MINISTERUL EDUCAȚIEI NAȚIONALE
Universitatea Națională de Arte "George Enescu"

Universitatea Națională de Arte
George Enescu
Iași

Str. Cuza Vodă 29,
700040, Iași, RO

T: 0040 232 / 212 549
F: 0040 232 / 212 551

rector@arteiasi.ro
www.arteiasi.ro

REGULAMENTUL

Universității Naționale de Arte " George Enescu " Iași

privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu

caracter personal și privind libera circulație a acestor date

ELABORAT	VERIFICAT	APROBAT		CODUL – R 29	
D.P.O. Bahnea Dragos	Oficiu juridic	Consiliul de administrație	Senat		
	Consilier juridic Dragoș Bahnea	Prof. univ. dr. Atena – Elena Simionescu	Prof. univ. dr. Doru Albu		
18.02.2019	21.02.2019	18.03.2019	20.03.2019		
				EDIȚIA	1
				REVIZIA	

COLEGIUL CONSILIERILOR JURIDICI IAȘI
BAHNEA DRAGOS
CONSILIER JURIDIC DEFINITIV
22D-0316

Prezentul regulament are la bază dispozițiile Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor), precum și legislația internă, respectiv Legea nr.102/2005 republicată prvind inființarea, organizarea și funcționarea A.N.S.P.D.C.P.

I. DISPOZIȚII CU CARACTER GENERAL

Art. 1 Obiect și obiective

(1) Prezentul regulament are ca scop implementarea normelor referitoare la protecția persoanelor fizice (angajați, studenți, invitați, asociați și alți terți cu care universitatea contractează) în ceea ce privește prelucrarea datelor acestora cu caracter personal, normele referitoare la libera circulație a datelor cu caracter personal în cadrul UNAGE Iași, precum și în relațiile cu terțe instituții.

Art. 2 Domeniul de aplicare

(1) Prezentul regulament se aplică prelucrării datelor cu caracter personal, efectuată total sau parțial prin mijloace automatizate, precum și prelucrării prin alte mijloace decât cele automatizate a datelor cu caracter personal care fac parte dintr-un sistem de evidență a datelor sau care sunt destinate să facă parte dintr-un sistem de evidență a datelor.

Art. 3 Definiții

3.1. „date cu caracter personal" (datele) reprezintă 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;

3.2. „prelucrare" înseamnă orice operațiune sau set de operațiuni efectuate asupra datelor, 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 stocate cu scopul de a

limita prelucrarea viitoare a acestora;

4. „creare de profiluri" înseamnă orice formă de prelucrare automată a datelor care constă în utilizarea acestora 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 (aplicabil si in cazul studentilor, privind performantele la studio, etc.), situația economică, sănătatea, preferințele personale, interesele, fiabilitatea, comportamentul, locul în care se află persoana fizică respectivă sau deplasările acesteia;

5. „pseudonimizare" înseamnă prelucrarea datelor 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 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 (universitatea);

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.

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 transmise, stocate sau prelucrate într-un alt mod, sau la accesul neautorizat la acestea;

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 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;

II. DISPOZIȚII SPECIFICE

Art. 4. Principii legate de prelucrarea datelor cu caracter personal

(1) Datele trebuie prelucrate numai în mod legal, echitabil și transparent față de persoana vizată („legalitate, echitate și transparență");

(2) Datele trebuie colectate în scopuri determinate, explicite și legitime și nu trebuie prelucrate ulterior într-un mod incompatibil cu aceste scopuri; prelucrarea ulterioară în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice nu este considerată incompatibilă cu scopurile inițiale;

(3) Datele sunt adecvate, relevante și limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate („reducerea la minimum a datelor"); În acest sens, se vor solicita doar datele strict necesare pentru indeplinirea scopului.

(4) Datele trebuie sa fie exacte și să fie actualizate, daca este necesar („exactitate");

(5) Datele trebuie păstrate într-o formă care permite identificarea persoanelor vizate pe o perioadă care nu depășește perioada necesară îndeplinirii scopurilor în care sunt prelucrate datele; datele cu caracter personal pot fi stocate pe perioade mai lungi în măsura în care acestea vor fi prelucrate exclusiv în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice;

(6) Datele trebuie sa fie prelucrate într-un mod care asigură securitatea adecvată a datelor cu caracter personal, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luarea de măsuri tehnice sau organizatorice corespunzătoare („integritate și confidențialitate").

(7) UNAGE Iași, în calitatea sa de operator, este responsabil de respectarea acestor principii și trebuie să poata demonstra această respectare („responsabilitate").

Art.5. Legalitatea prelucrării

(1) Prelucrarea datelor de către UNAGE Iași are un caracter legal numai dacă și în măsura în care se aplică cel puțin una dintre următoarele condiții:

(a) persoana vizată și-a dat consimțământul pentru prelucrarea datelor sale pentru unul sau mai multe scopuri specifice;

(b) prelucrarea este necesară pentru executarea unui contract/conventie/acord/etc. la care persoana vizată este parte sau pentru a face demersuri la cererea persoanei vizate înainte de încheierea unui contract;

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

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

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

(f) prelucrarea este necesară în scopul intereselor legitime urmărite de universitate sau de o parte terță, cu excepția cazului în care prevalează interesele sau drepturile și libertățile fundamentale ale persoanei vizate, care necesită protejarea datelor cu caracter personal, în special atunci când persoana vizată este un copil.

Art.6. Condiții privind consimțământul

(1) În cazul în care prelucrarea se bazează pe consimțământ, UNAGE Iași trebuie să demonstreze că persoana vizată și-a dat consimțământul pentru prelucrarea datelor sale.

(2) În cazul în care consimțământul persoanei vizate este dat în contextul unei declarații scrise care se referă și la alte aspecte, cererea privind consimțământul trebuie să fie prezentată într-o formă care o diferențiază în mod clar de celelalte aspecte, într-o formă inteligibilă și ușor accesibilă, utilizând un limbaj clar și simplu.

(3) Persoana vizată are dreptul să își retragă în orice moment consimțământul, exceptie situatiile prin care acest lucru este expres interzis prin lege. Înainte de acordarea consimțământului, persoana vizată este informată cu privire la acest lucru. Retragerea consimțământului se face la fel de simplu ca acordarea acestuia.

(4) Este interzisă prelucrarea datelor care dezvăluie originea rasială sau etnică, opiniile politice, confesiunea religioasă sau convingerile filozofice sau apartenența la sindicate și prelucrarea de date genetice, de date biometrice pentru identificarea unică a unei persoane fizice, de date privind sănătatea sau de date privind viața sexuală sau orientarea sexuală ale unei persoane fizice, cu exceptia cazurilor in care:

(a) persoana vizată și-a dat consimțământul explicit pentru prelucrarea acestor date cu caracter personal pentru unul sau mai multe scopuri specifice ;

(b) prelucrarea este necesară în scopul îndeplinirii obligațiilor și al exercitării unor drepturi specifice ale universitatii sau ale persoanei vizate în domeniul ocupării forței de muncă și al securității si protecției sociale, în măsura în care acest lucru este autorizat de lege ori de un acord colectiv de muncă încheiat în temeiul dreptului intern care prevede garanții adecvate pentru drepturile fundamentale și interesele persoanei vizate;

(c) prelucrarea este necesară în scopuri legate de medicina preventivă sau a muncii, ori de evaluarea capacității de muncă a angajatului ;

Art.7. Transparența informațiilor, a comunicărilor și a modalităților de exercitare a drepturilor persoanei vizate

(1) UNAGE Iași va lua toate măsurile adecvate pentru a furniza persoanei vizate orice informații referitoare la prelucrare, într-o formă concisă, transparentă, inteligibilă și ușor accesibilă, utilizând un limbaj clar și simplu. Informațiile se furnizează în scris sau prin alte mijloace, inclusiv, atunci când este oportun, în format electronic. La solicitarea persoanei vizate, informațiile pot fi furnizate verbal, cu condiția ca identitatea persoanei vizate să fie dovedită prin alte mijloace.

Art.8. (1)În cazul în care datele unei persoane vizate sunt colectate de la aceasta, universitatea va furniza de indata persoanei informațiile următoare:

(a) identitatea și datele de contact ale universitatii și, după caz, ale reprezentantului acestuia;

(b) datele de contact ale responsabilului cu protecția datelor, după caz;

(c) scopurile în care sunt prelucrate datele cu caracter personal, precum și temeiul juridic al prelucrării;

(d) destinatarii sau categoriile de destinatari ai datelor cu caracter personal;

(2) În plus, universitatea va mai furniza persoanei vizate si următoarele informații suplimentare :

(a) perioada pentru care vor fi stocate datele cu caracter personal sau, dacă acest lucru nu este posibil, criteriile utilizate pentru a stabili această perioadă;

(b) existența dreptului de a solicita universitatii, în ceea ce privește datele cu caracter personal referitoare la persoana vizată, accesul la acestea, rectificarea sau ștergerea acestora sau restricționarea prelucrării sau a dreptului de a se opune prelucrării, precum și a dreptului la portabilitatea datelor;

(c) existența dreptului de a retrage consimțământul în orice moment, fără a afecta legalitatea prelucrării efectuate pe baza consimțământului înainte de retragerea acestuia, atunci cand aceasta este permis de lege;

(d) dreptul de a depune o plângere în fața unei autorități de supraveghere;

(e) dacă furnizarea de date reprezintă o obligație legală sau contractuală sau o obligație necesară pentru încheierea unui contract, precum și dacă persoana vizată este obligată să furnizeze aceste date și care sunt eventualele consecințe ale nerespectării acestei obligații;

(3) În cazul în care UNAGE Iași intenționează să prelucreze ulterior datele cu caracter personal într-un alt scop decât cel pentru care acestea au fost colectate, universitatea furnizează persoanei vizate, înainte de această prelucrare ulterioară, informații privind scopul secundar respectiv și orice informații suplimentare relevante, în conformitate cu alineatul (3).

Art.9. (1)În cazul în care datele cu caracter personal nu au fost obținute de la persoana vizată, universitatea furnizează persoanei vizate următoarele informații:

(a) identitatea și datele de contact ale universitatii și, după caz, ale reprezentantului acestuia;

(b) datele de contact ale responsabilului cu protecția datelor, după caz;

(c) scopurile în care sunt prelucrate datele cu caracter personal, precum și temeiul juridic al prelucrării;

(d) categoriile de date cu caracter personal vizate;

(e) destinatarii sau categoriile de destinatari ai datelor cu caracter personal, după caz;

(2) Pe lângă informațiile menționate la alin. (1), universitatea furnizează și următoarele informații necesare pentru a asigura o prelucrare echitabilă și transparentă în ceea ce privește persoana vizată:

(a) perioada pentru care vor fi stocate datele cu caracter personal sau, dacă acest lucru nu este posibil, criteriile utilizate pentru a stabili această perioadă;

(b) existența dreptului de a solicita operatorului, în ceea ce privește datele cu caracter personal referitoare la persoana vizată, accesul la acestea, rectificarea sau ștergerea acestora sau restricționarea prelucrării și a dreptului de a se opune prelucrării, precum și a dreptului la portabilitatea datelor;

(c) existența dreptului de a retrage consimțământul în orice moment, fără a afecta legalitatea prelucrării efectuate pe baza consimțământului înainte de retragerea acestuia;

(d) dreptul de a depune o plângere în fața unei autorități de supraveghere;

(e) sursa din care provin datele cu caracter personal și, dacă este cazul, dacă acestea provin din surse disponibile public;

(g) existența unui proces decizional automatizat incluzând crearea de profiluri, precum și informații pertinente privind logica utilizată și privind importanța și consecințele preconizate ale unei astfel de prelucrări pentru persoana vizată.

(3) UNAGE Iași furnizează informațiile menționate mai sus:

(a) într-un termen rezonabil după obținerea datelor cu caracter personal, dar nu mai mare de o lună ;

(b) dacă datele cu caracter personal urmează să fie utilizate pentru comunicarea cu persoana vizată, cel târziu în momentul primei comunicări către persoana vizată respectivă; sau

(c) dacă se intenționează divulgarea datelor cu caracter personal către un alt destinatar, cel mai târziu la data la care acestea sunt divulgate pentru prima

oară.

(4) În cazul în care UNAGE Iași intenționează să prelucreze ulterior datele cu caracter personal într-un alt scop decât cel pentru care acestea au fost obținute, universitatea furnizează persoanei vizate, înainte de această prelucrare ulterioară, informații privind scopul secundar respectiv și orice informații suplimentare relevante.

Art.10. Dreptul de acces al persoanei vizate

(1) Persoana vizată are dreptul de a obține din partea universității o confirmare că se prelucrează sau nu date cu caracter personal care o privesc și, în caz afirmativ, acces la datele respective și la informații privind scopul prelucrarii, categorii de date prelucrate, destinatari carora le-au fost divulgate datele sau le vor fi divulgate, prerioada de stocare, etc.:

(2) În cazul în care datele sunt transferate către un terț, persoana vizată are dreptul să fie informată cu privire la acest lucru si privind garantia protectiei datelor.

(3) UNAGE Iași furnizează o copie a datelor care fac obiectul prelucrării.

(4) Dreptul de a obține o copie menționată la alineatul (3) nu aduce atingere drepturilor și libertăților altora.

Art.11. Rectificare și ștergere

(1) Persoana vizată are dreptul de a obține de la universitate rectificarea de îndată a datelor cu caracter personal inexacte care o privesc.

(2)Dreptul la ștergerea datelor („dreptul de a fi uitat")

(a) Persoana vizată are dreptul de a obține din partea universității ștergerea datelor cu caracter personal care o privesc, fără întârzieri nejustificate, iar operatorul are obligația de a șterge datele cu caracter personal fără întârzieri nejustificate cu excepția cazului în care dispoziții legale nu permit acest lucru;

(3) În cazul în care universitatea a făcut publice datele cu caracter personal și este obligata să le șteargă, universitatea va lua măsuri rezonabile, inclusiv măsuri tehnice, pentru a informa operatorii care prelucrează datele cu caracter personal că persoana vizată a solicitat ștergerea oricăror linkuri către datele respective sau a oricăror copii sau reproduceri ale acestor date cu caracter personal.

Art.12. Dreptul la restricționarea prelucrării

(1)Persoana vizată are dreptul de a obține din partea universității restricționarea prelucrării în cazul în care se aplică unul din următoarele cazuri:

(a) persoana vizată contestă exactitatea datelor, pentru o perioadă care îi

permite operatorului să verifice exactitatea datelor;

(b) prelucrarea este ilegală, iar persoana vizată se opune ștergerii datelor cu caracter personal, solicitând în schimb restricționarea utilizării lor;

(c) universitatea nu mai are nevoie de datele cu caracter personal în scopul prelucrării, dar persoana vizată i le solicită pentru constatarea, exercitarea sau apărarea unui drept în instanță;

(2) În cazul în care prelucrarea a fost restricționată, astfel de date pot, cu excepția stocării, să fie prelucrate numai cu consimțământul persoanei vizate sau pentru constatarea, exercitarea sau apărarea unui drept în instanță sau pentru protecția drepturilor unei alte persoane fizice sau juridice sau din motive de interes public.

(3) O persoană vizată care a obținut restricționarea prelucrării este informată de către universitatea înainte de ridicarea restricției de prelucrare.

(4) Universitatea comunică fiecărui destinatar căruia i-au fost divulgate datele cu caracter personal orice rectificare sau ștergere a datelor cu caracter personal sau restricționare a prelucrării efectuate, cu excepția cazului în care acest lucru se dovedește imposibil sau presupune eforturi disproporționate.

Art.13. Dreptul la portabilitatea datelor

(1) Persoana vizată are dreptul de a primi datele cu caracter personal care o privesc și pe care le-a furnizat universității într-un format structurat, care poate fi citit automat și are dreptul de a transmite aceste date altui operator, fără obstacole din partea universitatii, în cazul în care:

(a) prelucrarea se bazează pe consimțământ sau pe un contract;

(b) prelucrarea este efectuată prin mijloace automate.

(2) În exercitarea dreptului său la portabilitatea datelor în temeiul alineatului (1), persoana vizată are dreptul ca datele cu caracter personal să fie transmise direct de la un operator la altul acolo unde acest lucru este fezabil din punct de vedere tehnic.

(3) Dreptul menționat la alineatul (1) nu aduce atingere drepturilor și libertăților altora.

Art.14. Dreptul la opoziție

(1) În orice moment, persoana vizată are dreptul de a se opune, din motive legate de situația particulară în care se află, prelucrării datelor sale cu caracter personal, în măsura în care dispozițiile legale în materie o permit. Univesitatea nu va mai prelucra datele, cu excepția cazului în care demonstrează că are motive legitime și imperioase care justifică prelucrarea și care prevalează asupra

intereselor, drepturilor și libertăților persoanei vizate sau că scopul este constatarea, exercitarea sau apărarea unui drept în instanță.

(2) Atunci când prelucrarea datelor are drept scop marketingul direct, persoana vizată are dreptul de a se opune în orice moment prelucrării în acest scop a datelor cu caracter personal care o privesc, inclusiv creării de profiluri, în măsura în care este legată de marketingul direct respectiv.

(3) În cazul în care persoana vizată se opune prelucrării în scopul marketingului direct, datele nu vor mai fi prelucrate în acest scop.

(4) Cel târziu în momentul primei comunicări cu persoana vizată, dreptul menționat la alineatele (1) și (2) este adus în mod explicit în atenția persoanei vizate și este prezentat în mod clar și separat de orice alte informații.

(6) În cazul în care datele sunt prelucrate în scopuri de cercetare științifică sau istorică sau în scopuri statistice, persoana vizată, din motive legate de situația sa particulară, are dreptul de a se opune prelucrării datelor cu caracter personal care o privesc, cu excepția cazului în care prelucrarea este necesară pentru îndeplinirea unei sarcini din motive de interes public.

Art.15. Procesul decizional individual automatizat, inclusiv crearea de profiluri

(1) Persoana vizată are dreptul de a nu face obiectul unei decizii bazate exclusiv pe prelucrarea automată, inclusiv crearea de profiluri, care produce efecte juridice care privesc persoana vizată sau o afectează în mod similar într-o măsură semnificativă.

(2) Alineatul (1) nu se aplică în cazul în care decizia:

(a) este necesară pentru încheierea sau executarea unui contract între persoana vizată și universitate;

(b) este autorizată prin legislația aplicabilă universității și care prevede, de asemenea, măsuri corespunzătoare pentru protejarea drepturilor, libertăților și intereselor legitime ale persoanei vizate; sau

(c) are la bază consimțământul explicit al persoanei vizate.

(3) Deciziile menționate la alineatul (2) nu au la bază categoriile speciale de date cu caracter personal, cu excepția cazurilor premise de lege.

III. RESPONSABILITATEA UNAGE Iași

Art.16. Asigurarea protecției datelor cu caracter personal

(1) Universitatea va pune în aplicare măsuri tehnice și organizatorice adecvate pentru a garanta și a fi în măsură să demonstreze că prelucrarea se efectuează în

conformitate cu prezentul regulament. Respectivele măsuri se revizuiesc și se actualizează dacă este necesar.

(2) Atunci când sunt proporționale în raport cu operațiunile de prelucrare, măsurile menționate la alineatul (1) includ punerea în aplicare de către universitate a unor politici adecvate de protecție a datelor.

(3) Universitatea, atât în momentul stabilirii mijloacelor de prelucrare, cât și în cel al prelucrării în sine, pune în aplicare măsuri tehnice și organizatorice adecvate, cum ar fi pseudonimizarea, care sunt destinate să pună în aplicare în mod eficient principiile de protecție a datelor, precum reducerea la minimum a datelor, și să integreze garanțiile necesare în cadrul prelucrării, pentru a proteja drepturile persoanelor vizate.

(4) Universitatea se va asigura că sunt prelucrate numai datele care sunt necesare pentru fiecare scop specific al prelucrării. Respectiva obligație se aplică volumului de date colectate, gradului de prelucrare a acestora, perioadei lor de stocare și accesibilității lor.

Art.17. Evidențele activităților de prelucrare

(1) Datele de contact :

- Operator : Universitatea Nationala de Arte "G.Enescu" Iasi, Iasi, str.Cuza Voda 29, tel.0232/212549, rectorat@arteiasi.ro.
- Responsabil protecția datelor cu caracter personal : Bahnea Dragoș, tel.0745328396, email juridicdpo@arteiasi.ro ;

(2) Scopurile prelucrării :

- Încheierea și derularea contractelor de muncă/cercetare/proiecte/susținerea masterclass-uri/worhshop-uri, etc.;
- Încheierea și derularea contractelor de studii nivel licență/masterat/doctorat/post universitare/formare profesională/etc. ;
- Arhivarea în interes public, conform prevederilor legale în vigoare ;
- În scopuri privind medicina muncii ;
- În scopul realizării unor lucrări de cercetare științifică/istorică ori în scopuri statistici ;

(3) Categorii de persoane vizate și de date cu caracter personal prelucate în cadrul UNAGE Iași :

(a) Persoane vizate :

- Angajați personal didactic de predare, didactic de cercetare, didactic

auxiliar și nedidactic ;

- Personal didactic invitat ;
- Studenți la cele trei niveluri, participanții la studii post doctorale ori de perfecționare;
- Terți cocontractanți ;
- Voluntari;

(b) Categorii de date prelucrate de către UNAGE Iași :

- Toate cele prevăzute la art.3 pct.1, plus datele genetice, biometrice și cele privind sănătatea ;

(4) Termen de păstrare a datelor prelucrate :

- Datele privind angajații, personalul invitat, studenții, terții cocontractanți și voluntarii vor fi arhivate și păstrate conform termenelor prevăzute de legislația specifică .
- Imaginile înregistrate de camerele sistemului de securitate din incintele universitatii se vor pastra pentru perioada permisa de DVR –ul (dispozitivul de stocare) a sistemului, urmand a fi sterse automat ulterior acestei perioadei.

(5) Categoriile de activități de prelucrare desfășurate în UNAGE Iasi :
- toate cele prevazute la art.3 pct.2 din prezentul regulament.

(6) Comparimente/birouri/servicii care prelucreaza date cu caracter personal :

- secretariatele ;
- serviciul informatizare și activități tipografice ;
- compartimentul resurse umane ;
- serviciul contabilitate și salarizare ;
- oficiul juridic ;
- registratura ;
- biblioteca ;
- administrare cămin ;

Art.18. Măsuri de protecție a datelor cu caracter personal

(1) Utilizarea de sisteme, programe și dispozitive de prelucrare a datelor care sa asigure protecția acestora împotriva acțiunilor de sustragere ori distrugere. Compartimentele, secretariatele, birourile, serviciile care operează cu date cu

caracter personal vor face propuneri în acest sens (achiziționarea de sisteme, programe, etc.).

(2) Accesul unui număr cât mai restrâns de persoane la bazele de date cu caracter personal.

(3) Evitarea transmiterii de date prin intermediul poștei electronice de tip gmail, yahoo, Hotmail, etc.

(4) Transmiterea documentelor ce conțin date cu caracter personal, în format letric, în plic închis și sigilat;

(6) Pseudonimizarea și criptarea (atunci când este posibil) a datelor cu caracter personal;

(7) Testarea, evaluarea și aprecierea periodică ale eficacității măsurilor tehnice și organizatorice pentru a garanta securitatea prelucrărilor;

(8) Pastrarea datelor pentru un termen cât mai scurt, acolo unde este posibil, cu respectarea dispozițiilor legale în acest sens;

(9) Securizarea serverelor, a bazelor de date și monitorizarea traficului de internet.

În rețeaua UNAGE Iași există servere ce utilizează sisteme de operare tip Microsoft Windows Server și care găzduiesc aplicații cu acces online pe bază de IP real. Aceste aplicații deservesc diversele departamente ale universității, incluzând totodată baze de date: University management system (UMS) - pentru secretariatele facultăților, Liberty - pentru Bibliotecă, Premier – pentru Contabilitate și Administrativ, Legis – pentru Oficiul juridic și Resurse umane, Registrul Matricol Unic – pentru secretariatele facultăților. În afara serverelor enumerate mai există servere ce utilizează sisteme de operare de tip Linux, folosite fie ca și router - cazul serverului ce susține traficul de internet pentru sediile din str. Costache Negruzzi și cel din str. Sărărie, fie ca și server pentru site-urile aparținând UNAGE Iași, server de e-mail, server pentru aplicații cloud, e-learning etc.

În afara acestora, mai exista un router hardware tip Cisco, ce deserveste traficul de internet pentru sediul din str. Cuza Vodă.

Configurarea, securizarea și monitorizarea acestor servere se face conform următoarelor proceduri:

- **Serverele bazate pe Microsoft Windows Server**

  - Instalarea Microsoft Windows Server se execută doar pe stații

performante, cu arhitectură tip server, specifică funcționării non-stop;

- Alimentarea de la rețeaua electrică a serverului se face prin intermediul unei unități UPS, ce asigură protecție la șocuri electrice și funcționează ca o baterie atunci când se înregistrează întreruperi ale alimentării cu electricitate;

- Sistemul de operare poate fi configurat astfel încât, atunci când bateria ajunge la un nivel minim stabilit, acesta să poată lansa comanda de închidere a serverului, pentru a evita închiderea bruscă a acestuia, fapt ce poate duce la coruperea sau pierderea datelor stocate sau la deteriorarea componentelor hardware;

- Este recomandată eliminarea altor conturi de utilizator și păstrarea unui singur cont de administrator, în cazul serverelor ce găzduiesc aplicații și baze de date cu acces online, fără a fi nevoie de deployment pe stații client din rețeaua internă;

- Parolarea alfanumerică (conține litere și cifre) a conturilor de administrator;

- Se actualizează zilnic, de pe site-ul Microsoft, cu update-uri de securitate și stabilitate a sistemului de operare;

- Instalarea de aplicații antivirus performante și programarea updatării zilnice (cel puțin) a bazei acestora de date urmată de scanarea fișierelor serverului. Dacă este cazul, se poate activa și configura, conform nevoilor, protecția firewall;

- Se recomandă instalarea și configurarea doar a acelor opțiuni ale sistemului de operare (server role) necesare scopului dedicat al serverului;

- Este recomandată evitarea instalării de aplicații care nu sunt absolut necesare scopului dedicat al serverului (codecuri, playere, browsere, office etc.)

- Monitorizarea la distanță (remote) a serverului se poate face activând funcția de remote acces a sistemului de operare, configurată cu acces doar pentru contul de administrator. Se

recomandă, de asemenea, activarea și configurarea aplicației firewall pentru remote acces;

- Pentru serverele unde, din diverse motive tehnice, nu poate fi activat și configurat satisfăcător un firewall, se recomandă dezactivarea funcției remote acces și înlocuirea acestea cu o aplicație ce permite controlul serverului la distanță printr-o conexiune virtuală securizată;
- Sistemul de operare Windows trebuie programat să realizeze backup-ul datelor ce le conține și a configurărilor sale la sfârșitul fiecărei săptămâni de lucru. Un astfel de backup se face pe un alt dispozitiv de stocare decât HDD-ul pe care sistemul este instalat și care conține datele ce trebuie salvate. Astfel, copia de siguranță se poate realiza pe un alt HDD intern, pe un HDD extern, pe un network adress storage securizat (NAS) sau pe un alt calculator din rețeaua internă dedicat;
- Se recomanda realizarea unor copii de siguranță (backup) și cu o terță aplicație (Acronis, Clonezilla etc.) decât cea oferită de sistemul de operare, cel puțin o dată pe lună;
- În plus, tot pentru siguranța datelor, se recomandă, de la bun inceput, instalarea sistemului de operare pe o matrice RAID de tip mirroring.

- **Serverele bazate pe sisteme de operare Linux**

Procedurile de configurare, securizare, monirorizare și backup pentru sistemele server ce rulează sisteme de operare Linux (distribuții Linux) sunt, în principiu, aceleași ca la serverele bazate pe Microsoft Windows.

Avantajele sistemelor de operare Linux sunt legate de gratuitatea lor, de numărul mare de distribuții diponibile și de faptul că sunt mai puțin expuse atacurilor de tip malware sau hacker. Dezavantajele față de sistemele de operare Windows sunt legate de numarul inferior de aplicații consacrate dezvoltate pentru ele, de suportul tehnic al celor care le produc și de dicerse probleme de compatibilitate și stabilitate.

Diferențele între distribuțiile Linux cât și față de Windows derivă și din scopul, rolul pe care îl îndeplineste un server. În general serverele Linux sunt preferate pentru: router internet, server pentru hostare site-uri, server de email, cloud etc. Astfel, sunt de menționat următoarele proceduri:

- Actualizarea zilnică cu update-uri de securitate și stabilitate a sistemului de operare se face doar de pe unul dintre serverele dedicate distribuției de Linux folosite și nu de pe serverele altor distribuției. Este necesară, după caz, verificarea periodică a configurării automate de update, în vederea confirmării adreselor serverelor pentru download;

- În afară de update-urile menționate se recomandă verificarea periodică (de obicei 6-12 luni) pentru apariția unei versiuni superioare a distribuției. Se recomandă ca această nouă versiune să fie testată pe un server de probă înainte de a fi instalată pe serverul de lucru;

- Accesul, monitorizarea și alertarea remote este mult mai facilă în cazul serverelor cu distribuții Linux, oferta de aplicații gratuite fiind mai bogată. Se pot configura alerte pentru breșe de securitate, pierderea conexiunii internet sau shutdown neprogramat ce pot fi primite de către administratorul de sistem pe mail sau SMS;

- Serverele dedicate traficului de internet (routere) pot fi configurate astfel încât să aibă o listă de excluderi (acces blocat) pentru adrese de internet sau IP-uri cunoscute sau înregistrate ca fiind amenințări de securitate;

- În afară de metodele de backup menționate în cazul serverelor Windows, metode ce pot fi aplicate asemănător și pentru Linux, se recomandă și salvarea configurației setărilor (config) sistemului de operare, după ce a fost testat cu succes. Aceasta se realizează mai ușor decât un backup clasic și este foarte utilă atunci când se înregistrează un update necorespunzător sau o corupere, din diverse motive, a kernelului distribuției, ori când dorim reinstalarea distribuției pe un server similar sau asemănător (pentru sistemele linux nu e nevoie de serial sau activare la o nouă instalare);

(10) Utilizarea stațiilor de lucru și a rețelei de internet

În afară de servere, rețeaua UNAGE Iași pune la dispoziție utilizatorilor, prin intermediul adminitratorilor de rețea, elemente de rețea active (routere WiFi, switch-uri), câteva clase de adrese IP interne, calculatoare, siteme de operare Microsoft Windows și aplicații compatibile cu licență.

Dintre procedurile de urmat în vederea utilizării corespunzătoare, atât de către membrii Serviciului Informatizare cât și de către utilizatorii obișnuiți, a inventarului hardware-software și a facilităților puse la dispoziție în rețeaua informatică a UAGE, sunt de menționat:

- Fiecare utilizator, angajat al universității, primește, în funcție de cerințele postului și de priorități, conform unui referat aprobat de către departamentele specifice (contabilitate, adminstrativ, conducerea universității) o stație de lucru (PC sau laptop). Această stație îi este atribuită în inventar, din inventarul existent al universității, fie prin achiziționare (echipament nou), fie în urma ocupării unui post eliberat care a avut în inventarul sau o stație de lucru. Același lucru este valabil și în cazul perifericelor, consumabilelor sau echipamentelor de birotică atașate (boxe, cameră web, claviaturi, printere, cartușe etc.) și a aplicațiilor software utilizate. Prioritățile, necesitățile și nivelul de acces la facilități hardware și software (inclusiv birotică și accesorii) și la facilitățile rețelei UNAGE Iași sunt stabilite individual sau colectiv (după caz, angajați sau studenți);

- Fiecare stație are atribuită o adresă IP prin care se identifică în rețea și se poate conecta la internet și la aplicațiile sau bazele de date de pe servere. Pe fiecare stație de lucru se instalează doar software cu licență sau freeware, open source, după caz. Este interzisă instalarea de către utilizatori a altor aplicații fără licență sau altele decât cele instalate de către membrii Serviciului Informatizare cât și stergerea sau modificarea adresei IP. De asemenea este interzisă stocarea și utilizarea pe stația de lucru de conținut ce încalcă legile dreptului de autor sau alte legi în vigoare. Fiecare utilizator își asumă în orice moment atât aplicațiile rulate cât și conținutul stocat pe stația lui de lucru;

- Nu este permisă schimbarea structurii hardware a stațiilor de lucru și nici deteriorarea intenționată sau prin manevrarea necorespunzătoare a echipamentelor primite în inventar sau altor echipamente apațînând infrastructurii informatice a universității;

- Accesul fiecărui utilizator la stația de lucru se face pe baza de user și parola individuală. Userul sau parola pot fi schimbate la cerere de către personalul IT. Aceste date trebuie știute doar de către utilizator;

- Modificarea datelor din aplicațiile cu acces online la bazele de date găzduite de serverele din rețeaua UNAGE Iași se face conform nivelului de acreditare pentru aplicația respectivă a fiecărui utilizator, cu acces tot pe bază de user și parolă, fiind asumată de utilizatorul respectiv;

- Este necesar ca fiecare utilizator să salveze periodic datelor sensibile, necesare, pe alte dispozitive decât stația de lucru: stick USB, HDD extern, mail etc., pentru a se evita pierderea lor în caz de avarie tehnică;

- Se recomandă scanarea antivirus a tuturor dispozitivelor externe introduse în porturile stației de lucru (stick USB, HDD extern, e-SATA etc.). De asemenea, se recomandă ca aceste dispozitive de stocare să nu mai fie folosite pe nicio altă stație de lucru, în vederea evitării infectării malware;

- Membrii serviciului informatizare nu își asumă trainingul utilizatorilor în vederea folosirii unor aplicații ce țin de specificul activității fiecăruia, conform fișei postului

  (aplicații Office, editare, grafică, prelucrare audio-video etc.).

- Studenții universității au acces la laboratoarele universității, ce utilizează tehnică de calcul, sub supravegherea cadrelor didactice sau laboranților și se pot loga la stațiile de lucru doar pe conturi de utilizator cu acces limitat (nu au privilegii de administrator, nu pot modifica setarile sistemului);

- Accesul la resursa de internet a universitții, fie că se face prin adresă IP fixă sau prin IP dinamic (WiFi), prin intermediul browserelor de

net, aplicațiilor de tip messenger, mail, cloud etc., se face conform legilor în vigoare și regulamentelor universității. Este interzisă accesarea de siteuri ori adrese cu conținut neadecvat sau care pot propaga atacuri malware, descărcarea de conținut care nu respectă legislația drepturilor de autor. Nu este permisă, de asemenea, utilizarea de aplicații ce au ca efect exploatarea în exces a rețelei de internet (flodarea) sau pentru atacuri malware ori de tip hacker asupra rețelei UNAGE Iași ori a altor rețele, browsing anonim etc. O parte dintre aceste interdicții și recomandări este cuprinsă și în prevederile 2703/05.07.2010 aprobat de conducerea universității.

- În cazul nerespectării acestor proceduri/recomandări, care sunt aduse la cunoștința utilizatorilor în momentul predării echipamentelor, se trece la identificarea utilizatorilor care le-au încălcat și apoi sesizarea conducerii universității sau, după caz, autorităților îndreptățite a aplica prevederile regulamentelor universității și legislației specifice în vigoare. De asemenea, se interzice accesul la rețea a utilizatorului respectiv până la clarificarea situației astfel create;

(11) Remedierea defecțiunilor tehnice ce pot apărea în rețeaua de internet

În rețeaua informatică a universității pot apărea defecțiuni tehnice sau avarii datorate defectării unor echipamente, ori utilizării necorespunzătoare de către utiluizatori a unor resurse hardware și software ale rețelei.

Una dintre cele mai importante avarii, care afectează procesul de lucru al colectivului universității și constituie prioritate spre rezolvare, o reprezintă întreruperea conexiunii de internet. Pentru remedierea acesteia se recomandă următoarele **proceduri**:

- **Identificarea tipului de defecțiune**
  - Se verifică accesul în exterior de pe serverele cu rol de router, DNS primar (pentru sediile din str. Costache Negruzzi) și secundar (sediul din str. Sărărie 189)
  - Dacă serverul nu are ieșire la internet se verifică cu un tester de

rețea sau cu alte mijloace specifice starea de funcționare a convertorului de fibră optică și a distribuitorului de fibră către rețeaua internă. Se mai verifică de asemenea, luând legătura cu centrul ROEDU (furnizorul serviciilor de internet pentru sistemul public de învățământ) din Iași, situat în incinta Univ. Al. I. Cuza, dacă nu există întreruperi ale semnalului în sistemul public (avarii, lucrări etc.). Tot în acest caz se verifică dacă sistemul de operare Linux nu a fost corupt din pricina unui update sau ca urmare a unui atac informatic;

- Dacă serverul tip router are ieșire la internet se verifică accesul din interiorul rețelelor interne către router. Apoi, prin excludere și deconectări succesive, se verifică elementele active de rețea (switchuri, routere WiFi) de pe fiecare etaj în parte, pentru a micșora aria de căutare a posibilei defecțiuni, până la identificarea acesteia;
- Aceleași proceduri se aplică și în cazul unui router internet dedicat de tip Cisco.

- **Remedierea defecțiunii**

În funcție de tipul defecțiunii identificate sunt de urmat o serie de proceduri intre care menționăm:

- Se așteaptă restabilirea semnalului internet în sistemul public, anunțând toate departamentele universității de existența întreruperii și timpul estimat împreună cu responsabilii ROEDU până la restabilirea semnalului;
- Înlocuirea convertorului sau a distribuitorului de fibră optică;
- Înlocuirea sau repararea eventualelor surse defecte de alimentare cu curent electric a echipamentelor de rețea;
- Reconfigurarea hardware/software (după caz) sau înlocuirea serverului Linux pentru internet sau a routerului Cisco dedicat;
- Înlocuirea switch-urilor sau routerelor WiFi identificate ca defecte în rețea sau reconfigurarea celor compromise din punct de vedere

software. După caz, se încearcă și identificarea împrejurărilor care au dus la compromiterea funcțională a routerelor configurabile;

- Verificarea cablajelor din patch panel, switch, router sau prize din rețeaua de calculatoare pentru a vedea dacă nu au fost reconectate necorespunzător (accidental sau intenționat);

- Urmărirea traficului în și dinspre rețeaua internă spre exterior, identificarea și izolarea stațiilor client cu trafic neobisnuit. Verificarea stațiilor de lucru sau serverelor din aria unde a fost identificată "sursa" întreruperii în rețea, pentru a stabili dacă prin acea stație s-a desfășurat un atac informatic cauzat fie de infectărea cu malware, fie de folosirea de către un utilizator a unor aplicații sau proceduri nepermise;

(12) Securizarea adreselor de email instituționale

Serviciul de Informatizare și Activități tipografice pune la dispoziția comunității academice serviciul de email folosit pentru comunicații membrii comunității academice. Utilizatorii unui cont de email se supun regulilor și procedurilor generale de securitate informatică:

- Accesul la email (client web-based) se realizează din pagina web principală a universității, www.arteiasi.ro . Se folosește protocolul de securitate destinat transferului de informație criptată, https, cu un certificat digital gratuit.

- Pe serverul de email este instalată o aplicație antivirus si anti-spam care verifică mesajele. Reprezentanții IT recomandă utilizatorilor să permită accesul mesajelor cu eticheta Spam dar să le direcționeze către un folder pentru a identifica eventuale mesaje "fals pozitive".

- Parola folosită trebuie să fie una puternică formată din minim 8 caractere să conțină litere majuscule, cifre sau/si caractere speciale;

- Parola este confidențială nu se destăinuie și nu se notează în calculator sau la vedere;

- Utilizatorii trebuie să fie conștienți de implicațiile folosirii unei parole neadecvate sau înscrierea acestei adrese pe diverse site-uri, altele decat cele în scopuri academice.
- Utilizatorii pot obține lămuriri de la reprezentanții IT ai Universității dacă sunt ambiguități în privința unui email receptionat chiar si de la persoane cunoscute, pentru a evita atacuri tip phishing sau infectări locale ori în rețea.

Toate aceste reguli și preocupări tehnice, în vederea asigurării protecției cibernetice a datelor cu caracter personal, sunt detaliate în Strategia de securitate IT (nr. 1362/28.05.2015), Politici în domeniul IT (1363/28.05.2015), Registrul riscurilor, Planul de continuitate al activității și o serie de Proceduri operaționale cum ar fi: Procedură operațională de utilizare a stațiilor de lucru șia rețelei de internet, Procedură operațională de securizare și monitorizare a serverelor, Procedură operațională de utilizare a UMS, Procedură operațională de utilizare a programului de contabilitate Premier, Procedură operațională de utilizare a aplicației Liberty, Procedură operațională de utilizare a dispozitivelor mobile în rețeaua universității, elaborate de către membrii Serviciului de Informatizare și Activități tipografice și auditate în anul 2015. De asemenea, gradul de implementare hardware și software a acestor măsuri este reflectat în rapoartele anuale ale serviciului.

IV. NOTIFICAREA AUTORITATII DE SUPRAVEGHERE

(1) În cazul în care are loc o încălcare a securității datelor cu caracter personal, UNAGE Iași notifică acest lucru autorității de supraveghere fără întârzieri nejustificate și în termen de cel mult 72 de ore de la data la care a luat cunoștință de aceasta . În cazul în care notificarea nu are loc în termen de 72 de ore, aceasta este însoțită de o explicație motivată din partea universitatii.

(2) Notificarea menționată la alineatul (1) cel puțin:

(a) descrie caracterul încălcării securității datelor, inclusiv, acolo unde este posibil, categoriile și numărul aproximativ al persoanelor vizate în cauză, precum și categoriile și numărul aproximativ al înregistrărilor de date cu caracter personal în cauză;

(b) comunică numele și datele de contact ale responsabilului cu protecția datelor sau un alt punct de contact de unde se pot obține mai multe informații;

(c) descrie consecințele probabile ale încălcării securității datelor cu caracter personal;

(d) descrie măsurile luate sau propuse spre a fi luate pentru a remedia problema încălcării securității datelor, inclusiv, după caz, măsurile pentru atenuarea eventualelor sale efecte negative.

(3) Atunci când și în măsura în care nu este posibil să se furnizeze informațiile în același timp, acestea pot fi furnizate în mai multe etape, fără întârzieri nejustificate.

(4) Universitatea va păstra documente referitoare la toate cazurile de încălcare a securității datelor cu caracter personal, care cuprind o descriere a situației de fapt în care a avut loc încălcarea securității datelor cu caracter personal, a efectelor acesteia și a măsurilor de remediere întreprinse. Această documentație permite autorității de supraveghere să verifice conformitatea cu prezentul articol.

V. INFORMAREA PERSOANEI VIZATE PRIVIND INCALCAREA SECURITATII DATELOR

(1) În cazul în care încălcarea securității datelor cu caracter personal este susceptibilă să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice, UNAGE Iași va informa persoana vizată fără întârzieri nejustificate cu privire la această încălcare.

(2) În informarea se include o descriere într-un limbaj clar și simplu a caracterului încălcării securității datelor cu caracter personal, masurile luate si efectele produse de incalcarea securitatii datelor.

(3) Informarea nu este necesară în cazul în care oricare dintre următoarele condiții este îndeplinită:

(a) universitatea a implementat măsuri de protecție tehnice și organizatorice adecvate, iar aceste măsuri au fost aplicate în cazul datelor cu caracter personal afectate de încălcarea securității datelor cu caracter personal, în special măsuri prin care se asigură că datele cu caracter personal devin neinteligibile oricărei persoane care nu este autorizată să le acceseze, cum ar fi criptarea;

(b) universitatea a luat măsuri ulterioare prin care se asigură că riscul ridicat pentru drepturile și libertățile persoanelor vizate menționat la

alineatul (1) nu mai este susceptibil să se materializeze;

(c) ar necesita un efort disproporționat. În această situație, se efectuează în loc o informare publică sau se ia o măsură similară prin care persoanele vizate sunt informate într-un mod la fel de eficace.

VI. EVALUAREA IMPACTULUI ASUPRA PROTECȚIEI DATELOR ȘI CONSULTAREA PREALABILĂ

Art.19. Evaluarea impactului asupra protecției datelor

(1) În cazul în care un tip de prelucrare, în special cel bazat pe utilizarea noilor tehnologii, este susceptibil să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice, UNAGE Iași va efectua, înaintea prelucrării, o evaluare a impactului respectivelor operațiuni de prelucrare asupra protecției datelor cu caracter personal. O evaluare unică poate aborda un set de operațiuni de prelucrare similare care prezintă riscuri ridicate similare.

(2) La realizarea unei astfel de evaluări universitatea va solicita avizul responsabilului cu protecția datelor.

(3) Evaluarea menționată la alineatul (1) se impune mai ales în cazul:

(a) unei evaluări sistematice și cuprinzătoare a aspectelor personale referitoare la persoane fizice, care se bazează pe prelucrarea automată, inclusiv crearea de profiluri, și care stă la baza unor decizii care produc efecte juridice privind persoana fizică sau care o afectează în mod similar într-o măsură semnificativă;

(b) prelucrării pe scară largă a unor categorii speciale de date (rasa, etnie, orientare politica, religioasa, convingeri filosofice, apartenenta la sindicate, date genetice, biometrice ori privind sanatatea sau orienatarea/viata sexuala), sau a unor date cu caracter personal privind condamnări penale și infracțiuni;

(c) unei monitorizări sistematice pe scară largă a unei zone accesibile publicului.

(4) Evaluarea conține cel puțin:

(a) o descriere sistematică a operațiunilor de prelucrare preconizate și a scopurilor prelucrării, inclusiv, după caz, interesul legitim urmărit de universitate;

(b) o evaluare a necesității și proporționalității operațiunilor de prelucrare

în legătură cu aceste scopuri;

(c) o evaluare a riscurilor pentru drepturile și libertățile persoanelor vizate menționate la alineatul (1);

(d) măsurile preconizate în vederea abordării riscurilor, inclusiv garanțiile, măsurile de securitate și mecanismele menite să asigure protecția datelor cu caracter personal și să demonstreze conformitatea cu dispozițiile prezentului regulament, luând în considerare drepturile și interesele legitime ale persoanelor vizate și ale altor persoane interesate.

(5) Universitatea solicită, acolo unde este cazul, avizul persoanelor vizate sau al reprezentanților acestora privind prelucrarea prevăzută, fără a aduce atingere protecției intereselor comerciale sau publice ori securității operațiunilor de prelucrare.

(11) Acolo unde este necesar, universitatea efectuează o analiză pentru a evalua dacă prelucrarea are loc în conformitate cu evaluarea, cel puțin atunci când are loc o modificare a riscului reprezentat de operațiunile de prelucrare.

Art.20. Consultarea prealabilă

(1) Universitatea va consulta autoritatea de supraveghere înainte de prelucrarea atunci când evaluarea impactului asupra protecției datelor indică faptul că prelucrarea ar genera un risc ridicat în absența unor măsuri luate pentru atenuarea riscului.

(2) Atunci când consideră că prelucrarea prevăzută menționată la alineatul (1) ar încălca prezentul regulament, în special atunci când riscul nu a fost identificat sau atenuat într-o măsură suficientă de către operator, autoritatea de supraveghere oferă consiliere în scris în cel mult opt săptămâni de la primirea cererii de consultare. Această perioadă poate fi prelungită cu șase săptămâni, ținându-se seama de complexitatea prelucrării prevăzute.

(3) Atunci când consultă autoritatea de supraveghere în conformitate cu alineatul (1), universitatea îi furnizează acesteia:

(a) dacă este cazul, responsabilitățile respective ale universitatii ;

(b) scopurile și mijloacele prelucrării preconizate;

(c) măsurile și garanțiile prevăzute pentru protecția drepturilor și libertăților persoanelor vizate, în conformitate cu prezentul regulament;

(d) datele de contact ale responsabilului cu protecția datelor;

(e) evaluarea impactului asupra protecției datelor ;

(f) orice alte informații solicitate de autoritatea de supraveghere.

VII. RESPONSABILUL CU PROTECȚIA DATELOR

Art.21. Desemnarea responsabilului cu protecția datelor

(1) Responsabilul cu protecția datelor este desemnat pe baza calităților profesionale și, în special, a cunoștințelor de specialitate în dreptul și practicile din domeniul protecției datelor, precum și pe baza capacității de a îndeplini sarcinile specific acestei functii.

(6) Responsabilul cu protecția datelor poate fi un membru al personalului universitatii sau poate să își îndeplinească sarcinile în baza unui contract de servicii.

(7) Universitatea publică datele de contact ale responsabilului cu protecția datelor și le comunică autorității de supraveghere.

Art.22. Funcția responsabilului cu protecția datelor

(1) Universitatea se asigură că responsabilul cu protecția datelor este implicat în mod corespunzător și în timp util în toate aspectele legate de protecția datelor cu caracter personal.

(2) Universitatea sprijină responsabilul cu protecția datelor în îndeplinirea sarcinilor sale specifice, asigurându-i resursele necesare pentru executarea acestora, precum și accesarea datelor cu caracter personal și a operațiunilor de prelucrare, și pentru menținerea cunoștințelor sale de specialitate.

(3) Universitatea se asigură că responsabilul cu protecția datelor nu primește niciun fel de instrucțiuni în ceea ce privește îndeplinirea acestor sarcini. Acesta nu este demis sau sanctionat pentru îndeplinirea sarcinilor sale. Responsabilul cu protecția datelor răspunde direct în fața celui mai înalt nivel al conducerii universității.

(4) Persoanele vizate pot contacta responsabilul cu protecția datelor cu privire la toate chestiunile legate de prelucrarea datelor lor și la exercitarea drepturilor lor în temeiul prezentului regulament.

(5) Responsabilul cu protecția datelor are obligația de a respecta secretul sau confidențialitatea în ceea ce privește îndeplinirea sarcinilor sale, în conformitate cu dreptul UE sau cu dreptul intern.

(6) Responsabilul cu protecția datelor poate îndeplini și alte sarcini și atribuții. Universitatea se asigură că niciuna dintre aceste sarcini și atribuții

nu generează un conflict de interese.

Art.23. Sarcinile responsabilului cu protecția datelor

(1) Responsabilul cu protecția datelor are cel puțin următoarele sarcini:

(a) informarea și consilierea conducerii universității, precum și a angajaților care se ocupă de prelucrare cu privire la obligațiile care le revin în temeiul prezentului regulament și al altor dispoziții de drept al UE sau drept intern referitoare la protecția datelor;

(b) monitorizarea respectării prezentului regulament, a altor dispoziții de drept al UE sau de drept intern referitoare la protecția datelor și a politicilor universității în ceea ce privește protecția datelor cu caracter personal, inclusiv alocarea responsabilităților și acțiunile de sensibilizare și de formare a personalului implicat în operațiunile de prelucrare, precum și auditurile aferente;

(c) furnizarea de consiliere la cerere în ceea ce privește evaluarea impactului asupra protecției datelor și monitorizarea funcționării acesteia;

(d) cooperarea cu autoritatea de supraveghere;

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

(2) În îndeplinirea sarcinilor sale, responsabilul cu protecția datelor ține seama în mod corespunzător de riscul asociat operațiunilor de prelucrare, luând în considerare natura, domeniul de aplicare, contextul și scopurile prelucrării.

VIII. DISPOZIȚII FINALE

(1) Dispozițiile prezentului regulament se completează cu cele ale RGPD 2016/679 al Parlamentului European și Consiliului, precum și cu cele ale Legii 102/2005 republicată privind înființarea, organizarea și funcționarea A.N.S.P.D.C.P. și de abrogare a Legii 677/2001.

(2) Prezentul regulament intra în vigoare la data publicării sale pe site-ul UNAGE Iași, devenind obligatoriu pentru întreg personalul universității .