UNIVERSITATEA
SAPIENTIA

Decizia Senatului nr.
2475/12.02.2021. – anexa 8.

Regulamentul intern

privind protecția datelor cu caracter personal în cadrul Universității Sapientia

Subiect	Regulament intern GDPR
Instituția	Universitatea Sapientia
Versiune	1.1
Tipul documentului	Descriere sarcini
Întocmit	Pisak-Lukáts Ioan-Marius
Responsabil	Responsabilul pentru protecția datelor cu caracter personal
Data ultimei actualizări	12 februarie 2021
Interval actualizări	Anual, sau în cazul modificărilor legislative

Data	**Descrierea modificării**	**Autorul modificărilor**
15 iulie 2020	Întocmirea documentului	Pisak-Lukáts Ioan Marius

Cuprins

DISPOZIȚII GENERALE 5
Scop 5
Aplicare 5
Baza legală de reglemantare 5
Definiţii şi termeni specifici 5
Principii generale în prelucrarea datelor personale 7
Principiul confidenţialităţii 8
Principiul securităţii prelucrării datelor 8
Prelucrarea datelor sensibile 8
Incidente privind protecția datelor 8
Categorii de persoane care sunt vizate 8
Scopul general al colectării datelor 9
Modalităţi de colectare a datelor 9
Accesul la informaţiile cu caracter personal 9
Obligaţiile operatorului 10
Atribuţiile Responsabilul pentru protecția datelor cu caracter personal 10
Obligaţiile utilizatorilor 12
Drepturile persoanelor vizate 13
Responsabilități și sancțiuni 17
DISPOZIȚII SPECIFICE 19
Prelucrarea datelor personale ale salariaților 19
Evidența personalului. 19
Prelucrarea datelor personale ale candidaților prezentați în vederea angajării. 20
Prelucrarea datelor personale la verificarea aptitudinilor profesionale. 21
Reguli privind controlul mijloacelor puse la dispoziția salariatului de către angajator. 22
Prelucrarea datelor personale în vederea respectării unei obligații legale. 22
Prelucrarea datelor personale în vederea respectării obligațiilor privind taxele şi impozitele. 22
Prelucrarea datelor personale în vederea executării unor rețineri/popriri pe salariu 23
Măsuri specifice personalului didactic 23
Prelucrarea datelor personale ale candidaților prezentați în vederea angajării. 23
Sistemul informatic pentru gestionarea studiilor Neptun 24
Managementul calității 24
Activitatea de cercetare. Sistemul Online al Programelor de Cercetare, KPIOR 25
Reguli privind controlul mijloacelor puse la dispoziția salariatului de către angajator. 25
Prelucrarea datelor personale ale specialiștilor și/sau cadrelor didactice ale altor instituții în calitate de cadre didactice asociate invitate 25
Prelucrarea datelor personale ale cadrelor universitare aflate în mobilităţi Erasmus+, CEEPUS 26

Prelucrarea datelor personale ale studenților 26
Dispoziții specifice concursului de admitere 27
Candidaţi respinși la examenul de admitere și a cei neînscriși în primul an. 28
Absolvenți și foști studenți. Alumni 28
Servicii sociale - cămin studențesc, cantină. 28
Concursuri și conferințe 29
Sprijin material, burse, granturi Erasmus, CEEPUS, Makovecz acordate studenților 29
Vizite de documentare și schimb de experiență 30
Stagii de practică și cercetare 30
Reguli privind controlul mijloacelor puse la dispoziția studenților de către Universitate 30
Furnizare de date către Inspectoratele Teritoriale de Muncă 30
Datele personale ale partenerilor comerciali. 30
Prelucrarea datelor în scop publicitar 31
Prelucrarea datelor personale ale vizitatorilor site-ului web al Universității 32
Sistemul de supraveghere video al Universității 32

DISPOZIȚII GENERALE

Scop

Garantarea şi protejarea drepturilor şi libertaţilor fundamentale ale persoanelor fizice, în special a dreptului la viaţa intimă, familială şi privată, cu privire la prelucrarea datelor cu caracter personal, prin conformarea institutiei la Regulamentul Uniunii Europene nr.679/2016 privind protecţia datelor personale

Aplicare

Prezentul Regulament intern are ca obiect definirea metodelor de colectare, prelucrare, stocare, transmitere a datelor persoanelor fizice de către Universitatea Sapientia din Cluj-Napoca, cu sediul în Cluj-Napoca, str. Matei Corvin, Nr. 4., CP 400112. Regulamentul se aplică în cadrul activităţilor de prelucrare a datelor cu caracter personal efectuate, în totalitate sau în parte, prin mijloace automate, precum şi prelucrării prin alte mijloace decât cele automate a datelor cu caracter personal care fac parte dintr-un sistem de evidenţă sau care sunt destinate să fie incluse într-un asemenea sistem de structurile şi compartimentele Universităţii în calitate de operator sau de împuterniciţi ai operatorului.
Acest Regulament nu are ca obiect prelucrarea datelor persoanelor juridice.

Baza legală de reglemantare

Legea Educatiei Nationale 1/2011
Reglementările naţionale referitoare la sistemul de învățământ superiorLegea nr. 16/1996 a Arhivelor Naţionale
Legea nr. 544/2001 privind liberul acces la informaţiile de interes public.
Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul comunicaţiilor electronice.
Legea nr. 102/2005 privind înfiinţarea, organizarea şi funcţionarea Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal – ANSPDCP- (cu modificările ulterioare).
Regulamentul UE nr 679/2016 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
Regulemantele interne ale Universității Sapientia.

Definiţii şi termeni specifici

Conform Art. 4 din Regulamentul UE nr 679/2016, se definesc următoarele:
1. „date cu caracter personal” înseamnă orice informații privind o persoană fizică identificată sau identificabilă („persoana vizată”); o persoană fizică identificabilă este o persoană care poate fi identificată, direct sau indirect, în special prin referire la un element de identificare, cum ar fi un nume, un număr de identificare, date de localizare, un identificator online, sau la unul sau mai multe elemente specifice, proprii identității sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale;
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.
2. „prelucrare” înseamnă orice operațiune sau set de operațiuni efectuate asupra datelor cu caracter personal sau asupra seturilor de date cu caracter personal, cu sau fără utilizarea de mijloace automatizate, cum ar fi colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, divulgarea prin transmitere, diseminarea sau punerea la dispoziție în orice alt mod, alinierea sau combinarea, restricționarea, ștergerea sau distrugerea;

3. „restricționarea prelucrării” înseamnă marcarea datelor cu caracter personal stocate cu scopul de a limita prelucrarea viitoare a acestora;
4. „creare de profiluri” înseamnă orice formă de prelucrare automată a datelor cu caracter personal care constă în utilizarea datelor cu caracter personal pentru a evalua anumite aspecte personale referitoare la o persoană fizică, în special pentru a analiza sau prevedea aspecte privind performanța la locul de muncă, situația economică, sănătatea, preferințele personale, interesele, fiabilitatea, comportamentul, locul în care se află persoana fizică respectivă sau deplasările acesteia;
5. „pseudonimizare” înseamnă prelucrarea datelor cu caracter personal într-un asemenea mod încât acestea să nu mai poată fi atribuite unei anume persoane vizate fără a se utiliza informații suplimentare, cu condiția ca aceste informații suplimentare să fie stocate separat și să facă obiectul unor măsuri de natură tehnică și organizatorică care să asigure neatribuirea respectivelor date cu caracter personal unei persoane fizice identificate sau identificabile;
6. „sistem de evidență a datelor” înseamnă orice set structurat de date cu caracter personal accesibile conform unor criterii specifice, fie ele centralizate, descentralizate sau repartizate după criterii funcționale sau geografice;
7. „operator” înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care, singur sau împreună cu altele, stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal; atunci când scopurile și mijloacele prelucrării sunt stabilite prin dreptul Uniunii sau dreptul intern, operatorul sau criteriile specifice pentru desemnarea acestuia pot fi prevăzute în dreptul Uniunii sau în dreptul intern;
8. „persoană împuternicită de operator” înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care prelucrează datele cu caracter personal în numele operatorului;
9. „destinatar” înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism căreia (căruia) îi sunt divulgate datele cu caracter personal, indiferent dacă este sau nu o parte terță. Cu toate acestea, autoritățile publice cărora li se pot comunica date cu caracter personal în cadrul unei anumite anchete în conformitate cu dreptul Uniunii sau cu dreptul intern nu sunt considerate destinatari; prelucrarea acestor date de către autoritățile publice respective respectă normele aplicabile în materie de protecție a datelor, în conformitate cu scopurile prelucrării;
10. „parte terță” înseamnă o persoană fizică sau juridică, autoritate publică, agenție sau organism altul decât persoana vizată, operatorul, persoana împuternicită de operator și persoanele care, sub directa autoritate a operatorului sau a persoanei împuternicite de operator, sunt autorizate să prelucreze date cu caracter personal;
11. „consimțământ” al persoanei vizate înseamnă orice manifestare de voință liberă, specifică, informată și lipsită de ambiguitate a persoanei vizate prin care aceasta acceptă, printr-o declarație sau printr-o acțiune fără echivoc, ca datele cu caracter personal care o privesc să fie prelucrate;
12. „încălcarea securității datelor cu caracter personal” înseamnă o încălcare a securității care duce, în mod accidental sau ilegal, la distrugerea, pierderea, modificarea, sau divulgarea neautorizată a datelor cu caracter personal transmise, stocate sau prelucrate într-un alt mod, sau la accesul neautorizat la acestea, va fi folosit alternativ și termenul de “breșă de securitate”;
13. „date genetice” înseamnă datele cu caracter personal referitoare la caracteristicile genetice moștenite sau dobândite ale unei persoane fizice, care oferă informații unice privind fiziologia sau sănătatea persoanei respective și care rezultă în special în urma unei analize a unei mostre de material biologic recoltate de la persoana în cauză;
14. „date biometrice” înseamnă o date cu caracter personal care rezultă în urma unor tehnici de prelucrare specifice referitoare la caracteristicile fizice, fiziologice sau comportamentale ale unei persoane fizice care permit sau confirmă identificarea unică a respectivei persoane, cum ar fi imaginile faciale sau datele dactiloscopice;
15. „date privind sănătatea” înseamnă date cu caracter personal legate de sănătatea fizică sau mentală a unei persoane fizice, inclusiv prestarea de servicii de asistență medicală, care dezvăluie informații despre starea de sănătate a acesteia;
16. „autoritate de supraveghere” înseamnă o autoritate publică independentă instituită de un stat membru in temeiul articolului 51 / Regulament (UE) 679/2016;

17. „autoritate de supraveghere vizată” înseamnă o autoritate de supraveghere care este vizată de procesul de prelucrare a datelor cu caracter personal deoarece
(a) operatorul sau persoana împuternicită de operator este stabilita pe teritoriul statului membru al autorității de supraveghere respective;
(b) persoanele vizate care au reședința in statul membru în care se află autoritatea de supraveghere respectivă sunt afectate in mod semnificativ sau sunt susceptibile de a fi afectate in mod semnificativ de prelucrare; sau
(c) la autoritatea de supraveghere respectivă a fost depusă o plângere;
18. „prelucrare transfrontalieră” înseamnă:
(a) fie prelucrarea datelor cu caracter personal care are loc în contextul activităților sediilor din mai multe state membre ale unui operator sau ale unei persoane împuternicite de operator pe teritoriul Uniunii, dacă operatorul sau persoana împuternicită de operator are sedii in cel puțin două state membre; sau
(b) fie prelucrarea datelor cu caracter personal care are loc în contextul activităților unui singur sediu al unui operator sau al unei persoane împuternicite de operator pe teritoriul Uniunii, dar care afectează în mod semnificativ sau este susceptibilă de a afecta în mod semnificativ persoane vizate din cel puțin două state membre;
19. „obiecție relevantă și motivată” înseamnă o obiecție la un proiect de decizie în scopul de a stabili dacă există o încălcare a Regulamentului UE sau dacă măsurile preconizate în ceea ce privește operatorul sau persoana împuternicită de operator respectă prezentul regulament, care demonstrează în mod clar importanța riscurilor pe care le prezintă proiectul de decizie în ceea ce privește drepturile și libertățile fundamentale ale persoanelor vizate și, după caz, libera circulație a datelor cu caracter personal în cadrul Uniunii;
20. “stocarea” Păstrarea pe orice fel de suport a datelor cu caracter personal culese.
21. “codul numeric personal” Un număr semnificativ care individualizează în mod unic o persoană fizică, constituind un instrument de verificare a stării civile a acesteia și de identificare în anumite sisteme informatice de către persoanele autorizate.
22. „date anonime” Date care, datorită originii sau modalității specifice de prelucrare, nu pot fi asociate cu o persoană identificată sau identificabilă.
23. “date cu caracter personal cu funcție de identificare de aplicabilitate generală (date cu caracter special)” Numere prin care se identifică o persoană fizică în anumite sisteme de evidență și care au aplicabilitate generală, cum ar fi: codul numeric personal, seria si numărul actului de identitate, numărul pașaportului, al permisului de conducere, numărul de asigurare socială sau de sănătate.
24. “utilizator” Orice persoană care acționează sub autoritatea operatorului, a persoanei împuternicite sau a reprezentantului, cu drept recunoscut de acces la bazele de date cu caracter personal.
25. „procedură” Prezentarea în scris, a tuturor pașilor ce trebuie urmați, a metodelor de lucru stabilite si a regulilor de aplicat necesare îndeplinirii atribuțiilor și sarcinilor, având în vedere asumarea responsabilităților.
26. „procedură operațională” Prezentarea formalizată, în scris, a tuturor pașilor ce trebuie urmați, a metodelor de lucru stabilite și a regulilor de aplicat în vederea realizării activității, cu privire la aspectul procesual.
27. „ediție a unei proceduri operaționale” Forma inițială sau actualizată, după caz, a unei proceduri operaționale, aprobată și difuzată.
28. „revizia în cadrul unei ediții” Acțiunile de modificare, adăugare, suprimare sau altele asemenea, după caz, a uneia sau a mai multor componente ale unei ediții a procedurii operaționale, acțiuni care au fost aprobate și difuzate.

Principii generale în prelucrarea datelor personale

Principiul confidenţialităţii

Universitatea în calitatea de operator autorizat de colectare, prelucrare, stocare de date cu caracter personal va organiza activitatea asigurând pe tot parcursul activității în domeniu confidențialitatea datelor personale.
Angajaților/colaboratorilor/studenților li se interzice să colecteze, să prelucreze, să utilizeze date cu caracter personal în scopuri private sau comerciale, să le dezvăluie persoanelor neautorizate sau să le pună la dispoziție în orice alt mod. Această obligație rămâne în vigoare chiar și după încheierea perioadei de angajare/încetarea colaborării/încetarea calității de student.
Orice prelucrare de date efectuată de un angajat/colaborator/student care nu a fost autorizat să o îndeplinească, ca parte a îndatoririlor sale legitime de muncă, este neautorizată. Orice colectare, prelucrare sau utilizare neautorizată a datelor personale de către angajați/colaboratori/studenți este interzisă.
Angajații/colaboratorii/studenții pot avea acces la date personale numai pentru tipul și scopul sarcinii de serviciu în cauză. Conducerea fiecărui departament are obligația de a informa persoanele aflate în subordine despre obligația lor de a păstra confidențialitatea datelor personale.

Principiul securităţii prelucrării datelor

Datele personale sunt protejate împotriva accesului neautorizat, a prelucrării sau dezvăluirii ilegale, a pierderii, modificării sau distrugerii accidentale, indiferent de modul în care sunt stocate acestea (pe suport hârtie sau electronic).
Datele personale pot fi predate Poștei Române, unei firme de curierat în vederea transportului sau unei firme de pază și protecție.

Prelucrarea datelor sensibile

Datele cu caracter personal sensibile, cum ar fi date despre originea rasială, etnică, opiniile politice, credințele religioase sau filosofice, precum și date despre orientarea sexuală, vor fi prelucrate atunci când există o obligație legală. În condițiile actuale Universitatea nu prelucrează date sensibile în afara datelor privind starea de sănătate, dar numai cele absolut necesare din punct de vedere legal în cadrul raporturilor de muncă sau pentru acordarea unor drepturi, în cazul studenţilor.

Incidente privind protecția datelor

Fiecare angajat/colaborator sau student care ia cunoștință de încălcarea prevederilor acestui regulament sau a altor reglementări privind protecția datelor cu caracter personal (incidente de protecție a datelor) trebuie să informeze imediat șeful de departament sau responsabilul pentru protecția datelor, astfel încât să poată fi declanșate măsurile obligatorii în conformitate cu legislația în vigoare.
Acestea nereguli includ, dar nu se limitează la:

- Transmiterea necorespunzătoare a datelor cu caracter personal către terțe părți,
- Accesul neadecvat al terților la datele cu caracter personal sau
- Pierderea datelor cu caracter personal

Se vor respecta prevederile impuse de **Procedura de raportare și management al incidentelor privind protecția datelor cu caracter personal**.

Categorii de persoane care sunt vizate

Universitatea ca operator prelucrează datele cu caracter personal a următoarelor categorii de persoane fizice:

a) studenţii cursanţi, inclusiv părinţi sau reprezentanţi legali ai acestora, alţi membri ai familiei, după caz,
b) candidaţi la concursurile de admitere;
c) participanți la conferințe și concursuri pe diferite discipline;
d) personal didactic,

e) personal didactic auxiliar şi
f) personal administrativ aflat în relaţii contractuale cu universitatea,
g) candidaţi la concursurile de ocupare a posturilor didactice, de cercetare, didactice auxiliare şi administrative din învăţământul superior;
h) persoane aflate în mobilitate temporară în cadrul instituţiei;
i) vizitatori, orice persoană care intră într-o clădire a universităţii dotată cu sistem de supraveghere video;
j) Persoane fizice sau juridice care au raporturi de natură comercială sau contractuală cu instituţia.

Scopul general al colectării datelor

a) Pentru persoanele menționate la punctele a) - g) se colectează date pentru realizarea obiectului de activitate principal, respectiv: **educaţie şi cercetare ştiinţifică.**
b) Pentru persoanele menţionate la punctul i) datele se culeg pentru monitorizarea/ securitatea persoanelor, spaţiilor şi/ sau bunurilor publice/ private.
c) Pentru persoanele fizice sau juridice care au raporturi de natură comercială sau contractuală cu instituţia datele se colecteaza în scopul gestiunii economico-financiare şi administrative; servicii hoteliere şi de turism; servicii de comunicaţii electronice.

Modalităţi de colectare a datelor

1) Studenţii, angajaţii, candidaţii la admitere sau pe posturi scoase la concurs trebuie să furnizeze o serie de date obligatorii (informaţii despre identitatea persoanei precum şi despre părinţi sau reprezentanţii lor legali, acceptul monitorizării video pentru sporirea securităţii în sistemul educaţional etc.), acestea fiind necesare în derularea/ iniţierea de raporturi juridice cu universitatea, cu respectarea prevederilor legale (de exemplu: cele privind relaţia cu angajaţii sau cele privind înscrierea la studii sau cele privind evidenţa rezultatelor şcolare sau a actelor de studii).
În cazul refuzului de a furniza aceste date, universitatea poate să refuze iniţierea de raporturi juridice, întrucât poate fi pusă în imposibilitatea de a respecta cerinţele reglementărilor speciale în domeniul educaţional, iar în cazul angajaţilor, a prevederilor dreptului muncii şi dreptului fiscal.
2) Universitatea colectează şi o serie de informaţii care nu au caracter obligatoriu (de exemplu: adresa de e-mail, număr de telefon etc.) în vederea îmbunătăţirii modului de comunicare cu studenţii, cursanţii sau reprezentanţii legali ai acestora, precum şi pentru realizarea ulterioară de sondaje statistice (selectarea aleatoare a unui eşantion şi administrarea unui chestionar relativ la aspectele educaţionale) utilizând comunicarea prin sistemul poştei electronice. Refuzul furnizării şi/ sau prelucrării datelor informaţiilor opţionale poate duce la imposibilitatea ca universitatea să transmită informaţii despre serviciile sale.
3) În situaţiile persoanelor fizice sau juridice care au raporturi de natură comercială sau contractuală cu institutia, informaţiile cu caracter personal se colectează şi prelucrează pentru a respecta prevederile legale relativ la înregistrarea operaţiunilor financiar contabile. Furnizarea informaţiilor din această categorie este obligatorie, refuzul de a le furniza duce la imposibilitatea de a demara relaţii juridice între universitate şi respectivele persoane.

Accesul la informaţiile cu caracter personal

Informaţiile colectate sunt destinate utilizării de către universitate şi structurile sale (în calitate de operator) şi sunt comunicate numai următorilor destinatari:

- ✓ persoana vizată,
- ✓ reprezentanţii legali ai persoanei vizate,
- ✓ angajaţi cu drept de acces ai operatorului,
- ✓ împuternicitul operatorului,
- ✓ alte persoane fizice/ juridice care prelucrează datele personale în numele operatorului,
- ✓ compartimentele Ministerului Educației şi Cercetării,
- ✓ instituții partenere,

- ✓ instituţii ale Uniunii Europene
- ✓ autoritatea judecătorească, poliţia, organe de urmărire penală şi alte instituţii abilitate de lege să solicite informaţii.

Obligaţiile operatorului

(1) Universitatea şi structurile universităţii, în calitate de operator, au în principal următoarele obligaţii:

a) să asigure informarea persoanelor vizate şi să respecte drepturile acestora;

b) să ia măsurile necesare pentru a asigura securitatea prelucrării datelor cu caracter personal;

c) să respecte prezentul regulament privind măsurile de protecţie a persoanelor cu privire la prelucrarea datelor cu caracter personal.

d) să desemneze un responsabil cu protecția datelor cu caracter personal.

e) să acorde sprijin responsabilului cu protecția datelor cu caracter personal în îndeplinirea sarcinilor prevăzute în special prin, dar fără a se limita la:

- ➢ asigurarea resurselor necesare pentru îndeplinirea sarcinilor;
- ➢ asigurarea accesului la datele cu caracter personal și la operațiunile de prelucrare;
- ➢ asigurarea resurselor necesare pentru menținerea cunoștințelor de specialitate și adaptarea la noile tehnologii.

f) de a consulta responsabilul cu protecția datelor cu caracter personal în mod corespunzător și în timp util în toate aspectele legate de protecția datelor cu caracter personal.

g) să publice datele de contact ale responsabilului cu protecția datelor și să le comunice autorității de supraveghere.

(2) Conducătorii universităţii şi a structurilor sale sunt responsabili cu protecţia datelor cu caracter personal şi au următoarele atribuţii principale:

a) stabilesc scopul şi mijloacele de prelucrare a datelor cu caracter personal atunci când acestea sunt necesare pentru exercitarea unor competenţe legale;

b) asigură elaborarea regulamentelor/procedurilor proprii şi, după aprobarea acestora de către Senatul universităţii, le pune în aplicare;

c) asigură implementarea şi monitorizează respectarea normelor procedurale în materia prelucrării datelor cu caracter personal de către utilizatori;

d) coordonează şi monitorizează activitatea utilizatorilor pe linia protecţiei datelor cu caracter personal la nivelul operatorului;

e) asigură desfăşurarea pregătirii de specialitate şi instruirea utilizatorilor în acest domeniu;

f) dispun măsuri de completare sau, după caz, de modificare a fişei posturilor utilizatorilor;

g) analizează şi dispun în ceea ce priveşte suspendarea sau revocarea dreptului de acces al utilizatorului la sisteme de evidenţă a datelor cu caracter personal, în condiţiile legii;

h) dispun măsuri pentru exercitarea drepturilor de către persoana vizată;

i) coordonează soluţionarea cererilor persoanelor vizate;

j) ţin evidenţa cererilor persoanelor vizate;

k) analizează periodic activitatea utilizatorilor.

(3) Atribuţiile specifice conducătorilor operatorului (universitatea sau structurile sale) ca responsabili cu protecţia datelor cu caracter personal se stabilesc prin fişa postului/contractul managerial.

Atribuțiile Responsabilul pentru protecția datelor cu caracter personal

(1) Poate fi desemnată responsabil cu protecția datelor persoana care îndeplinește următoarele condiții:

- ➢ deține calități profesionale corespunzătoare;
- ➢ deține cunoștințe de specialitate în domeniul legislației și practicilor privind protecția datelor cu caracter personal;
- ➢ are capacitatea de a îndeplini următoarele sarcini:

a) informează și consiliază operatorul și utilizatorii care efectuează prelucrarea cu privire la obligațiile care le revin în temeiul regulamentului intern și al dispozițiilor legale privind protecția datelor cu caracter personal;

b) monitorizează respectarea dispozițiilor prezentui regulament, a altor dispoziții legale privind protecția datelor cu caracter personal și a politicilor operatorului în ceea ce privește protecția datelor cu caracter personal, inclusiv alocarea responsabilităților și acțiunilor de conștientizare și de formare a utilizatorilor implicaţi în operațiunile de prelucrare, precum și auditurile aferente;

c) consiliază, la cerere, cu privire la evaluarea impactului asupra protecției datelor cu caracter personal și monitorizarea funcționării acesteia,

d) cooperează cu autoritatea de supraveghere în calitatea sa de persoană de contact.

(2) Responsabilul pentru protecția datelor cu caracter personal la nivel de universitate

- participă la elaborarea/ modificarea Regulamentului privind protecția datelor cu caracter personal
- asigură implementarea şi monitorizează respectarea normelor procedurale în materia prelucrării datelor cu caracter personal de către utilizatorii operatorilor;
- analizează vulnerabilităţile şi riscurile semnalate în sistemul de securitate a prelucrării datelor cu caracter personal al structurii şi propune măsuri pentru înlăturarea acestora;
- analizează orice încălcare a normelor de protecţie a datelor cu caracter personal de natură a prejudicia drepturile persoanei vizate, cu privire la măsurile dispuse pentru identificarea persoanei responsabile şi limitarea efectelor unei diseminări neautorizate a datelor, precum şi cu privire la situaţiile în care au fost emise recomandări sau aplicate sancţiuni de către Autoritatea naţională de supraveghere sau când aceasta a dispus efectuarea unui control prealabil ori a unor investigaţii;
- informează Rectorul universităţii în legătură cu orice încălcare a normelor de protecţie a datelor cu caracter personal de natură a prejudicia drepturile persoanei vizate, cu privire a măsurile dispuse pentru identificarea persoanei responsabile şi limitarea efectelor unei diseminări neautorizate a datelor,
- propune stabilirea unor sarcini executive utilizatorilor, în funcţie de scopul prelucrării datelor personale.
- acționează în vederea respectării reglementărilor proprii, a celor naționale și internaționale privind protecția datelor.
- responsabilul pentru protecția datelor cu caracter personal la nivel de universitate are obligația de a informa utilizatorii de date personale, angajații și studenții despre reglementările interne în această privință, are dreptul de a efectua controale şi verificări – consemnate în procese verbale cu privire la modul de aplicare a regulamentului. Rezultatele controalelor se raportează conducătorului structurii supuse controlului.
- responsabilul este înștiințat de fiecare dată la efectuarea unui control a autorității tutelare.
- anchetele si controalele efectuate de Autoritatea de supraveghere trebuie să fie întotdeauna raportate către conducerea Universității.
- responsabilul pentru protecția datelor are obligația de a respecta secretul și/sau confidențialitatea în ceea ce privește îndeplinirea sarcinilor sale.

(3) Directorii de departamente respectiv şefii birourilor/serviciilor administrative au obligația să informeze cu promptitudine Responsabilul pentru protecția datelor cu caracter personal despre apariția oricăror riscuri de protecție a datelor personale.

(4) Persoanele vizate pot contacta responsabilul pentru protecția datelor în orice moment, cu privire la toate aspectele legate de prelucrarea datelor lor și la exercitarea drepturilor lor în temeiul prezentului regulament, cum ar fi de exemplu solicitarea de informații, sau depunerea plângerilor legate de protecția datelor personale.

(5) Dacă responsabilul pentru protecția datelor personale în cauză nu poate rezolva o plângere sau remedia o încălcare a politicii pentru protecția datelor, se va solicita consultanță la Autoritatea de suPraveghere.
(6) Deciziile luate de responsabilul pentru protecția datelor personale pentru a remedia încălcările privind protecția datelor trebuie să fie susținute de conducerea Universității.

Obligaţiile utilizatorilor

(1) Utilizatorii au următoarele obligaţii specifice:

a) să cunoască şi să aplice prevederile actelor normative din domeniul prelucrării datelor cu caracter personal precum şi ale Regulamentului Intern;

b) să informeze persoana vizată atunci când datele cu caracter personal sunt colectate direct de la aceasta, în condiţiile legii, cu privire la:

- identitatea operatorului,
- scopul în care se face prelucrarea datelor,
- destinatarii sau categoriile de destinatari ai datelor,
- obligativitatea furnizării tuturor datelor cerute,
- consecinţele refuzului de a le pune la dispoziţie,
- drepturile prevăzute de lege, în special,
- drepturile de acces, de intervenţie asupra datelor,
- de opoziţie,
- şi condiţiile în care pot fi exercitate aceste drepturi;

c) să prelucreze numai datele cu caracter personal necesare îndeplinirii atribuţiilor de serviciu şi să acorde sprijin conducătorului operatorului pentru realizarea activităţilor specifice ale acestuia;

d) să păstreze confidenţialitatea 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 şi 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 situaţie în care au fost accesate/ prelucrate date cu caracter personal prin încălcarea normelor legale, despre care a luat la cunoştinţă.

(2) Pentru fiecare utilizator, fişa postului se completează în mod corespunzător cu atribuţiile prevăzute la al. (1).
(3) Utilizatorul poate prelucra date cu caracter personal doar pe perioada în care ocupă funcţia respectivă.
(4) Extinderea sau restrângerea atribuţiilor de prelucrare a datelor cu caracter personal se dispune de operator atunci când utilizatorul se află în una dintre următoarele situaţii:

a) la modificarea raporturilor de muncă;

b) la modificarea atribuţiilor privind prelucrarea datelor cu caracter personal, prevăzute în fişa postului.

(5) Dreptul de acces al utilizatorului la sistemul de evidenţă a datelor cu caracter personal se suspendă pe perioada în care acesta se află în una dintre următoarele situaţii:

a) se află în concediu fără plată, concediu medical, concediu pentru creşterea sau îngrijirea copilului minor, pentru o perioadă mai mare de 3 luni;

b) se află în concediu de maternitate sau concediu pentru incapacitate temporară de muncă;

c) urmează un curs sau o specializare cu scoatere din program, pentru o perioadă mai mare de 3 luni;

d) pe perioada cercetării administrative, în situaţia în care faţă de utilizator se efectuează cercetări referitoare la prelucrarea datelor cu caracter personal cu încălcarea dispoziţiilor legale;

e) alte cazuri prevăzute de lege.

(6) Planurile anuale de pregătire continuă, elaborate în condiţiile legii de Direcţia Economică, trebuie să conţină teme privind cunoaşterea legislaţiei naţionale şi a acquis-ului comunitar în materia prelucrării datelor cu caracter personal, precum şi teme specifice privind riscurile pe care le

comportă prelucrarea datelor şi măsurile minime de securitate, în funcţie de specificul activităţii fiecărui operator.
(7) Pregătirea utilizatorilor se realizează în perioada tutelei profesionale.
(8) Periodic, conducătorii operatorului (prin Responsabilul pentru protecția datelor cu caracter personal) organizează instructaje cu utilizatorii pentru cunoaşterea procedurilor specifice de lucru instituite la nivelul fiecărui operator şi cu privire la riscurile generate de vulnerabilităţi şi ameninţări informatice.
(9) Instructajele se efectuează în mod obligatoriu la modificarea cadrului legal în materie, iar prelucrarea incidentelor se va realiza cu toti utilizatorii operatorului.

Drepturile persoanelor vizate

Dreptul de a fi informat

(1) În cazul în care datele cu caracter personal sunt obţinute direct de la persoana vizată, operatorul este obligat să furnizeze persoanei vizate cel puţin următoarele informaţii, cu excepţia cazului în care această persoană posedă deja informaţiile respective:

a) identitatea operatorului şi a reprezentantului acestuia, dacă este cazul;

b) scopul în care se face prelucrarea datelor;

c) informaţii suplimentare, precum: destinatarii sau categoriile de destinatari ai datelor; dacă furnizarea tuturor datelor cerute este obligatorie şi consecinţele refuzului de a le furniza; existenţa drepturilor prevăzute de lege pentru persoana vizată, în special a dreptului de acces, de intervenţie asupra datelor şi de opoziţie, precum şi condiţiile în care pot fi exercitate;

d) orice alte informaţii a căror furnizare este impusă prin dispoziţie a autorităţii de supraveghere, ţinând seama de specificul prelucrării.

(2) Clădirile care sunt supravegheate video vor avea, la intrare, afişat în loc vizibil, informarea privind preluarea şi stocarea de imaginii.

Dreptul de acces la date

(1) Orice persoană vizată are dreptul de a obţine de la universitate sau structurile sale (în calitate de operatori), la cerere şi în mod gratuit pentru o solicitare pe an, confirmarea faptului că datele care o privesc sunt sau nu sunt prelucrate de acesta. Operatorul este obligat, în situaţia în care prelucrează date cu caracter personal care privesc solicitantul, să comunice acestuia, împreună cu confirmarea, cel puţin următoarele:

a) informaţii referitoare la scopurile prelucrării, categoriile de date avute în vedere şi destinatarii sau categoriile de destinatari cărora le sunt dezvăluite datele;

b) comunicarea într-o formă inteligibilă a datelor care fac obiectul prelucrării, precum şi a oricărei informaţii disponibile cu privire la originea datelor;

c) informaţii asupra principiilor de funcţionare a mecanismului prin care se efectuează orice prelucrare automată a datelor care vizează persoana respectivă;

d) informaţii privind existenţa dreptului de intervenţie asupra datelor şi a dreptului de opoziţie, precum şi condiţiile în care pot fi exercitate;

e) informaţii asupra posibilităţii de a înainta plângere către autoritatea de supraveghere, precum şi de a se adresa instanţei pentru atacarea deciziilor operatorului, în conformitate cu dispoziţiile legii.

(2) Persoana vizată poate solicita de la operator (universitatea sau structurile sale informaţiile prevăzute la alin. (1), printr-o cerere întocmită în formă scrisă, înregistrată la registratura universităţii şi semnată. În cerere solicitantul poate arăta dacă doreşte ca informaţiile să îi fie comunicate la o anumită adresă, care poate fi şi de poştă electronică, sau printr-un serviciu de corespondenţă care să asigure că predarea i se va face numai personal.

(3) Operatorul (universitatea sau structurile sale) este obligat să comunice informaţiile solicitate, în termen de 15 zile de la data primirii cererii, cu respectarea eventualei opţiuni a solicitantului exprimate potrivit al. (2).

Dreptul de intervenţie asupra datelor

(1) Orice persoană vizată are dreptul de a obţine de la operator, la cerere şi în mod gratuit:

a) după caz, rectificarea, actualizarea, blocarea sau ştergerea datelor a căror prelucrare nu este conformă legii, în special a datelor incomplete sau inexacte;

b) după caz, transformarea în date anonime a datelor a căror prelucrare nu este conformă legii;

c) notificarea către terţii cărora le-au fost dezvăluite datele a oricărei operaţiuni efectuate conform lit. a) sau b), dacă această notificare nu se dovedeşte imposibilă sau nu presupune un efort disproporţionat faţă de interesul legitim care ar putea fi lezat.

(2) Pentru exercitarea dreptului prevăzut la al. (1), persoana vizată va înainta operatorului o cerere întocmită în formă scrisă, înregistrată la Registratura universităţii şi semnată. În cerere solicitantul poate arăta dacă doreşte ca informaţiile să îi fie comunicate la o anumită adresă, care poate fi şi de poştă electronică, sau printr-un serviciu de corespondenţă care să asigure că predarea i se va face numai personal.

(3) Operatorul este obligat să comunice măsurile luate în temeiul al. (1), precum şi, dacă este cazul, numele terţului căruia i-au fost dezvăluite datele cu caracter personal referitoare la persoana vizată, în termen de 15 zile de la data primirii cererii, cu respectarea eventualei opţiuni a solicitantului exprimate potrivit al. (2).

Dreptul de opoziţie

(1) Persoana vizată are dreptul de a se opune în orice moment, din motive întemeiate şi legitime legate de situaţia sa particulară, ca date care o vizează să facă obiectul unei prelucrări, cu excepţia cazurilor în care există dispoziţii legale contrare. În caz de opoziţie justificată prelucrarea nu mai poate viza datele în cauză.

(2) Persoana vizată are dreptul de a se opune în orice moment, în mod gratuit şi fără nici o justificare, ca datele care o vizează să fie prelucrate în scop de marketing direct, în numele operatorului sau al unui terţ, sau să fie dezvăluite unor terţi într-un asemenea scop.

(3) În vederea exercitării drepturilor prevăzute la al. (1) şi (2) persoana vizată va înainta operatorului o cerere întocmită în formă scrisă, înregistrată la Registratura universităţii şi semnată. În cerere solicitantul poate arăta dacă doreşte ca informaţiile să îi fie comunicate la o anumită adresă, care poate fi şi de poştă electronică, sau printr-un serviciu de corespondenţă care să asigure că predarea i se va face numai personal.

(4) Operatorul este obligat să comunice persoanei vizate măsurile luate în temeiul al. (1) sau (2), precum şi, dacă este cazul, numele terţului căruia i-au fost dezvăluite datele cu caracter personal referitoare la persoana vizată, în termen de 15 zile de la data primirii cererii, cu respectarea eventualei opţiuni a solicitantului exprimate potrivit al. (3).

Dreptul de a nu fi supus unei decizii individuale

(1) Orice persoană are dreptul de a cere şi de a obţine retragerea/ anularea/ reevaluarea oricărei decizii care produce efecte juridice în privinţa sa, adoptată exclusiv pe baza unei prelucrări de date cu caracter personal, efectuată prin mijloace automate, destinată să evalueze unele aspecte ale personalităţii sale, precum competenţa profesională, credibilitatea, comportamentul său ori alte asemenea aspecte.

(2) Respectându-se celelalte garanţii prevăzute de lege, o persoană poate fi supusă unei decizii de natura celei vizate la al. (1), numai în următoarele situaţii:

a) decizia este luată în cadrul încheierii sau executării unui contract, cu condiţia ca cererea de încheiere sau de executare a contractului, introdusă de persoana vizată, să fi fost satisfăcută sau ca unele măsuri adecvate, precum posibilitatea de a-şi susţine punctul de vedere, să garanteze apărarea propriului interes legitim;

b) decizia este autorizată de o lege care precizează măsurile ce garantează apărarea interesului legitim al persoanei vizate.

Dreptul de a se adresa justiţiei

(1) Fără a se aduce atingere posibilităţii de a se adresa cu plângere autorităţii de supraveghere, persoanele vizate au dreptul de a se adresa justiţiei pentru apărarea oricăror drepturi garantate de lege, care le-au fost încălcate.
(2) Orice persoană care a suferit un prejudiciu în urma unei prelucrări de date cu caracter personal, efectuată ilegal, se poate adresa instanţei competente pentru repararea acestuia.
(3) Prelucrarea datelor cu caracter personal se poate realiza prin mijloace automate sau neautomate în cadrul unor operaţiuni ori seturi de operaţiuni, fără a fi limitate la acestea, după cum urmează:

a) colectarea - strângerea, adunarea ori primirea datelor cu caracter personal prin orice mijloace legale şi din orice sursă;

b) înregistrarea - consemnarea datelor cu caracter personal într-un sistem de evidenţă automat ori neautomat, care poate fi registru, fişier automat, bază de date sau orice altă formă de evidenţă organizată, structurată ori ad-hoc sau într-un text, înşiruire de date ori document, indiferent de modalitatea în care se înscriu datele;

c) organizarea - ordonarea, structurarea sau sistematizarea datelor cu caracter personal, conform unor criterii prestabilite, potrivit atribuţiilor legale ale operatorului, în scopul eficientizării/ optimizării activităţilor de prelucrare a acestora;

d) stocarea - păstrarea pe orice fel de suport a datelor cu caracter personal culese, inclusiv prin efectuarea copiilor de siguranţă;

e) adaptarea - transformarea datelor cu caracter personal colectate iniţial, conform criteriilor prestabilite şi scopurilor pentru care au fost colectate;

f) modificarea - actualizarea, completarea, schimbarea, corectarea ori refacerea datelor cu caracter personal, în scopul menţinerii caracteristicilor de exactitate, realitate, actualitate;

g) extragerea - scoaterea unei părţi din categoria specifică de date cu caracter personal, în scopul utilizării acesteia, separat şi distinct de prelucrarea iniţială;

h) consultarea - examinarea, vizualizarea, interogarea ori cercetarea datelor cu caracter personal, fără a fi limitate la acestea, în scopul efectuării unei operaţiuni sau set de operaţiuni de prelucrare ulterioară;

i) utilizarea - folosirea datelor cu caracter personal, în tot sau în parte, de către şi în interiorul operatorului, împuterniciţilor operatorului ori destinatarului, după caz, inclusiv prin tipărire, copiere, multiplicare, scanare sau orice alte procedee similare;

j) dezvăluirea - a face disponibile date cu caracter personal către terţi prin comunicare, transmitere, diseminare sau în orice alt mod;

k) alăturarea - adăugarea, alipirea sau anexarea unor date cu caracter personal la cele deja existente, pe care nu le modifică;

l) combinarea - îmbinarea, unirea sau asamblarea unor date cu caracter personal separate iniţial, într-o formă nouă, pe baza unor criterii prestabilite, pentru scopuri anume determinate;

m) blocarea - întreruperea prelucrării datelor cu caracter personal;

n) ştergerea - eliminarea sau înlăturarea, în tot sau în parte, a datelor cu caracter personal din evidenţe sau înregistrări, prin împlinirea termenului de păstrare, la atingerea scopului pentru care au fost introduse, caducitatea, inexistenţa, inexactitatea;

o) transformarea - operaţiunea efectuată asupra datelor cu caracter personal având ca scop anonimizarea ori utilizarea acestora în scopuri exclusiv statistice;

p) distrugerea - aducerea la stare de neîntrebuinţare, în condiţiile legii, definitivă şi irecuperabilă, prin mijloace mecanice sau termice, a suportului fizic pe care au fost prelucrate date cu caracter personal.

(4) Prelucrarea datelor cu caracter personal se realizează de către universitate şi structurile sale în exercitarea atribuţiilor expres stabilite printr-un act normativ sau atunci când acesta prevede constituirea unor sisteme de evidenţă la nivel naţional/ teritorial, în scopul realizării unor activităţi/ servicii de interes public.
(5) Colectarea datelor cu caracter personal se poate face direct de la persoana vizată sau prin surse specifice, care pot fi, dar fără a se limita la: activitatea proprie a operatorului sau a împuterniciţilor acestuia, consultarea directă a unor sisteme de evidenţă a datelor cu caracter personal constituite de

alţi operatori ori schimbul de date şi informaţii cu alţi operatori, naţionali sau internaţionali, cu respectarea drepturilor persoanelor vizate şi instituirea unor măsuri adecvate de securitate a prelucrărilor.
(6) Informarea persoanei vizate se realizează în condiţiile şi cu excepţiile prevăzute de lege şi conform cu prevederile prezentui regulament
(7) Stocarea datelor cu caracter personal se realizează în condiţiile stabilite prin actul normativ care reglementează scopul prelucrării şi potrivit regulilor generale de arhivare a documentelor.
(8) Universitatea şi structurile sale prelucrează date cu caracter personal în scopuri de organizare, gestiune economico-financiară şi administrativă privind proprii angajaţi şi membrii de familie ai acestora, în cadrul activităţii de management resurse umane, asigurarea asistenţei medicale sau pentru desfăşurarea unor activităţi cultural artistice, jurnalistice ori sportive.
(9) Universitatea şi structurile sale care prelucrează date cu caracter personal cu ocazia organizării unor concursuri sau examene, stabilesc condiţiile concrete de asigurare a securităţii prelucrărilor, precum şi de informare a persoanelor vizate privind drepturile acestora. Datele cu caracter personal astfel prelucrate se arhivează conform legii după realizarea scopului în care au fost prelucrate. Stocarea acestor date pentru o perioadă mai mare decât cea necesară realizării scopului se poate efectua numai pentru interes statistic, după ce au fost transformate în date anonime.
(10) Supravegherea prin mijloace audio şi/ sau video, fixe sau mobile, a unor spaţii publice perimetrale ori adiacente propriilor sedii, precum şi a spaţiilor interioare ale acestora constituie o prelucrare a datelor cu caracter personal doar dacă aceasta este însoţită de un sistem de stocare a datelor care permite identificarea ulterioară, prin orice mijloace, a persoanei vizate. În acest caz este obligatorie avertizarea personalului propriu şi a publicului privind existenţa sistemului de supraveghere, precum şi informarea acestuia privind identitatea operatorului, scopul prelucrării, categoriile de date prelucrate, destinatarii datelor sau alte date suplimentare, după caz, conform legii. Instalarea acestor mijloace se realizează astfel încât, pe cât posibil, să nu fie vizualizat interiorul altor imobile sau căile de acces la acestea, aflate în zona adiacentă echipamentelor de supraveghere.

Comunicarea datelor cu caracter personal
(1) Datele cu caracter personal se pot comunica între operatori şi împuterniciţii acestora sau între operatori sau împuterniciţi ai acestora şi alte instituţii ori organisme publice sau entităţi de drept public sau privat în una dintre următoarele situaţii:
a) dacă persoana vizată şi-a dat consimţământul expres şi neechivoc pentru comunicarea datelor sale;
b) fără consimţământul persoanei vizate în cazurile prevăzute de lege.
(2) Comunicarea datelor cu caracter personal de către operatori şi împuterniciţii acestora se poate face şi on-line, cu respectarea dispoziţiilor al. (1) şi asigurarea securităţii sistemelor de comunicaţii a datelor cu caracter personal.
(3) Datele cu caracter personal asupra cărora persoanele vizate au exercitat şi li s-a recunoscut dreptul de opoziţie nu pot face obiectul prelucrării.
(4) Cererile pentru comunicarea datelor cu caracter personal adresate universităţii şi structurilor sale trebuie să conţină datele de identificare a solicitantului, precum şi motivarea şi scopul cererii, conform prevederilor legale.
(5) Cererile care nu conţin elementele prevăzute la al. (1) se restituie pentru completare, iar cele care nu se încadrează în condiţiile prevăzute de lege se resping, menţionându-se motivele pentru care comunicarea datelor cu caracter personal nu este posibilă.
(6) Înainte de comunicarea datelor cu caracter personal, operatorii verifică dacă acestea sunt exacte şi, dacă este cazul, actualizate.
(7) În situaţia în care se constată că au fost transmise date incorecte sau neactualizate, operatorii au obligaţia de a informa destinatarii respectivelor date asupra neconformităţii acestora, cu menţionarea datelor care au fost modificate.

(8) La comunicarea datelor cu caracter personal operatorii atenţionează destinatarii asupra interdicţiei de a prelucra datele pentru alte scopuri decât cele specificate în cererea de comunicare.
(9) Toate documentele care conţin date cu caracter personal se înregistrează şi urmează regulile de păstrare, procesare, multiplicare, transport, transmitere, distrugere şi arhivare stabilite prin Legea Arhivelor nationale şi prin proceduri interne.
(10) Conducătorul operatorului stabileşte fiecărui utilizator tipurile de acces şi operaţiunile permise acestuia, strict necesare pentru îndeplinirea atribuţiilor de serviciu.
(11) Cu ocazia proiectării, întreţinerii, actualizării aplicaţiilor de gestiune a bazelor de date, se interzice accesul programatorilor/ personalului de întreţinere a sistemelor informatice la orice fel de date cu caracter personal deţinute/ create/ accesate de personalul din structura respectivă. În aceste situaţii, se pun la dispoziţia programatorilor/ personalului de întreţinere numai date anonime.
(12) Pentru cazuri excepţionale, numai pe durata intervenţiei şi circumstanţiat limitativ la datele strict necesare, persoanele care asigură suportul tehnic pot avea acces la datele cu caracter personal numai în prezenţa unui utilizator desemnat de operator, în această situaţie, răspunderea pentru păstrarea confidenţialităţii datelor aparţine persoanelor în cauză, sens în care trebuie să semneze un angajament de confidenţialitate.
(13) Operaţiunile de colectare, introducere, modificare şi actualizare a datelor cu caracter personal se fac numai de personalul anume desemnat de către conducătorii operatorului.
(14) Conducătorii operatorilor dispun măsurile necesare care să permită identificarea utilizatorului care a introdus, modificat sau actualizat datele.
(15) Bazele de date cu caracter personal deţinute/ create şi programele folosite de operatori sunt salvate, prin copii de siguranţă, la un interval de timp stabilit de conducătorii operatorului, în funcţie de mărimea, volumul şi importanţa acestor baze de date, care nu poate depăşi 6 luni.
(16) Conducătorii operatorului desemnează utilizatori care trebuie să aibă ca atribuţie de serviciu şi executarea copiilor de siguranţă ale bazelor de date deţinute/ create şi ale programelor folosite.
(17) Accesul în încăperile în care se află documente ce conţin date cu caracter personal şi/ sau echipamente care prelucrează date cu caracter personal este strict limitat la utilizatorii desemnaţi de conducătorii operatorului şi numai pentru îndeplinirea atribuţiilor de serviciu.
(18) În cazul în care nu se poate restricţiona accesul în aceste încăperi, documentele se securizează în dulapuri/ fişete metalice închise cu chei; echipamentele se securizează cu chei sau cartele magnetice.
(19) Aplicaţiile informatice care gestionează date cu caracter personal trebuie prevăzute cu facilitatea închiderii automate a sesiunii de lucru dacă utilizatorul nu acţionează asupra datelor afişate pe ecran o perioadă de timp de până la 5 minute, stabilită în funcţie de operaţiile care trebuie executate.
(20) Terminalele de acces folosite în relaţia cu publicul se poziţionează astfel încât datele afişate să fie vizualizate numai de utilizatori. Aceste terminale de acces trebuie să aibă setată funcţia "screen saver" la o temporizare de maximum 5 minute, iar dacă acest lucru nu este posibil din punct de vedere tehnic, după trecerea intervalului de timp menţionat, datele afişate trebuie ascunse.

Responsabilități și sancțiuni

(1) Persoanele având funcții executive în Universitate sunt responsabile pentru prelucrarea datelor în zona lor de responsabilitate. Prin urmare, ei sunt obligați să se asigure că cerințele legale pentru protecția datelor și cele conținute în politica de protecție a datelor personale, sunt îndeplinite. Personalul de conducere este responsabil pentru asigurarea măsurilor organizatorice, tehnice și a celor care țin de resursele umane pentru ca orice prelucrare a datelor să se efectueze în conformitate cu protecția datelor. Conformitatea cu aceste cerințe este responsabilitatea fiecărui angajat/colaborator, respectiv student.
(2) Departamentele trebuie să informeze Responsabilul pentru protecția datelor în timp util cu privire la o nouă prelucrare a datelor cu caracter personal. Pentru prelucrarea datelor care pot prezenta riscuri speciale pentru drepturile individuale ale persoanelor vizate, Responsabilul pentru protecția datelor trebuie să fie informat înainte de începerea prelucrării.

(3) Prelucrarea necorespunzătoare a datelor cu caracter personal sau alte încălcări ale legilor privind protecția datelor conduce la suportarea sancțiunilor prevăzute de reglementările interne de Regulamentul UE nr.679/2016 și de legislația în vigoare.
(4) Regulamentul este revizuit anual sau ori de câte ori se impune, iar ultima versiune aprobată de către Senatul Universității va fi disponibilă prin postarea pe site-ul universității, pentru informare și conformare, în cel mult 7 zile de la adoptare.

DISPOZIȚII SPECIFICE

Prelucrarea datelor personale ale salariaților

Evidența personalului.

În cazul salariaților se pot colecta, stoca și prelucra în exclusivitate datele cu caracter personal necesare reglementărilor din domeniul raporturilor de muncă. Sunt admise doar examinările medicale care vizează capacitatea salariatului pentru îndeplinirea atribuțiilor ce îi revin conform fișei postului.

În vederea îndeplinirii obligațiilor legale, Universitatea colectează, prelucrează și păstrează următoarele date personale:

1. Numele și prenumele
2. Numele purtat anterior
3. Data nașterii
4. Numele tatălui
5. Numele mamei
6. Cetățenia
7. Codul numeric personal
8. Datele personale ale persoanei coasigurate la casa de sănătate
9. Decizie de pensionare
10. Număr de telefon,
11. Adresa e-mail
12. Numărul documentului de identitate
13. Adresa,
14. Numărul contului bancar
15. Data începerii și încetării activității
16. Funcția
17. Fotocopii ale documentelor referitoare la școlarizare și formare profesională necesare îndeplinirii funcției
18. Fotografie
19. Autobiografie
20. Date referitoare la salarii, îndemnizații, etc
21. Date privind situația familială a angajatului (starea civilă, numele și prenumele, datele de naștere ale soțului, copiilor minori)
22. Date referitoare la rețineri din salarii (obligații legale, pe bază de hotărâre definitivă sau cele pe baza unui acord exprimat în formă scrisă), precum temeiul legal ale acestora
23. Evaluarea muncii angajatului
24. Motivele și modalitatea încetării contractului de muncă
25. Semnătura
26. Rezultatele evaluării aptitudinilor profesionale la angajare
27. Vizele medicale la angajare
28. Denumirea casei de asigurări de pensii private, numărul de înregistrare al acestuia precum și numărul de identificare al angajatului
29. În cazul angajaților din străinătate: număr de pașaport și documentele care atestă dreptul la muncă
30. Procesele verbale referitoare la eventualele accidente de muncă suferite de angajat.
31. Date necesare alocațiilor individuale (tichete de masă, tichete cadou)
32. Înregistrări ale sistemului de supraveghere video
33. Date referitoare la mobilităţile personalului

Temeiul juridic al prelucrării datelor cu caracter personal constă din obligația legală a Universității, rezultată din dispozițiile Legii nr. 53/2003 privind Codul muncii, ale Legii nr. 1/2011 privind educația națională, din dispozițiile ordinelor emise de Ministerul Educației Naționale, din legislația privind învățământul superior. Furnizarea de date cu caracter personal este necesar pentru executarea unui contract la care persoana vizată este parte sau pentru a face demersuri la cererea persoanei vizate înainte de încheierea unui contract, în concordanță cu Art. 6 (b) din Regulamentul UE. Eventuala nefurnizare sau restricționare a acestora duce la imposibilitatea încheierii sau ducerii la îndeplinire a acestuia.

Scopul prelucrării o reprezintă crearea și menținerea raporturilor de muncă.

Destinatarii datelor cu caracter personal sunt: conducerea Universității, Rectoratul, personalul departamentului de resurse umane, Finanțatorii Universității, precum și operatorii de date ale Universității.

Universitatea păstrează aceste date în conformitate cu OMEF 3512/2008 și Anexa 6 a Legii Arhivelor Naționale, care stabilesc următoarele termene de păstrare a documentelor de resurse umane:

-Statele de plată a salariilor – 50 de ani de la crearea lor
-Statele de funcții – cu caracter permanent
-Jurnalele de prezență 3 ani
-Dosarele de personal, contractele de muncă, convențiile civile de prestări servicii – 70 de ani de la creare

Universitatea prelucrează datele referitoare la starea de sănătate numai pe baza obligațiilor ce-i revin din cele prescrise în Codul muncii.

Documentul informativ obligatoriu (Preambul GDPR (68)) privind prelucrarea datelor personale se află în Anexa 1. Acesta trebuie înmânat persoanei vizate la încheierea contractului de muncă.

Prelucrarea datelor personale ale candidaților prezentați în vederea angajării.
Datele personale colectate sunt următoarele:

1. Numele și prenumele
2. Numele purtat anterior
3. Data nașterii
4. Numele tatălui
5. Numele mamei
6. Cetățenia
7. Codul numeric personal
8. Număr de telefon,
9. Adresa e-mail
10. Numărul documentului de identitate
11. Adresa,
12. Fotocopii ale documentelor referitoare la școlarizare și formare profesională necesare îndeplinirii funcției
13. Fotografie
14. Autobiografie
15. În cazul persoanelor din străinătate: număr de pașaport și documentele care atestă dreptul la muncă

Scopul prelucrării datelor: selecționarea personalului în vederea angajării, crearea și menținerea raporturilor de muncă. Candidatul trebuie anunțat chiar dacă nu a fost ales pentru ocuparea postului.

Temeiul legal a prelucrării datelor : 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. (Art. 6 (b) din Regulamentul UE).

Destinatarii datelor cu caracter personal sunt: conducerea Universității, personalul Rectoratului şi al departamentului de resurse umane, precum și operatorii de date ale Universității.

Durata păstrării datelor este de 3 ani după expirarea termenelor pentru contestarea deciziei. Datele candidaților respinși precum și celor care și-au retras candidatura vor fi șterse respectiv distruse imediat.
Datele personale ale candidaților poate fi păstrată numai cu acordul scris ale persoanelor vizate. Acest acord se regăsește în Anexa 10 și trebuie solicitat la depunerea dosarului de candidatură,

Prelucrarea datelor personale la verificarea aptitudinilor profesionale.

La angajare, Universitatea acționează în conformitate cu art. 29 din Codul Muncii. Informațiile cerute, sub orice formă, de către angajator persoanei care solicită angajarea cu ocazia verificării prealabile a aptitudinilor nu pot avea un alt scop decât acela de a aprecia capacitatea de a ocupa postul respectiv, precum și aptitudinile profesionale. Universitatea poate cere informații în legătură cu persoana care solicită angajarea de la foștii săi angajatori, dar numai cu privire la activitățile îndeplinite și la durata angajării și numai cu notificarea prealabilă a celui în cauză.

Scopul prelucrării o reprezintă crearea și menținerea raporturilor de muncă.

Temeiul legal a prelucrării datelor o legislația muncii și (Art 6 (b) din Regulamentul UE) conform căruia 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.

Destinatarii datelor personale: Rezultatele testării aptitudinilor profesionale pot fi cunoscute doar de persoana testată și de specialistul care a efectuat testarea. Universitatea primește doar informația despre capacitatea persoanei de a îndeplini funcția, respectiv apt/neapt. Detaliile testării, documentația completă a acestuia nu pot fi puse la dispoziția Universității.

Durata păstrării datelor este de 3 ani după încetarea contractului de muncă, cu excepția situației în care legea prevede altfel.

Documentul informativ privind prelucrarea datelor la verificarea prealabilă a aptitudinilor se află în Anexa 1.

Teste psihologice sau alte teste de acest gen legate exclusiv de activitatea profesională, se pot executa și numai în scopul îmbunătățirii acestuia, dar numai în condițiile în care datele sunt anonimizate astfel încât persoanele vizate să nu mai poată fi identificabile.

Reguli privind controlul mijloacelor puse la dispoziția salariatului de către angajator.

Conducerea Universității are drept de control asupra mijloacelor puse la dispoziția salariatului.
Pe timpul controlului trebuie asigurată prezența salariatului, exceptând cazurile în care condițiile procesului de control nu poate permite acesta.

Salariatul trebuie informat despre scopul controlului, cine va efectua controlul și procedura de control, precum și care sunt drepturile și căile de atac judiciare în legătură cu prelucrarea datelor pe parcursul procesului de control.

Pe parcursul controlului se va aplica principiul gradualității și proporționalității, în sensul că se vor verifica prima dată adresele respectiv rezumatele pentru determinarea caracterului personal sau oficial al conținutului. Conținuturile nepersonale se pot verifica nemijlocit de către angajator.
În cazul în care se va dovedi, că mijlocul a fost utilizat în scopuri personale, angajatorul va dispune ștergerea acestor date de către persoana vizată. În lipsa persoanei controlate angajatorul va șterge datele personale găsite pe timpul controlului. Utilizarea neconformă cu regulamentele interne a mijlocului pus la dispoziția salariatului atrage după sine sancțiuni disciplinare.

Prelucrarea datelor personale în vederea respectării unei obligații legale.

Conform lit (68) din Preambulul Regulamentului UE, fiindcă prelucrarea datelor personale este necesară în vederea respectării unei obligațiilor legale, nu este nevoie de consimțământul persoanei vizate. Persoana vizată trebuie înștiințată despre obligativitatea prelucrării datelor personale (Preambul GDPR, (68)) Înștiințarea este cuprinsă în Anexa 1.

Prelucrarea datelor personale în vederea respectării obligațiilor privind taxele și impozitele.

Universitatea prelucrează datele personale ale clienților și furnizorilor în vederea respectării obligațiilor privind taxele și impozitele prescrise de Legea contabilității, nr. 82/1991 și Legea nr. 227/2015 privind Codul fiscal. Datele prelucrate sunt:

1. Numele și prenumele
2. Adresa
3. Codul unic de înregistrare fiscală/CNP
4. Număr de telefon
5. Adresa de email
6. Numărul documentului de identitate
7. Numărul contului bancar
8. Semnătura

În vederea decontării deplasărilor cu autoturismul proprietate personală fată de cele menționate mai sus se vor reține următoarele date:

9. Tipul autoturismului
10. Numărul de înmatriculare al autoturismului
11. Data deplasării
12. Destinația
13. Denumirea unității vizitate.

Durata păstrării datelor personale este stabilită în OMEF 3512/2008 și Anexa 6 a Legii Arhivelor Naționale și este de 10 ani.

Destinatarii datelor cu caracter personal sunt: conducerea Universității, personalul departamentului economic, Finanțatorii Universității, precum și operatorii de date ale Universității.

Prelucrarea datelor personale în vederea executării unor reţineri/popriri pe salariu

Reţinerile/popririle pe salariu sunt tratate conform Codului Muncii, şi art. 781 şi următoarele din Codul de Procedură Civilă, deci datele personale prelucrate sunt legate de respectarea unei obligaţii legale.

Datele cu caracter personal sunt următoarele
1. Numele și prenumele
2. Numele purtat anterior
2. Adresa
3. Codul unic de înregistrare fiscală/CNP
4. Număr de telefon
5. Adresa de email
6. Numărul documentului de identitate
7. Numărul contului bancar
8. Semnătura
9. Documentul care prezintă baza legală a reținerii salariale

Destinatarii datelor cu caracter personal sunt personalul departamentului de resurse umane, departamentului financiar-contabil, precum și operatorii de date ale Universității.

Durata păstrării datelor personale este identică cu cea a statelor de salarii, respectiv de 50 ani

Măsuri specifice personalului didactic

Prelucrarea datelor personalului didactic în cadrul raporturilor de muncă este identică cu cea expusă pentru angajați. În acest capitol sunt prezentate doar prelucrările de date specifice personalului didactic, care apar la ocuparea posturilor, la evaluarea activității profesionale de către management, la evaluarea de către studenți, şi evaluarea activității de cercetare.

Temeiul legal a prelucrării datelor o prezintă
- Legea educației naționale nr. 1/2011 din 5 ianuarie 2011,
- Metodologia-cadru de concurs pentru ocuparea posturilor didactice şi de cercetare vacante din învățământul superior, aprobată prin HG nr. 457 din 4 mai 2011,
- Regulamentul de concurs pentru ocuparea posturilor didactice al Universității,
- Legislația muncii
- reglementările naţionale referitoare la sistemul de învățământ superior
- (Art 6 (b) din Regulamentul UE) conform căruia 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.

Destinatarii datelor cu caracter personal sunt: conducerea Universității, personalul Rectoratului şi al departamentului de resurse umane, precum și operatorii de date ale Universității.

Prelucrarea datelor personale ale candidaților prezentați în vederea angajării.

Datele personale colectate sunt următoarele:
1. Numele și prenumele
2. Numele purtat anterior
3. Data și locul nașterii
4. Numele tatălui
5. Numele mamei
6. Cetățenia
7. Codul numeric personal

8. Număr de telefon,
9. Adresa e-mail
10. Numărul documentului de identitate
11. Adresa,
12. Fotocopii ale documentelor referitoare la școlarizare și formare profesională necesare îndeplinirii funcției
13. Fotografie
14. Autobiografie
15. În cazul persoanelor din străinătate: număr de pașaport și documentele care atestă dreptul la muncă
16. Lista lucrărilor științifice

Termenul de păstrarea datelor este de
- Statele de plată a salariilor – 50 de ani de la crearea lor
- Statele de funcții – cu caracter permanent
- Jurnalele de prezență 3 ani
- Dosarele de personal, contractele de muncă, convențiile civile de prestări servicii – 70 de ani de la creare
- Contracte plata cu ora 50 ani

Sistemul informatic pentru gestionarea studiilor Neptun

Sistemul informatic utilizat pentru managementul procesului de învățământ este sistemul Neptun,
Date personale ale cadrelor didactice prelucrate în cadrul sistemului Neptun:

1. Numele și prenumele
2. Numele purtat anterior
3. Data și locul nașterii
4. Numele mamei
5. Cetățenia
6. Sexul
7. Adresa email
…8. Domiciliul
9. Cod numeric personal
10. Numărul de telefon personal
11. Seria și numărul actului de identitate

Managementul calității

Date personale prelucrate: Calificativele acordate cadrelor didactice de către studenți și celelalte cadre didactice, fișele de autoevaluare.

Scopul prelucrării: Evaluarea, asigurarea și perfecționarea calității activității didactice, de cercetare și de management în cadrul Universității.

Temeiul legal al prelucrării
-Legea educației naționale nr. 1/2011,
-Regulamentul de asigurare a calității al Universității Sapientia din Cluj-Napoca
-Regulamentele de organizare și funcționare a Comisiilor de Evaluare și Asigurare a Calității la nivelul facultăților

Destinatarii datelor cu caracter personal sunt: membrii Comisiilor de evaluare și asigurare a calității la nivel de Universitate, membrii Comisiilor de evaluare și asigurare a calității la nivel de facultate,

conducerea Universității, personalul departamentului de resurse umane, precum și operatorii de date ale Universității, ARACIS.

Termenul de păstrare a datelor cu caracter personal este de 5 ani de la lichidare.

Activitatea de cercetare. Sistemul Online al Programelor de Cercetare, KPIOR

Scopul prelucrării: Asigurarea finanțării unor programe de cercetare.
Temeiul legal al prelucrării: Necesitatea de a executa un contract la care persoana vizată este parte sau pentru a parcurge etapele premergătoare încheierii unui contract, la solicitarea persoanei vizate cf literei (44) din Preambulul și Articolului 6 litera (1) din Regulamentul UE.

Date personale prelucrate:

1. Numele și prenumele
2. Codul numeric personal
3. Adresa e-mail
4. Funcția
5. Locul nașterii
6. Data nașterii
7. Cetățenia
8. Seria și numărul actului de identitate
9. Data eliberării actului de identitate
10. Numărul de telefon personal
11. Numărul de telefon la locul de muncă

Destinatarii datelor cu caracter personal: Finanțatorii programelor de cercetare, persoanele care prelucrează datele în cadrul biroului KPIOR.
Durata păstrării datelor personale este identică cu cea a contractelor plata cu ora, adică 50 ani.
Nota de confidențialitate se găsește în Anexa 1.

Reguli privind controlul mijloacelor puse la dispoziția salariatului de către angajator.

Conducerea Universității are drept de control asupra mijloacelor puse la dispoziția salariatului.
Pe timpul controlului trebuie asigurat prezența salariatului, exceptând cazurile în care condițiile procesului de control nu poate permite acesta.

Salariatul trebuie informat despre scopul controlului, cine va efectua controlul și procedura de control, precum și care sunt drepturile și căile de atac judiciare în legătură cu prelucrarea datelor pe parcursul procesului de control.

Pe parcursul controlului se va aplica principiul gradualității și proporționalității, în sensul că se vor verifica prima dată adresele respectiv rezumatele pentru determinarea caracterului personal sau oficial al conținutului. Conținuturile nepersonale se pot verifica nemijlocit de către angajator.
În cazul în care se va dovedi, că mijlocul a fost utilizat în scopuri personale, angajatorul va dispune ștergerea acestor date de către persoana vizată. În lipsa persoanei controlate angajatorul va șterge datele personale găsite pe timpul controlului. Utilizarea neconformă cu regulamentele și politicile interne a mijlocului pus la dispoziția salariatului atrage după sine sancțiuni disciplinare.

Prelucrarea datelor personale ale specialiștilor și/sau cadrelor didactice ale altor instituții în calitate de cadre didactice asociate invitate

În cazul în care invitații sunt remunerați în cadrul Universității pentru activitatea lor, se vor procesa aceleași date cu caracter personal și vor fi păstrate în aceleași condiții ca și în cazul angajaților plătiți cu ora.

Temeiul legal: 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.

În cazul în care invitații nu sunt remunerați, prelucrarea datelor cu caracter personal va fi efectuată pe baza consimțământului liber exprimat, Anexa 2.

Datele personale colectate sunt următoarele:

1. Numele și prenumele
2. Cetățenia
3. Număr de telefon,
4. Adresa e-mail
5. Fotografii
6. Înregistrări video

Prelucrarea datelor personale ale cadrelor universitare aflate în mobilităţi Erasmus+, CEEPUS

Universitatea primeşte cadre universitare (cadre didactice şi administrative) de la instituțiile partenere aflate în mobilități.

1. -Numele și prenumele
2. -Datele actului de identitate
3. -Cetățenie
4. -Sexul
5. -Adresa
6. -Număr de telefon
7. -Adresa e-mail:
8. -Instituţia de proveniență
9. -Contul bancar
10. -Date financiare (granturi)

Destinatarii datelor cu caracter personal sunt: Comisia Europeană, Agenţia Naţională pentru Programe Comunitare în Domeniul Educaţiei şi Formării Profesionale (ANPCDEFP), organismele externe autorizate responsabile de verificare şi audit, institutiile partenere, conducerea Universității, coordonatorii programelor din facultati si coordonatorul institutional Erasmus, personalul secretariatelor administrative şi economice din cadrul facultăţilor şi al Rectoratului.

Temeiul legal:
- Art. 6 (b) din Regulamentul UE, conform căruia 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. În acest context termenul de contract se referă la contractul de mobilitate.
-Regulamentul programelor Erasmus+, CEEPUS

Prelucrarea datelor personale ale studenților

Temeiul legal:
- Ordinul Ministerului Educației și Învățământului nr. 3.714/2018 privind aprobarea Regulamentului de organizare, funcționare si operaționalizare a Registrului Matricol Unic al Universităților din Romania
- Legislația specifică funcționării instituțiilor de învățământ superior- Art 6 (b) din Regulamentul UE, conform căruia 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. În acest context termenul de contract se referă la contractul de școlarizare.

Scopul prelucrării este:
Asigurarea desfășurării procesului educațional, în conformitate cu Art. 2 al Ordinul Ministerului Educației și Învățământului nr. 3.174/2018
Efectuarea viramentelor diferitelor drepturi financiare şi recuperarea creanțelor (ex. diferite taxe legate de studii).
Asigurarea mijlocului de comunicare pe durata studiilor legat de administrarea studiilor, şi după încheierea studiilor în vederea urmăririi situației legată de inserția pe piața muncii, respectiv continuarea studiilor şi includerea în sistemul Alumni al absolvenților Universității.

În vederea îndeplinirii obligațiilor legale, Universitatea colectează, prelucrează și păstrează următoarele date personale ale studenților:

1. Numele și prenumele
2. Numele purtat anterior
3. Data și locul nașterii
4. Numele tatălui
5. Numele mamei
6. Cetățenia
7. Sexul
8. Etnia
9. Codul numeric personal
10. Număr de telefon
11. Adresa e-mail
12. Datele documentului de identitate
13. Adresa
14. Numărul contului bancar
15. Studii anterioare, disciplinele studiate, rezultatele studiilor şi ale examenului de finalizare a studiilor, diplome şi certificate obţinute, prezență, competenţe de limbi străine, mobilităţi efectuate, etc.
16. Fotocopii ale actului de identitate şi a documentelor referitoare la școlarizare și formare profesională necesare admiterii
17. Fotografie
18. Date referitoare la burse şi alte îndemnizații, etc
19. Vize medicale la înscriere, date medicale
20. În cazul studenților din străinătate: număr de pașaport și documentele care atestă dreptul la studiu
21. Înregistrări ale sistemului de supraveghere video
22. Date sociale
23. Starea civilă
24. Date financiare: diferite plăți şi încasări
25. Semnătura
26. Înregistrări legate de procesul de învăţământ online

Destinatarii datelor cu caracter personal sunt: conducerea Universității, personalul secretariatelor, Finanțatorii Universității, operatorii de date ale Universității precum și RMU, autoritățile statului (direcţii teritoriale de muncă, case de asigurări etc.). Datele studenților sunt păstrate şi prelucrate atât pe suport de hârtie cât şi electronic, inclusiv prin sistemul informatic Neptun.

Dispoziții specifice concursului de admitere

Scopul prelucrării datelor este în scopul participării la examenul de admitere, în vederea obținerii dreptului de a participa la procesul de învățământ.

Temei legal

- Ordinul Ministrului Educației Naționale privind privind organizarea admiterii în ciclurile de studii universitare de licență, de master și de doctorat valabil în anul universitar respective,
- Regulamentul de admitere al Universității aprobată pentru anul in curs prin Decizia Senatului,
- Legislația specifică funcționării instituțiilor de învățământ superior.
- Consimțământul persoanei vizate

Persoana vizată va fi informată în scris despre scopul prelucrării, destinația și durata păstrării datelor, acesta poate fi regăsit în Anexa 3.

Candidaţi respinși la examenul de admitere și a cei neînscriși în primul an.

Scopul prelucrării datelor: Rezolvarea contestațiilor, respectiv dovadă în cazul fraudelor sau tentativelor de fraudă

Durata păstrării datelor: 5 ani după la terminarea anului universitar pentru care a fost organizat concursul de admitere, sau în care candidatul trebuia să se înscrie.

Absolvenți și foști studenți. Alumni

Universitatea, în concordanță cu cererile și recomandările ARACIS a elaborat proceduri pentru urmărirea în carieră a absolvenților, le aplică și elaborează rapoarte anuale pe care le face publice, inclusiv pe situl Universității.

Temeiul legal al prelucrării este consimțământul liber exprimat a persoanei vizate.

Durata păstrării datelor este permanent.

Modelul de notificare și consimțământ se află în Anexa 4.

Datele personale colectate, suplimentar față de cele din perioada de școlaritate sunt următoarele:

1. Numele și prenumele
2. Facultatea/specializarea absolvită
3. Număr de telefon
4. Adresa email
5. Adresa paginii web personale
6. Funcția la locul de muncă
7. Locul de muncă actual și cele anterioare
8. Alte studii efectuate după absolvire
9. Dacă este membru într-o organizație profesională
10. Referințe la publicări pe rețelele profesionale
11. Recunoaștere profesională, brevete, concursuri, premii, etc.

Servicii sociale - cămin studențesc, cantină.

Datele sunt prelucrate în scopul încheierii și executării contractelor și raporturilor juridice specifice procesului de cazare în spațiile/căminele Universității, pentru a desfășura în condiții optime ale activităților Universității, de educație și cultură.

Datele prelucrate sunt:

1. Numele și prenumele
2. Adresa e-mail
3. Facultatea/specializarea
4. Locul nașterii
5. Data nașterii
6. Codul Numeric Personal

7. Nr. actului de identitate
8. Cetățenia
9. Numărul de telefon personal

Temeiul legal
- Art. 6 (b) din Regulamentul UE, conform căruia 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.

Durata de păstrare a datelor este de 10 ani

Concursuri și conferințe

Facultățile pot organiza concursuri pe diferite discipline și conferințe.
Prelucrarea datelor este în scopul participării la concursurile pe diferite discipline și confereințe organizate de către Universitate.
Temeiul legal al prelucrării este consimțământul liber exprimat a persoanei vizate.
Durata păstrării datelor este permanent.
Modelul de consimțământ se află în Anexa 5.

Datele personale colectate sunt următoarele:
1. Numele și prenumele
2. Adresa
3. Adresa e-mail
4. Institutul de învățământ
5. Data nașterii
6. Cetățenia
7. Rezultatele obținute la concurs.

Sprijin material, burse, granturi Erasmus, CEEPUS, Makovecz acordate studenţilor

Universitatea asigură prin coordonatorii la nivelul instituţiei şi ale facultăților obținerea finanțărilor de mobilitate studențească în cadrul programelor Erasmus+, CEEPUS și Makovecz.
Pentru studenţii proprii, datele colectate sunt, suplimentar faţă de cele menţionate la datele legate de statutul de student:
1. autobiografie (Curriculum vitae)
2. date medicale ale participanţilor cu nevoi speciale
3. număr conturi bancare
4. date financiare (granturi)
5. rezultatele obţinute pe perioada mobilităţii

Pentru studenţii incoming se colectează următoarele date:
1. -Numele și prenumele
2. -Datele actului de identitate
3. -Cetățenie
4. -Sexul
5. -Adresa de corespondenţă
6. -Număr de telefon
7. -Adresa e-mail:
8. -Date privind studiile la Universitatea Sapientia
9. -Instituţia de proveniență, facultatea, specializarea, anul de studii, nivel de studii
10. -Rezultatele obţinute în cadrul mobilităţii
11. -Contul bancar
12. -Date financiare (granturi)

Destinatarii datelor cu caracter personal sunt: Comisia Europeană, Agenţia Naţională pentru Programe Comunitare în Domeniul Educaţiei şi Formării Profesionale (ANPCDEFP), organismele externe autorizate responsabile de verificare şi audit, institutiile partenere, conducerea Universității, coordonatorii programelor din facultăţi şi coordonatorul instituţional Erasmus, personalul secretariatelor administrative şi economice din cadrul facultăţilor şi al Rectoratului.

Temeiul legal:
- Art. 6 (b) din Regulamentul UE, conform căruia 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. În acest context termenul de contract se referă la contractul de mobilitate.
- Regulamentul programelor Erasmus+, CEEPUS, Makovecz

Termenul de păstrare a datelor în cadrul programului Erasmus este de 5 ani după încheierea programului de mobilitate

Vizite de documentare și schimb de experiență

Universitatea primește vizitatori cadre didactice şi administrative precum
- elevi de la alte instituții de învățământ primar, secundar
- studenți din instituțiile de învățământ superior partenere.

Universitatea nu prelucrează datele vizitatorilor doar în cazul în care li se asigură cazare.
În aceste cazuri sunt valabile principiile și dispozițiile din capitolul referitor la serviciile sociale - cămine studențești și cantină.

Stagii de practică și cercetare

Sunt aplicabile prevederile capitolului precedent.

Reguli privind controlul mijloacelor puse la dispoziția studenților de către Universitate

Conducerea Universității are drept de control asupra mijloacelor puse la dispoziția studentului.
Pe timpul controlului trebuie asigurat prezența studentului, exceptând cazurile în care condițiile procesului de control nu poate permite acesta.

Studentul trebuie informat despre scopul controlului, cine va efectua controlul şi procedura de control, precum și care sunt drepturile și căile de atac judiciare în legătură cu prelucrarea datelor pe parcursul procesului de control.

Pe parcursul controlului se va aplica principiul gradualității și proporționalității, în sensul că se vor verifica prima dată adresele respectiv rezumatele pentru determinarea caracterului personal sau oficial al conținutului. Conținuturile nepersonale se pot verifica nemijlocit de către Universitate.

Furnizare de date către Inspectoratele Teritoriale de Muncă

Universitatea este obligată să furnizeze date către Inspectoratele Teritoriale de Muncă în legătură cu cei înscriși în primul an de licență și primul an de masterat.

Temeiul legal:
-prelucrare de date în vederea respectării unei obligații legale –Art. 6 (c) din Regulamentul UE

Datele personale ale partenerilor comerciali.

Scopul prelucrării datelor este desfășurarea activității economice al Universității.

Universitatea păstrează aceste date în conformitate cu OMEF 3512/2008 și Anexa 6 a Legii Arhivelor Naționale, care stabilesc următoarele termene de păstrare a documentelor în felul următor

- în cazul registrelor și a documentelor justificative și contabile termenul de păstrare este de 10 ani, cu începere de la data încheierii exercițiului financiar în cursul căruia au fost întocmite.
- Facturile aferente bunurilor de capital, respectiv bunurilor imobile, care stau la baza determinării taxei pe valoarea adăugată se vor păstra conform termenului prevăzut în Codul Fiscal, și anume facturile se păstrează timp de 10 ani. Deși termenul de păstrarea a chitanțelor este de 5 ani, acestea fiind păstrate împreună cu celelalte documente fiscale se vor păstra și ele timp de 10 ani.
- Documentele financiar-contabile care atestă proveniența unor bunuri cu durată de viață mai mare de 10 ani se păstrează, de regulă, pe o perioadă de timp mai mare, respectiv pe perioada de utilizare a bunurilor.
- Contractele cu clienții sau furnizorii, precum si actele adiționale rezultate din acestea au termen de păstrare de 10 ani de la data încetării acestora.

Temeiul legal pentru care Universitatea păstrează datele persoanelor fizice care reprezintă și care semnează documente în numele persoanelor juridice cu care Universitatea intră în relații contractuale o prezintă îndeplinirea unei obligații legale.

Scopul păstrării datelor este pentru a ține legătura, pentru a exercita drepturile și obligațiile stipulate în aceste documente, termenul de păstrare a acestora fiind de 10 ani după expirare.

Temeiul legal pentru care Universitatea păstrează datele persoanelor fizice care nu semnează documente în numele persoanelor juridice cu care Universitatea intră în relații contractuale, dar sunt indicate ca fiind persoane de legătură, o prezintă interesul legitim al Universității. Datorată faptului că între părți există o relație contractuală, prelucrarea datelor nu lezează drepturile persoanei vizate legate de prelucrarea datelor personale. Partenerul contractual al Universității declară că a informat persoana vizată despre prelucrarea datelor personale. Termenul de păstrare a acestora este de 10 ani după expirare.

În toate cazurile enumerate mai sus destinatarii datelor sunt: conducătorul Universității, persoanele însărcinate cu interacțiunile cu partenerii comerciali, operatorii datelor contabile, Finanțatorii Universității.

Colectarea datelor personale în cazul licitațiilor anunțate este guvernată litera 44 din Preambulul și de Articolul 6 litera (1) din Regulamentului UE. Ofertanții trebuie anunțați în această privință.

Este obligația și responsabilitatea salariatului Universității însărcinat cu redactarea contractelor ca clauzele privind prelucrarea datelor personale să fie incluse în textul contractelor. Aceste clauze sunt redactate în Anexa 6.

Prelucrarea datelor în scop publicitar

Dacă persoana vizată contactează Universitatea pentru a solicita informații (de exemplu să primească materiale informative despre oferta educațională), prelucrarea datelor pentru a răspunde acestei solicitări este permisă.
Universitatea poate prelucra date personale în scopuri publicitare cum ar fi de exemplu fotografii sau imagini filmate ale studenților care participă la evenimente organizate de către Universitate, de către Organizația Studenților, sau alte entități, în cadrul campaniilor de imagine sau de promovare a Universității. Prelucrarea acestor date se face numai pe baza consimțământului persoanelor vizate.

Formularele de informare și consimțământ se află în Anexa 7. Dacă persoana vizată nu este de acord, aceste date nu se vor folosi în aceste scopuri.
În cazul în care obținerea consimțământului ar necesita un efort nejustificat, cum ar fi în cazul unui număr mare de persoane, fețele acestora va fi prelucrată în așa fel, ca persoanele să nu poată fi identificate. (blurare). În asemenea cazuri se va specifica: *"Din considerente privind protecția datelor cu caracter personal această fotografie a fost prelucrată."*

Prelucrarea datelor personale ale vizitatorilor site-ului web al Universității

Vizitatorii site-ului web al Universității trebuie informați despre utilizarea cookie-urilor. Utilizatorii își exprimă acordul sau dezacordul privind utilizarea acestora.
Cookie-urile sunt date speciale, care sunt trimise de situl web vizitat către browserul utilizatorului. Cookie-urile pot fi folosite pentru autentificare precum și pentru urmărirea comportamentului utilizatorilor, de exemplu reținerea preferințelor utilizatorilor. Durata valabilității cookie-urilor poate varia de la durata unui singur acces până la o durată indefinită.
Natura serviciilor web necesită marcarea utilizatorului (de exemplu consemnarea faptului că a intrat pe site) pentru a fi posibil afișarea conținutul corespunzător. Pericolul constă în existența posibilității de a urmări comportamentul pe internet al utilizatorului, chiar de către terți, cum ar fi Facebook sau Google Analytics, și creării de profiluri despre utilizatori, ceea ce deja ține de protecția datelor personale. Un alt pericol constă în faptul că utilizatorul nu are cunoștință despre existența acestor cookie-uri, și nici despre natura lor.
Tipuri de cookie
Session cookies. Acest tip de cookie constă dintr-un identificator de sesiune (session id). Acestea nu au o dată de expirare, browserele își pot da seama astfel că trebuie să fie șterse după fiecare sesiune.
Cookie-urile persistente sunt cele care expiră la un anumit moment de timp sau după o anumită perioadă de timp.
Cookie-urile esențiale sunt utilizate exclusiv pentru a facilita accesul la informațiile de pe site-ul Universității. Temeiul legal al utilizării cookie-urilor esențiale este, Art. 6 (1) litera (f) din GDPR, interesul legitim-asigurarea funcționării corecte a site-ului Universității.
Cookie-urile neesențiale sunt cele care nu sunt absolut necesare pentru afișarea conținutului în condiții bune de pe site-ul Universității. Aceste cookie-uri pot permite înregistrarea obiceiurilor de navigare ale utilizatorului pe o perioadă de timp.
Cookie-uri proprii sunt cookie-urile plasate pe dispozitivul utilizatorului de către domeniul **sapientia.ro.**
Cookie-uri părților terțe. Aceste cookie-uri sunt furnizate de domenii terțe, pentru facilitarea analizei accesării site-ului Universității.
Cookie-uri analitice. Site-ul Universității utilizează cookie-uri analitice de la Google Analytics, pentru a înțelege modul în care vizitatorii interacționează cu site-ul, cum ar fi de exemplu paginile vizitate, timpul petrecut pe o pagină, locația utilizatorului bazat pe IP, cum a ajuns pe site, etc. Cookie-urile Google Analytics sunt considerate proprii. Informații suplimentare se găsesc la adresa
https://support.google.com/analytics/answer/6004245?hl=ro
https://policies.google.com/technologies/partner-sites?hl=ro
Cookie-urile funcționale sunt
- proprii sau a părților terțe, de sesiune sau persistente, utilizate pentru identificarea utilizatorului.
-proprii sau a părților terțe, de sesiune sau persistente, utilizate pentru afișarea corectă a conținutului precum și personalizarea acestuia. Temeiul legal este consimțământul utilizatorului exprimat prin acceptarea termenilor de utilizare.
Lista cookie-urilor utilizate se află în Anexa 8.

Sistemul de supraveghere video al Universității

Scopul prelucrării

Scopul prelucrării datelor în cazul sistemului de supraveghere video este asigurarea securității persoanelor și bunurilor, pazei și protecției bunurilor, imobilelor și valorilor, respectând în același timp obligațiile ce revin Universității în calitate de operator de date, conform Regulamentului UE 2016/679 și măsurile de securitate adoptate pentru protecția datelor cu caracter personal, protejarea vieții private, a intereselor legitime și garantarea drepturilor fundamentale ale persoanelor vizate.

Utilizarea sistemului video este necesară pentru buna administrare și funcționare a Universității, în special în vederea controlului de securitate și pază.

Cu ajutorul acestui sistem se controlează accesul în incinta unității, se asigură securitatea bunurilor și siguranța persoanelor - angajați ai Universității, studenți, clienți sau vizitatori, precum și a proprietăților și informațiilor deținute. Sistemul de supraveghere video completează celelalte măsuri fizice de securitate, ajută la prevenirea, combaterea și, dacă e cazul, cercetarea accesului fizic neautorizat, inclusiv a accesului neautorizat la spațiile securizate și la încăperile protejate, accesul neautorizat la infrastructura informatică sau la informațiile operaționale. În plus, sistemul de supraveghere video ajută la prevenirea, detectarea sau investigarea furturilor de echipament sau de bunuri deținute de societate.

Sistemul de supraveghere video nu este utilizat în alt scop decât cel notificat, nu folosește la monitorizarea activității angajaților sau la pontaj. De asemenea, sistemul nu este mijloc de investigare sau de obținere a unor informații pentru anchetele interne sau procedurile disciplinare, cu excepția situațiilor în care se produce un incident de securitate fizică sau se observă un comportament infracțional (în circumstanțe excepționale imaginile pot fi transferate organelor de cercetare în cadrul unei investigații disciplinare sau penale).

Totodată sistemul video al Universității nu are ca scop captarea sau prelucrarea imaginilor, nici a creării profilurilor, nici a indexării, nici a dezvăluirii categoriilor speciale de date.

Temeiul legal al prelucrării o prezintă interesul legitim al Universității, precum și consimțământul părților vizate.

Informarea primară a persoanelor vizate se realizează în mod clar și permanent, prin intermediul semnelor adecvate, cu vizibilitate suficientă și localizate în zona supravegheată, astfel încât să semnaleze existența camerelor de supraveghere, dar și pentru a comunica informațiile esențiale privind prelucrarea datelor personale. Persoanele vizate sunt atenționate asupra existenței sistemului de supraveghere video și a proprietarului prin note de informare corespunzătoare, care cuprind scopul și durata prelucrării.

Politica privind utilizarea sistemelor video va fi disponibilă pe pagina de internet a Universității cât și în format fizic la sediul Universității.

Politica se aplică în cadrul activității de supraveghere prin mijloace video de către
- personalul externalizat care execută serviciul de pază și protecție
- personalul intern care asigură paza și mentenanța sistemelor de supraveghere

Sistemul de supraveghere prin mijloace video, cuprinde
-Rectoratul, Cluj-Napoca, str. Matei Corvin nr. 4, 400112 jud Cluj
-Facultatea de Științe Economice, Socio-Umane și Inginerești Miercurea Ciuc, Piața Libertății nr. 1 Miercurea Ciuc 530104 jud Harghita
-Facultatea de Științe și Arte Cluj-Napoca, Calea Turzii nr. 4, 400193 Cluj-Napoca jud. Cluj
-Facultatea de Științe Tehnice și Umaniste Târgu-Mureș, Târgu-Mureș/Corunca, 1C 547367 jud. Mureș

-Centrul de Studii Sfântu-Gheorghe, Str. Ciucului 20, Sfântu Gheorghe, 520019 jud Covasna

Zonele supravegheate prin mijloace video:
- zonele de acces și spațiile destinate publicului
- zonele cu acces restricționat
- împrejurimile clădirilor pentru a proteja spațiile exterioare
- locurile de păstrare, depozitare și manipulare a suporturilor de stocare a documentelor, a datelor și informațiilor cu caracter personal sau confidențial, precum și locurile unde se desfășoară activități care au un asemenea caracter.

Amplasarea camerelor a fost atent revizuită pentru a asigura limitarea pe cât posibil a monitorizării zonelor care nu prezintă interes pentru scopul urmărit și este anexată prezentei proceduri.
Dispozitivele de înregistrare sunt amplasate în spații bine protejate, asigurate și încuiate corespunzător, pentru eliminarea posibilității sustragerii suportului de stocare sau a dispozitivului, în special în timpul producerii unui eveniment.
Nu sunt monitorizate zonele în care există un nivel ridicat al așteptărilor privind viața privată, precum birourile, toaletele și alte locații similare.
În vederea asigurării unei protecții eficiente a drepturilor și libertăților fundamentale ale persoanelor fizice, în cadrul operațiunilor de supraveghere video a căilor publice de acces și a spațiilor publice deschise este interzisă prelucrarea de imagini care să vizualizeze interiorul imobilelor locuite sau a căilor de acces în acestea. Echipamentele sunt astfel instalate încât să se afle sub supraveghere doar acele spații identificate ca având nevoie de protecție suplimentară. Utilizatorii sistemului video sunt instruiți să monitorizeze doar astfel de zone.

Imaginile captate de sistemul de supraveghere video sunt vizualizate în timp real sau înregistrările doar de către administrația societății atunci când se observă o breșă de securitate, aceste imagini sunt vizualizate la sediul societății, într-o încăpere securizată, iar monitoarele nu pot fi văzute din exterior. Accesul în încăperea securizată este permisă doar persoanelor autorizate.
Persoanele autorizate sunt:
-personalul intern care execută serviciul de mentenanță a sistemului video
-angajații din punctele de control acces (portari)
-administratorul de sistem desemnat
-responsabilul cu securitatea datelor
-conducerea societății.
De la caz la caz, se poate acorda accesul în Camera de control și altor persoane, în afara celor menționate mai sus, doar pe bază de autorizare, iar aceste persoane vor fi în permanență supravegheate. Aceste persoane nu vor avea acces la datele personale prelucrate în activitatea de supraveghere video. Orice accesare a înregistrărilor video va fi documentată.

Sistemul de supraveghere video are ca funcție înregistrarea imaginilor și este echipat cu senzori de mișcare. Sistemul poate înregistra orice mișcare detectată de camerele instalate în zona supravegheată, alături de dată și oră. Toate camerele sunt funcționale 24 de ore, 7 zile pe săptămână.

Calitatea imaginilor permite recunoașterea celor care trec prin zona de acțiune a camerelor. Pentru o mai mare siguranță a prelucrării datelor care pot fi obținute în urma supravegherii video, camerele sunt fixe, astfel utilizatorul nu poate modifica perimetrul/ scopul supravegherii.
Nu se înregistrează sunetul.
Nu există conexiuni cu alte sisteme.

Stocarea datelor
Universitatea stochează aceste date pe baza următoarelor reguli:

- timpului de stocare a materialului filmat, în conformitate cu cerințele legale actuale, este limitat la un maxim de 30 de zile
- mediile de stocare (serverele pe care se stochează imaginile înregistrate) se află în spații securizate, protejate de măsuri de securitate fizică
- toți utilizatorii cu drept de acces au semnat declarații de confidențialitate, prin care se obligă să respecte prevederile legale în domeniu
- dreptul de acces se acordă utilizatorilor pe baza nevoii de a cunoaște, doar pentru acele resurse care sunt strict necesare pentru îndeplinirea atribuțiilor de serviciu
- doar administratorul de sistem, numit în acest sens de către Universitate, are dreptul de a acorda, modifica sau anula dreptul de acces al utilizatorilor
- Responsabilul de Protecție a Datelor Personale va fi consultat înainte de achiziționarea sau instalarea oricărui nou sistem video de protecție.

Exercitarea drepturilor de acces, intervenție, opoziție, ștergere și portabilitate
Pe întreaga perioadă de stocare a datelor cu caracter personal, persoanele vizate au dreptul de acces la datele personale care le privesc deținute de Universitate, de a solicita intervenția (acces/ștergere/actualizare/rectificare) sau de a se opune prelucrărilor, precum și dreptul la portabilitate conform legii.

Orice cerere de a accesa, rectifica, porta, bloca și/sau șterge date cu caracter personal ca urmare a utilizării camerelor video va trebui să fie adresată rectorului Universității sau decanilor facultăților la adresele de e-mail:

Unitatea	**Rector/Decan**	**Adresa email**
Rectorat, Cluj Napoca	Prof. dr. Tonk Márton	rektor@sapientia.ro
Facultatea de Științe și Arte Cluj Napoca	Lect. dr. Szenkovics Dezső	szenkovics@sapientia.ro
Facultatea de Ştiinţe Economice, Socio-Umane şi Inginereşti Miercurea Ciuc	Conf. dr. Lázár Ede	lazarede@uni.sapientia.ro
Centrul de studii Sfântu Gheorghe	Conf. dr. Domokos József	domi@ms.sapientia.ro
Facultatea de Ştiinţe Tehnice şi Umaniste Târgu Mureş	Conf. dr. Domokos József	domi@ms.sapientia.ro

Răspunsul la solicitarea de acces, intervenție sau opoziție se dă în termen de 15 zile calendaristice.
Dacă nu se poate respecta acest termen, persoana vizată va fi informată asupra motivului de amânare a răspunsului, de asemenea i se va comunica și procedura care va urma pentru soluționarea cererii.

Dacă există solicitarea expresă a persoanei vizate, se poate acorda dreptul de a vizualiza imaginile înregistrate care o privesc. Imaginile furnizate cu condiția de a nu prejudicia drepturile terților (persoana vizată va putea vizualiza doar propria imagine). În cazul unei asemenea solicitări, persoana vizată este obligată să se identifice dincolo de orice suspiciune (să prezinte actul de identitate și să atașeze o fotocopie a acestuia când solicită accesul la date), să menționeze data, ora, locația și împrejurările în care a fost înregistrată de camerele de supraveghere. De asemenea, persoana vizată va prezenta și o fotografie recentă astfel încât utilizatorii desemnați să o poată identifica mai ușor în imaginile filmate.
În cazul în care cererile din partea unei persoane vizate sunt în mod vădit nefondate sau excesive, în special din cauza caracterului lor repetitiv, Universitatea poate:
- fie să perceapă o taxă rezonabilă ținând cont de costurile administrative pentru furnizarea informațiilor sau a comunicării sau pentru luarea măsurilor solicitate;
- fie să refuze să dea curs cererii.
Exercitarea drepturilor este gratuită pentru o singură solicitare în cursul unui an calendaristic.

În cazul în care are îndoieli întemeiate cu privire la identitatea persoanei fizice care înaintează cererea având ca obiect exercitarea unuia din drepturile menționate, Universitatea poate solicita furnizarea de informații suplimentare necesare pentru a confirma identitatea persoanei vizate.

Necesitatea de a restricționa accesul se poate impune și în cazul în care există obligația de a proteja drepturile și libertățile unor terțe persoane, de exemplu dacă în imagini apar și alte persoane și nu există posibilitatea de a obține consimțământul lor sau nu se pot extrage, prin editarea imaginilor, datele personale nerelevante.

De asemenea, potrivit Regulamentului general privind protecția datelor, persoana vizată are dreptul de a depune plângere (art. 77) la Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal la sediul acesteia din B-dul G-ral Gheorghe Magheru, nr. 28-30, sector 1, București, cod poștal 0103336, e-mail: anspdcp@dataprotection.ro, sau de a se adresa justiției (art. 79).

PREŞEDINTELE SENATULUI
Prof. univ. dr. ing. DÁVID László

Avizat,
Av. ZSIGMOND Erika, consilier juridic