigure că anunțul de post vacant pentru funcția de DPO sau contractul de prestari servicii este suficient de precis şi detaliat pentru a evita conflictul de interese.

13) Evaluarea impactului asupra protecției datelor - DPIA

13.1 (1) Evaluarea impactului asupra protecției datelor intervine atunci când prelucrarea, în special cea bazată pe noile tehnologii, este susceptibilă să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice.
(2) O evaluare unică poate fi utilizată pentru analiza unor operațiuni de procesare multiple care prezintă similitudini din perspectiva riscului generat;
(3) Evaluarea trebuie realizată anterior prelucrării datelor cu caracter personal.
13.2 Evaluarea conține cel puțin:
(a) o descriere sistematică a operațiunilor de prelucrare preconizate și a scopurilor prelucrării, inclusiv, după caz, interesul legitim urmărit de operator;
(b) o evaluare a necesității și proportionalității operațiunilor de prelucrare în legătură cu aceste scopuri;
(c) o evaluare a riscurilor pentru drepturile și libertățile persoanei vizate;
(d) măsurile preconizate în vederea abordării riscurilor, inclusiv garanțiile, măsurile de securitate și mecanismele menite să asigure protecția datelor cu caracter personal și să demonstreze conformitatea cu dispozițiile prezentului regulament, luând în considerare drepturile și interesele legitime ale persoanei vizate și ale persoanei interesate.

13.3 (1) DPIA este necesară atunci când o operațiune de prelucrare „este susceptibilă să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice”. Ca exemplu, prelucrarea pe scară largă datelor privind starea de sănătate este considerată ca fiind susceptibilă să genereze un risc ridicat și necesită o DPIA.
(2) Atunci este responsabilitatea operatorului de date să evalueze riscurile pentru drepturile și libertățile persoanei vizate și să identifice măsurile prevăzute pentru a reduce aceste riscuri la un nivel acceptabil și pentru a demonstra conformitatea cu GDPR. Un exemplu ar putea fi utilizarea unor măsuri de securitate tehnice și organizaționale adecvate (criptarea eficientă a discului complet, gestionarea robustă a cheilor, controlul adecvat al accesului, copiile securizate etc.) pe lângă politicile existente (notificarea, consimțământul, dreptul de acces, dreptul de a se opune etc.) pentru stocarea datelor cu caracter personal pe computerele portabile.

14) Confidențialitatea și securitatea

14.1 Operatorul și persoana împuternicită de acesta trebuie să implementeze măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător acestui risc, incluzând printre altele, după caz:
a) pseudonimizarea și criptarea datelor cu caracter personal;
b) capacitatea de a asigura confidențialitatea, integritatea, disponibilitatea și rezistența continue ale sistemelor și serviciilor de prelucrare;
c) capacitatea de a restabili disponibilitatea datelor cu caracter personal și accesul la acestea în timp util în cazul în care are loc un incident de natura fizică sau tehnică;
d) un proces pentru testarea, evaluarea și aprecierea periodice ale eficacității măsurilor tehnice și organizatorice pentru a garanta securitatea prelucrării.

14.2 (1) Este necesar să se stabilească dacă au fost implementate toate măsurile tehnologice de protecție și organizatorice corespunzătoare în scopul de a se stabili imediat dacă s-a produs o încălcare a securității datelor cu caracter personal și de a se informa cu promptitudine autoritatea de supraveghere și persoana vizată.
(2) Există diferite exemple de încălcări ale securității datelor: atacuri informatice tip ransomware, pierderea cheii de criptare a datelor, nefuncţionarea sistemelor informatice, pierderea unor documente, transmiterea unei corespondenţe la adresa gresită etc.).
(3) Încălcările de securitate pot avea cauze diferite: de la nefuncționarea sau funcționarea necorespunzătoare a sistemelor informatice până la erori umane.
(4) Este foarte important ca operatorul să se asigure că indiferent de cauza acesteia și forma în care se manifestă, apariția unei breșe de securitate este identificată imediat și adusă în mod corespunzător la cunoștința persoanelor competente să implementeze măsurile care se impun.
(5) Pentru gestionarea incidentelor de securitate, UNEFS va desemna una sau mai multe echipe, pentru fiecare structură din cadrul UNEFS, dacă este cazul, care va acționa pentru gestionarea rapidă și eficientă a incidentelor de securitate a datelor cu caracter personal.
14.3 În cazul în care are loc o încălcare a securității datelor cu caracter personal, operatorul are obligația de a notifica acest lucru autorității de supraveghere, fără întârzieri nejustificate și, dacă este posibil, în termen de cel mult 72 de ore de la data la care a luat cunoștință de aceasta, cu excepția cazului în care este susceptibilă să genereze un risc pentru drepturile și libertățile persoanelor fizice.
14.4 Notificarea trimisă autorității de supraveghere conține cel puțin următoarele:
(a) descrie caracterul încălcării securității datelor cu caracter personal, inclusiv, acolo unde este posibil, categoriile şi numărul aproximativ al persoanelor vizate în cauză, precum și categoriile și numărul aproximativ al înregistrărilor de date cu caracter personal în cauză;
(b) comunică numele și datele de contact ale responsabilului cu protecția datelor sau un alt punct de contact de unde se pot obține mai multe informații;
(c) descrie consecințele probabile ale încălcării securității datelor cu caracter personal;
(d) descrie măsurile luate sau propuse spre a fi luate de operator pentru a remedia problema încălcării securității datelor cu caracter personal, inclusiv, după caz, măsurile pentru atenuarea eventualelor sale efecte negative.
14.5 Atunci când și în măsura în care nu este posibil să se furnizeze informațiile în același timp, acestea pot fi furnizate în mai multe etape, fără întârzieri nejustificate.
14.6 În cazul în care încălcarea securității datelor cu caracter personal este susceptibilă să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice, operatorul informează persoana vizată fără întârzieri nejustificate cu privire la această încălcare.
14.7 Informarea persoanei vizate nu este necesară în cazul în care oricare dintre următoarele condiții este îndeplinită:
(a) operatorul a implementat măsuri de protecție tehnice și organizatorice adecvate, iar aceste măsuri au fost aplicate în cazul datelor cu caracter personal afectate de încălcarea securității datelor cu caracter personal, în special măsuri prin care se asigură că datele cu caracter personal devin neinteligibile oricărei persoane care nu este autorizată să le acceseze, cum ar fi criptarea;
(b) operatorul a luat măsuri ulterioare prin care se asigură ca riscul ridicat pentru drepturile și libertățile persoanei vizate nu mai este susceptibil să se materializeze;
(c) ar necesita un efort disproporționat. În această situație, se efectuează pe loc o informare publică sau se ia o masură similară prin care persoana vizată sunt informate într-un mod la fel de eficace.

Regulamentul nu prescrie un anume formalism pentru informarea persoanei vizate. Dacă circumstanțele concrete nu reclamă o alta abordare, informarea se va face printr-o comunicare adresată direct persoanei vizate, printr-un mijloc de comunicare corespunzator (poștă electronică).

14.8 Operatorul păstrează documente referitoare la toate cazurile de încălcare a securității datelor cu caracter personal, care cuprind o descriere a situației de fapt în care a avut loc încălcarea securității datelor cu caracter personal, a efectelor acesteia și a măsurilor de remediere întreprinse.

15) Transferul datelor cu caracter personal către state terțe sau o organizație internațională

15.1 Transferul de date cu caracter personal către o țară terță sau o organizație internațională se poate realiza atunci când :

I. Comisia a decis ca țară terță, un teritoriu ori unul sau mai multe sectoare specificate din acea țară terță sau organizația internațională în cauză asigură un nivel de protecție adecvat. Transferurile realizate în aceste condiții nu necesită autorizări speciale". Decizia Comisiei în acest sens este obligatorie pentru toate statele membre UE.

II. În absența unei decizii a Comisiei care să constate asigurarea unui nivel adecvat de protecție, datele cu caracter personal pot fi transferate către state terțe sau organizații internaționale doar dacă (i) operatorul sau persoană împuternicită de operator a oferit garanții adecvate și (ii) cu condiția să existe drepturi opozabile și căi de atac eficiente pentru persoanele vizate.

Aceste garanții adecvate pot fi furnizate fără să fie nevoie de nicio autorizație specifică din partea unei autorități de supraveghere, prin:
a) un instrument obligatoriu din punct de vedere juridic și executoriu între autoritățile sau organismele publice;
b) reguli corporatiste obligatorii în conformitate cu articolul 47 din Regulament;
c) clauze standard de protecție a datelor adoptate de Comisie în conformitate cu procedura de examinare menționată la articolul 93 alineatul (2) din Regulament;
d) clauze standard de protecție a datelor adoptate de o autoritate de supraveghere și aprobate de Comisie în conformitate cu procedura de examinare menționată la articolul 93 alineatul (2) din Regulament;
e) un cod de conduită aprobat în conformitate cu articolul 40 din Regulament, însoțit de un angajament obligatoriu și executoriu din partea operatorului sau a persoanei împuternicite de operator din țară terță de a aplica garanții adecvate, inclusiv cu privire la drepturile persoanelor vizate;
f) un mecanism de certificare aprobat în conformitate cu articolul 42 din Regulament, însoțit de un angajament obligatoriu și executoriu din partea operatorului sau a persoanei împuternicite de operator din țară terță de a aplica garanții adecvate, inclusiv cu privire la drepturile persoanelor vizate.

III. În absența unei decizii a Comisiei privind caracterul adecvat al nivelului de protecție sau a unor garanții adecvate, un transfer de date cu caracter personal către o țară terță sau o organizație internațională poate avea loc numai în una dintre condițiile următoare (derogări pentru situaţii specifice):

(a) persoana vizată şi-a exprimat în mod explicit acordul cu privire la transferul propus, după ce a fost informată asupra posibilelor riscuri pe care astfel de transferuri le pot implica pentru persoana vizată ca urmare a lipsei unei decizii privind caracterul adecvat al nivelului de protecție și a unor garanții adecvate;
(b) transferul este necesar pentru executarea unui contract între persoana vizată și operator sau pentru aplicarea unor măsuri precontractuale adoptate la cererea persoanei vizate;
(c) transferul este necesar pentru încheierea unui contract sau pentru executarea unui contract încheiat în interesul persoanei vizate între operator și o altă persoană fizică sau juridică;
(d) transferul este necesar din considerente importante de interes public;
(e) transferul este necesar pentru stabilirea, exercitarea sau apărarea unui drept în instanță;
(f) transferul este necesar pentru protejarea intereselor vitale ale persoanei vizate sau ale altor persoane, atunci când persoana vizată nu are capacitatea fizică sau juridică de a-și exprimă acordul;
(g) transferul se realizează dintr-un registru care, potrivit dreptului Uniunii sau al dreptului intern, are scopul de a furniza informații publicului și care poate fi consultat fie de public în general, fie de orice persoană care poate face dovada unui interes legitim, dar numai în măsura în care sunt îndeplinite condițiile cu privire la consultare prevăzute de dreptul Uniunii sau de dreptul intern în acel caz specific.

IV. În cazul în care un transfer nu ar putea să se intemeieze pe niciunul dintre temeiurile prezentate anterior inclusiv dispoziții privind reguli corporatiste obligatorii, si nu este aplicabilă niciuna dintre derogările pentru situații specifice, un transfer către o țară terță sau o organizație internațională poate avea loc numai în cazul în care:

a) transferul nu este repetitiv;
b) se referă doar la un număr limitat de persoane vizate;
c) este necesar în scopul realizării intereselor legitime majore urmărite de operator asupra căruia nu prevalează interesele sau drepturile și libertățile persoanei vizate;
d) operatorul a evaluat toate circumstanțele aferente transferului de date și, pe baza acestei evaluări, a prezentat garanții corespunzatoare în ceea ce privește protecția datelor cu caracter personal.

15.2 Operatorul informează autoritatea de supraveghere cu privire la transfer. Operatorul, în plus față de furnizarea informațiilor mentionate în prezenta Procedură, informează persoana vizată cu privire la transfer și la interesele legitime majore pe care le urmărește.

16) Atribuții și obligații specifice Operator (UNEFS)

16.1 Atribuții si obligații specifice UNEFS

(1) Conducerea structurilor UNEFS din cadrul acesteia sale sunt responsabili cu protecția datelor cu caracter personal și au următoarele atribuții principale:

a) stabilesc scopul și mijloacele de prelucrare a datelor cu caracter personal atunci când acestea sunt necesare pentru exercitarea unor competențe legale;
b) asigură elaborarea procedurilor proprii și, după aprobarea acestora de către Senatul universității, le pune în aplicare;
c) asigură implementarea și monitorizează respectarea normelor procedurale în materia prelucrării datelor cu caracter personal de către utilizatori;
d) coordonează și monitorizează activitatea personalului pe linia protecției datelor cu caracter personal la nivelul operatorului;
e) asigura desfășurarea pregătirii de specialitate și instruirea utilizatorilor în acest domeniu;
f) dispun măsuri de completare sau, după caz, de modificare a fișei posturilor utilizatorilor;
g) analizează și dispun în ceea ce privește suspendarea sau revocarea dreptului de acces al utilizatorilor la sisteme de evidență a datelor cu caracter personal, în condițiile legii;
h) dispun măsuri pentru exercitarea drepturilor de către persoana vizata;
i) coordonează soluționarea cererilor persoanelor vizate;
j) țin evidența cererilor persoanelor vizate;
k) analizează periodic activitatea utilizatorilor;
l) aprobă componența Comisiei de ștergere și distrugere a datelor cu caracter personal la nivelul structurilor UNEFS.
m) informează operativ Rectorul UNEFS despre vulnerabilitățile și riscurile semnalate în sistemul de securitate a prelucrării datelor cu caracter personal a structurii UNEFS și propune măsuri pentru înlăturarea acestora;
m.1) aprobă componența echipei/echipelor de gestionare a incidentelor de securitate a datelor cu caracter personal;
n) informează Rectorul UNEFS în legatură cu orice încălcare a normelor de protecție a datelor cu caracter personal de natură a prejudicia drepturile persoanei și limitarea efectelor unei diseminari neautorizate a datelor, precum și cu privire la situațiile în care au fost emise recomandări sau aplicate sancțiuni de către autoritatea națională de supraveghere sau când aceasta a dispus efectuarea unui control prealabil ori a unor investigații.

16.2 Obligații specifice utilizatori de date

(1) Utilizatorii au următoarele obligații specifice:

a) să cunoască și să aplice prevederile actelor normative din domeniul prelucrării datelor cu caracter personal precum și ale prezentei proceduri;
b) să informeze persoana vizată atunci când datele cu caracter personal sunt colectate direct de la aceasta, în condițiile legii, cu privire la: identitatea operatorului, scopul specific în care se face prelucrarea datelor, destinatarii sau categoriile de destinatari ai datelor, obligativitatea furnizării tuturor datelor cerute și consecințele refuzului de a le pune la dispozitie, drepturile prevazute de lege, în special drepturile de acces, de intervenție asupra datelor și de opoziție, dreptul de ștergere și condițiile în care pot fi exercitate aceste drepturi;
c) să prelucreze numai datele cu caracter personal necesare îndeplinirii atribuțiilor de serviciu și să acorde sprijin conducătorului operatorului pentru realizarea activităților specifice ale acestuia;
d) să păstreze confidențialitatea datelor prelucrate, a contului de utilizator, a parolei/ codului de acces la sistemele informatice/ baze de date prin care sunt gestionate date cu caracter personal;
e) să respecte măsurile de securitate, precum și celelalte reguli stabilite de operator;

f) să informeze de îndată conducerea operatorului despre împrejurări de natură a conduce la o diseminare neautorizată de date cu caracter personal sau despre o situație în care au fost accesate/ prelucrate date cu caracter personal prin încălcarea normelor legale, despre care a luat la cunoștință.

17) Măsuri tehnice generale privind prelucrarea datelor cu caracter personal

17.1 Măsurile tehnice privind prelucrarea si asigurarea datelor cu caracter personal sunt detaliate în cadrul Anexei nr. 1 - Procedura de asigurare a securității datelor cu caracter personal.

18) RESPONSABILITĂȚI

18.1 Responsabilul de proces – …….:

- elaborează/ revizuieşte procedura;
- aplică procedura/ monitorizează aplicarea procedurii.

18.2 CEAC

- verifică procedurile şi le înaintează structurilor spre revizie/ avizare/ aprobare, după caz;
- coordonează aplicarea procedurilor de asigurare şi evaluare a calităţii.

18.3 Prorectorat

- Verifică, modifică, avizează, retrage procedura.

18.4 Consiliul de Administrație

- analizează şi avizează procedura.

18.5 Rector UNEFS

- impune aplicarea procedurii
- asigură resurse pentru aplicarea procedurii

18.6 Senat

- aprobă procedura.

18.7 Directorii de departamente:

- aplică şi respectă prezenta procedură;
- difuzează procedura în cadrul compartimentului;
- organizează grupuri de lucru pentru discutarea şi aplicarea procedurii.

19) ÎNREGISTRĂRI

19.1. Calendar de elaborare proceduri

19.2 Documentele actuale ale UNEFS precum și cele aflate în arhiva UNEFS, inclusiv cele stocate în mediu electronic.

20) ANEXE ȘI FORMULARE

Anexa nr. 1- Procedura de asigurare a securității datelor cu caracter personal;
Anexa nr. 2 - Procedura de soluționare a cererilor formulate de persoana vizată;
Anexa nr. 3 - Procedura privind ștergerea și distrugerea datelor cu caracter personal;
Anexa nr. 4 - Procedura de prelucrare a datelor cu caracter personal aplicabilă candidaților în situația recrutării personalului didactic, didactic auxiliar, administrativ care se completează cu procedurile prevăzute de lege pentru învățământul superior
Anexa nr. 5 - Procedura de colectare și prelucrare a datelor la momentul depunerii dosarelor de către candidații la toate ciclurile (licență, master, doctorat) și formele de învățământ (universitar, postuniversitar, de pregătire a adulților sau cu frecvență redusă);
Anexa nr. 6 – Procedura de colectare și prelucrare a datelor aplicabilă studenților și personalului didactic care solicita echivalarea studiilor, recunoașterea acestora și a calității de doctor în știință;
Anexa nr. 7 – Procedura pentru gestionarea incidentelor de securitate
Anexa nr. 8 – Informarea persoanei vizate
Anexa nr. 9 - Registrul de evidență a datelor cu caracter personal.

21) LISTA DE DIFUZARE

1. Rectorat
2. Prorectorat
3. Facultatea de Educaţie Fizică şi Sport
4. Facultatea de Kinetoterapie
5. Școala Doctorală
6. Centrul de formare și Dezvoltare profesională
7. Secretariatul Universităţii
8. Direcţia Generală Administrativă
9. Direcţia Economică
10. Direcţia Resurse Umane
11. Oficiul Juridic