MINISTERUL EDUCAȚIEI NAȚIONALE
UNIVERSITATEA „1 DECEMBRIE 1918” DIN ALBA IULIA
SENATUL UNIVERSITĂȚII

REGULAMENTUL PRIVIND PROTECȚIA PERSOANELOR FIZICE ÎN CEEA CE PRIVEȘTE PRELUCRAREA DATELOR CU CARACTER PERSONAL ȘI PRIVIND LIBERA CIRCULAȚIE A ACESTOR DATE, APLICABIL ÎN CADRUL UNIVERSITĂȚII „1 DECEMBRIE 1918” DIN ALBA IULIA

UNIVERSITATEA „1 DECEMBRIE 1918” DIN ALBA IULIA	**COD: R-SFDA-27**	**Ediția: 1**
	Regulamentul privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date, aplicabil în cadrul Universității „1 Decembrie 1918” din Alba Iulia	**Revizia: 1**
		Aprobat SENAT Data: 20.02.2019

	Nume și prenume	**Funcția**	**Data**	**Semnătura**
ELABORAT	Rotar Claudia	Responsabil protecția datelor	14.02.2019	
AVIZAT	Hurbean Ada	Președinte Comisia juridică	19.02.2019	

INDICATORUL APROBĂRILOR ȘI AL REVIZIILOR

Nr. crt.	**Ediția**	**Revizia**	**Data aprobării în Senat**
1.	1	0	24.05.2018
2.	1	1	20.02.2019

Capitolul I. DISPOZIȚII GENERALE

Art. 1. (1) Prezentul regulament are ca scop stabilirea unor norme privind prelucrarea datelor cu caracter personal de către Universitatea „1 Decembrie 1918" din Alba Iulia, denumită în continuare UAB, în calitatea de Operator.

(2) Prezentul regulament stabilește exercitarea drepturilor și obligațiilor pe care UAB le are cu privire la protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date, în relațiile instituției cu persoanele vizate, autoritățile statului, furnizorii implicați în mod direct/indirect, bănci, instanțe judecătorești sau arbitrale, notari publici, avocați, executori judecătorești, alte servicii autorizate, experți evaluator, alte instituții de învățământ.

(3) Normele cuprinse în prezentul regulament nu aduc atingere altor obligații legale imperative sau deontologice ce revin UAB.

Capitolul II. CADRUL LEGAL

Art. 2. În vederea elaborării prezentului Regulament, aplicabil în cadrul Universității „1 Decembrie 1918" din Alba Iulia, s-a avut în vedere Regulamentul (UE) 679/2016, 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).

Capitolul III. TERMENI ȘI ABREVIERI

Art. 3. (1) Termenii folosiți în cadrul prezentului regulament au următorul sens:

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;

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, UAB 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 UAB;

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, UAB, persoana împuternicită de operator și persoanele care, sub directa autoritate a UAB 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;

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;

Capitolul IV. PRINCIPIILE ȘI CADRUL INSTITUȚIONAL PRIVIND PRELUCRAREA DATELOR CU CARACTER PERSONAL DE CĂTRE UAB

Art. 4. Principii

1. **Legalitate, echitate și transparență** – un principiu esențial, strâns asociat cu drepturile fundamentale ale omului. Datele cu caracter personal trebuie să fie prelucrate „*în mod legal, echitabil și transparent față de persoana vizată*.”;

2. **Limitări legate de scop – datele personale trebuie să fie colectate în scopuri bine determinate, explicite și legitime, iar prelucrările ulterioare nu trebuie să se abată de la aceste scopuri.** Prelucrarea ulterioara în scopuri de arhivare în interes public, în scopuri de cercetare științifică/ istorică ori în scopuri statistice nu se consideră incompatibilă de la scopurile inițiale;

3. **Minimizarea/Reducerea la minimum a datelor** – orice colectare de date personale trebuie foarte bine analizată înainte de obținerea efectivă a datelor, care trebuie să fie **cele mai adecvate, relevante și strict limitate** la ceea ce este absolut necesar pentru scopurile în care sunt prelucrate;

4. **Exactitatea informațiilor** – datele cu caracter personal trebuie să fie exacte, și, în cazul în care este necesar, trebuie sa fie actualizate; operatorii trebuie să ia toate măsurile pentru a se asigura că datele cu caracter personal care sunt inexacte, având în vedere scopurile pentru care sunt prelucrate, sunt șterse sau rectificate fără întârziere;

5. **Limitarea stocării** – datele trebuie păstrate fix atât timp cat sunt necesare pentru prelucrarea asumată. Perioadele mai lungi de stocare sunt excepții asociate cu activități de prelucrare în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice, conform art. 89, alin. 1 din GDPR, sub rezerva punerii în aplicare a măsurilor tehnice și organizatorice adecvate prevăzute de GDPR în vederea garantării drepturilor și libertăților persoanei vizate;

6. **Integritate și confidențialitate** – prelucrarea datelor personale trebuie făcută în cele mai adecvate condiții de siguranță, care să includă „protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luarea de măsuri tehnice sau organizatorice corespunzătoare".

Nerespectarea acestui principiu expune direct la breșe de securitate și confidențialitate și, implicit, la penalitățile extrem de severe prevăzute de GDPR;

7. **Responsabilitate – Operatorul este responsabil de respectarea principiilor GDPR și de a demonstra această respectare.** GDPR impune nu numai respectarea principiilor GDPR – de exemplu, prin documentarea deciziilor luate cu privire la o activitate de procesare, ci și să se demonstreze oricând aceasta respectare (responsabilitate).

În consecință:

- Orice prelucrare de date cu caracter personal trebuie să fie legală și echitabilă;
- Ar trebui să fie transparent pentru persoanele fizice vizate că sunt colectate, utilizate, consultate sau prelucrate datele cu caracter personal care le privesc și în ce măsură datele sunt sau vor fi prelucrate;
- Principiul transparenței prevede că orice informații și comunicări referitoare la prelucrarea respectivelor date cu caracter personal trebuie să fie ușor accesibile și ușor de înțeles și că trebuie să se utilizeze un limbaj simplu și clar; acest principiu se referă în special la informarea persoanei vizate privind identitatea operatorului și scopurile prelucrării, precum și la oferirea de informații suplimentare, pentru a asigura o prelucrare echitabilă și transparentă în ceea ce privește persoanele fizice vizate și dreptul acestora de a li se confirma și comunica datele cu caracter personal care sunt prelucrate;
- Persoanele fizice trebuie informate cu privire la riscurile, normele, garanțiile și drepturile în materie de prelucrare a datelor cu caracter personal și cu privire la modul în care să își exercite drepturile în legătură cu prelucrarea;
- Scopurile specifice în care datele cu caracter personal sunt prelucrate trebuie să fie explicite și legitime și să fie determinate la momentul colectării datelor respective;
- Datele cu caracter personal trebuie să fie adecvate, relevante și limitate la ceea ce este necesar pentru scopurile în care sunt prelucrate. Aceasta necesită, în special, asigurarea faptului că perioada pentru care datele cu caracter personal sunt stocate este limitată strict la minimum;

- Datele cu caracter personal ar trebui prelucrate doar dacă scopul prelucrării nu poate fi îndeplinit în mod rezonabil prin alte mijloace;
- Operatorul trebuie să stabilească termene pentru ștergere sau revizuirea periodică. Operatorul trebuie să ia toate măsurile rezonabile pentru a se asigura că datele cu caracter personal care sunt inexacte sunt rectificate sau șterse;
- Datele personale trebuie prelucrate într-un mod care să asigure în mod adecvat securitatea și confidenţialitatea, inclusiv în scopul prevenirii accesului neautorizat la acestea sau utilizarea neautorizată a datelor cu caracter personal și a echipamentului utilizat pentru prelucrare.

Capitolul V. RESPONSABILITATEA

Art. 5 (1) UAB utilizează datele cu caracter personal ale persoanelor vizate prin intermediul unor baze de date alcătuite din informații obținute direct de la persoanele vizate, alte date personale pentru care persoana vizată și-a dat consimțământul și informații furnizate de orice sursă externă autorizată de lege.

(2) UAB în calitate de Operator este responsabilă pentru datele cu caracter personal menționate la alin. 1, aflate sub controlul său, precum și pentru datele transferate către terți.

Capitolul VI. LEGALITATEA PRELUCRĂRII

Art. 6 Prelucrarea este legală 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 cu caracter personal pentru unul sau mai multe scopuri specifice*;

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

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

(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 UAB*;

(f) *prelucrarea este necesară în scopul intereselor legitime urmărite de operator 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. Litera (f) din primul paragraf nu se aplică în cazul prelucrării efectuate de autorități publice în îndeplinirea atribuțiilor lor*.

Capitolul VII. CONSIMȚĂMÂNTUL

Art. 7 (1) În cazul în care prelucrarea se bazează pe consimțământ, UAB trebuie să fie în măsură să demonstreze că persoana vizată și-a dat consimțământul pentru prelucrarea datelor sale cu caracter personal.

(2) Persoana vizată are dreptul să își retragă în orice moment consimțământul. Retragerea consimțământului nu afectează legalitatea prelucrării efectuate pe baza consimțământului înainte de retragerea acestuia. Înainte de acordarea consimțământului, persoana vizată este informată cu privire la acest lucru. Retragerea consimțământului se face la fel de simplu ca acordarea acestuia.

(3) Daca prelucrarea datelor personale se bazează pe consimțământ, prelucrarea datelor unui copil este legală dacă acesta are cel puțin vârsta de 16 ani. Dacă copilul are sub vârsta de 16 ani, respectiva prelucrare este legală numai dacă și în măsura în care consimțământul respectiv este acordat sau autorizat de titularul răspunderii părintești asupra copilului. UAB depune toate eforturile rezonabile pentru a verifica în astfel de cazuri dacă titularul răspunderii părintești a acordat sau a autorizat consimțământul, ținând seama de tehnologiile disponibile.

Capitolul VIII. REGULI SPECIALE PRIVIND PRELUCRAREA DATELOR CU CARACTER PERSONAL

Art. 8. Prelucrarea unor categorii speciale de date cu caracter personal

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

(2) **Prevederile anterioare nu se aplica în următoarele situații:**

a) când persoana vizată și-a dat consimțământul explicit pentru prelucrarea acestor date cu caracter personal pentru unul sau mai multe scopuri specifice, cu excepția cazului în care dreptul Uniunii sau dreptul intern prevede că interdicția prevăzută anterior să nu poată fi ridicată prin consimțământul persoanei vizate;

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

c) când prelucrarea este necesară pentru protejarea intereselor vitale ale persoanei vizate sau ale unei alte persoane fizice, atunci când persoana vizată se află în incapacitate fizică sau juridică de a-și da consimțământul;

d) când prelucrarea este efectuată în cadrul activităților lor legitime și cu garanții adecvate de către o fundație, o asociație sau orice alt organism fără scop lucrativ și cu specific politic, filozofic, religios sau sindical, cu condiția ca prelucrarea să se refere numai la membrii sau la foștii membri ai organismului respectiv sau la persoane cu care acesta are contacte permanente în legătură cu scopurile sale și că datele cu caracter personal să nu fie comunicate terților fără consimțământul persoanelor vizate;

e) când prelucrarea se referă la date cu caracter personal care sunt făcute publice în mod manifest de către persoana vizată;

f) când prelucrarea este necesară pentru constatarea, exercitarea sau apărarea unui drept în instanță sau ori de câte ori instanțele acționează în exercițiul funcției lor judiciare;

g) când prelucrarea este necesara din motive de interes public major, în baza dreptului Uniunii sau a dreptului intern, care este proporțional cu obiectivul urmărit, respectă esența dreptului la protecția datelor și prevede măsuri corespunzătoare și specifice pentru protejarea drepturilor fundamentale și a intereselor persoanei vizate;

h) când prelucrarea este necesară în scopuri legate de medicina preventivă sau a muncii, de evaluarea capacității de muncă a angajatului, de stabilirea unui diagnostic medical, de furnizarea de asistență medicală sau socială sau a unui tratament medical sau de gestionarea sistemelor și serviciilor de sănătate sau de asistență socială, în temeiul dreptului Uniunii sau al dreptului intern sau în temeiul unui contract încheiat cu un cadru medical și sub rezerva respectării condițiilor și garanțiilor prevăzute de lege; datele cu caracter personal pot fi prelucrate în scopurile menționate anterior în cazul în care datele respective sunt prelucrate de către un profesionist supus obligației de păstrare a secretului profesional sau sub responsabilitatea acestuia, în temeiul dreptului Uniunii sau al dreptului intern sau în temeiul normelor stabilite de organisme naționale competente sau de o altă persoană supusă, de asemenea, unei obligații de confidențialitate în temeiul dreptului Uniunii sau al dreptului intern ori al normelor stabilite de organisme naționale competente.

i) când prelucrarea este necesară din motive de interes public în domeniul sănătății publice, cum ar fi protecția împotriva amenințărilor transfrontaliere grave la adresa sănătății sau asigurarea de standarde ridicate de calitate și siguranță a asistenței medicale și a medicamentelor sau a dispozitivelor medicale, în temeiul dreptului Uniunii sau al dreptului intern, care prevede măsuri adecvate și specifice pentru protejarea drepturilor și libertăților persoanei vizate, în special a secretului profesional; sau

j) când prelucrarea este necesară în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice, în baza dreptului Uniunii sau a dreptului intern, care este proporțional cu obiectivul urmărit, respectă esența dreptului la protecția datelor și prevede măsuri corespunzătoare și specifice pentru protejarea drepturilor fundamentale și a intereselor persoanei vizate.

(3) **Prelucrarea datelor cu caracter personal cu funcție de identificare generală**

Datele cu caracter personal cu funcție de identificare generală (Codul numeric personal - CNP, seria și numărul actului de identitate/pașaportului etc.) vor fi prelucrate, exclusiv în situațiile în care este necesară stabilirea identității persoanelor vizate și prelucrarea este prevăzută în mod expres de o dispoziție legală.

(4) **Prelucrarea datelor cu caracter personal referitoare la condamnări penale și infracțiuni**

Prelucrarea de date cu caracter personal referitoare la condamnări penale și infracțiuni sau la masuri de securitate conexe se efectuează numai sub controlul unei autorități de stat sau atunci când prelucrarea este autorizată de dreptul Uniunii sau de legislația națională care prevede garanții adecvate pentru drepturile și libertățile persoanelor vizate. Orice registru cuprinzător al condamnărilor penale se tine numai sub controlul unei autorități de stat.

(5) **Prelucrarea care nu necesită identificarea**

În cazul în care scopurile pentru care UAB prelucrează date cu caracter personal nu necesită sau nu mai necesită identificarea unei persoane vizate de către operator, operatorul nu are obligația de a păstra, obține sau prelucra informații suplimentare pentru a identifica persoana vizata în scopul unic al respectării legislației specifice.

Dacă, în cazurile menționate anterior, operatorul poate demonstra ca nu este în măsură să identifice persoana vizata, operatorul informează persoana vizată în mod corespunzător, în cazul în care este posibil. În astfel de cazuri, prevederile legale privind dreptul de acces, de rectificare, de ștergere, la restricționarea prelucrării, dreptul la portabilitatea datelor nu se aplica, cu excepția cazului în care persoana vizată, în scopul exercitării drepturilor sale menționate anterior, oferă informații suplimentare care permit identificarea sa.

(6) **Prelucrarea datelor cu caracter personal prin mijloace de supraveghere video**

UAB, prin intermediul sistemelor de supraveghere video, prelucrează datele cu caracter personal, respectiv imaginea și alte informații ce permit identificarea persoanelor vizate.

Imaginile referitoare la persoane identificate sau identificabile, prelucrate prin mijloace de supraveghere video, constituie date cu caracter personal:

a) chiar dacă nu sunt asociate cu datele de identificare ale persoanei sau

b) chiar daca nu conțin imaginea persoanei filmate, ci alte informații de natură să conducă la identificarea acesteia (ex: numărul de înmatriculare al vehiculului)

Scopul prelucrării datelor personale consta în: securitatea persoanelor, spațiilor și/sau bunurilor private, prevenirea și combaterea infracțiunilor, îndeplinirea obligațiilor legale și realizarea intereselor legitime.

Prelucrarea datelor cu caracter personal prin mijloace de supraveghere video se realizează numai de către persoane autorizate de UAB.

Informațiile înregistrate sunt destinate utilizării de către UAB și pot fi comunicate numai următorilor destinatari: persoana vizată, reprezentanții legali/împuterniciții persoanei vizate,

reprezentanții autorizați UAB, organele de urmărire/cercetare penală, instanțe judecătorești, în conformitate cu prevederile legislației interne și comunitare aplicabile activității desfășurate de **UAB**.

Durata de stocare a datelor obținute prin intermediul sistemului de supraveghere video este de 30 de zile, cu excepția situațiilor expres reglementate de lege sau a cazurilor temeinic justificate. La expirarea termenului înregistrările se distrug sau se șterg.

Persoanele vizate, respectiv angajații, clienții/potențialii clienți, vizitatorii și alte persoane care intră în imobilele UAB sunt informate în legătură cu prelucrarea datelor personale prin intermediul sistemelor de supraveghere video.

Informările în cauză, precum și indicatoarele de marcare a existentei sistemului de supraveghere video vor fi aplicate în locurile unde sunt amplasate camere de supraveghere video. Personalul de pază din cadrul Direcției Administrativă va verifica periodic starea fizică a informărilor și a indicatoarelor anterior menționate și va răspunde de siguranța și confidențialitatea datelor personale stocate în sistemul de supraveghere/monitorizare video.

Capitolul IX. RESPONSABILUL CU PROTECȚIA DATELOR

Art. 9. **Desemnarea responsabilului cu protecția datelor**

a. Operatorul și persoana împuternicită de operator desemnează un responsabil cu protecția datelor.

b. 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 prevăzute la articolul 10.

c. Operatorul și persoana împuternicită de operator 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 sancționat de către operator sau de persoana împuternicită de operator pentru îndeplinirea sarcinilor sale. Responsabilul cu protecția datelor răspunde direct în fața celui mai înalt nivel al conducerii operatorului sau persoanei împuternicite de operator.

d. 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.

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

f. Responsabilul cu protecția datelor poate îndeplini și alte sarcini și atribuții. Operatorul sau persoana împuternicită de operator se asigură că niciuna dintre aceste sarcini și atribuții nu generează un conflict de interese.

Art. 10. **Sarcinile responsabilului cu protecția datelor**

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

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

(b) monitorizarea respectării prezentului regulament, a altor dispoziții de drept al Uniunii sau de drept intern referitoare la protecția datelor și a politicilor operatorului sau ale persoanei împuternicite de operator în ceea ce privește protecția datelor cu caracter personal, inclusiv alocarea responsabilităților și 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.

Capitolul X. TRANSPARENȚA INFORMAȚIILOR, A COMUNICĂRILOR ȘI A MODALITĂȚILOR DE EXERCITARE A DREPTURILOR PERSOANEI VIZATE

Art. 11. (1) UAB ia măsuri adecvate pentru a furniza persoanei vizate orice informații și orice comunicări referitoare la prelucrare, într-o formă concisă, transparentă, inteligibilă și ușor accesibilă, utilizând un limbaj clar și simplu, în special pentru orice informații adresate în mod specific unui copil. 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.

(2) UAB furnizează persoanei vizate informații privind acțiunile întreprinse în urma unei cereri fără întârzieri nejustificate și în orice caz în cel mult o lună de la primirea cererii. Această perioadă poate fi prelungită cu două luni atunci când este necesar, ținându-se seama de complexitatea și numărul cererilor. UAB informează persoana vizată cu privire la orice astfel de prelungire, în termen de o lună de la primirea cererii, prezentând și motivele întârzierii. În cazul în care persoana vizată introduce o cerere în format electronic, informațiile sunt furnizate în format electronic acolo unde este posibil, cu excepția cazului în care persoana vizată solicită un alt format.

(3) Dacă nu ia măsuri cu privire la cererea persoanei vizate, UAB informează persoana vizată, fără întârziere și în termen de cel mult o lună de la primirea cererii, cu privire la motivele pentru care nu ia măsuri și la posibilitatea de a depune o plângere în fața unei autorități de supraveghere și de a introduce o cale de atac judiciară.

(4) Informațiile furnizate în temeiul articolelor 13 și 14 din Regulament și orice comunicare și orice măsuri luate în temeiul articolelor 15-22 și 34 din Regulament sunt oferite gratuit. În cazul în care cererile din partea unei persoane vizate sunt în mod vădit nefondate sau excesive, în special din cauza caracterului lor repetitiv, UAB poate:

(a) fie să perceapă o taxă rezonabilă ținând cont de costurile administrative pentru furnizarea informațiilor sau a comunicării sau pentru luarea măsurilor solicitate;

(b) fie să refuze să dea curs cererii. În aceste cazuri, UAB îi revine sarcina de a demonstra caracterul vădit nefondat sau excesiv al cererii.

Capitolul XI. INFORMAȚII CARE SE FURNIZEAZĂ ÎN CAZUL ÎN CARE DATELE CU CARACTER PERSONAL SUNT COLECTATE DE LA PERSOANA VIZATĂ

Art. 12. (1) În cazul în care datele cu caracter personal referitoare la o persoană vizată sunt colectate de la aceasta, UAB, în momentul obținerii acestor date cu caracter personal, furnizează persoanei vizate toate informațiile următoare:

(a) identitatea și datele de contact ale UAB 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) în cazul în care prelucrarea se face în temeiul articolului 6 alineatul (1) litera (f), din Regulament interesele legitime urmărite de operator sau de o parte terță;

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

(f) dacă este cazul, intenția UAB de a transfera date cu caracter personal către o țară terță sau o organizație internațională

(2) În plus față de informațiile menționate la alineatul (1), în momentul în care datele cu caracter personal sunt obținute, UAB furnizează persoanei vizate următoarele informații suplimentare necesare pentru a asigura o prelucrare echitabilă și transparentă:

(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 UAB, 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) atunci când prelucrarea se bazează pe consimțământ, 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) dacă furnizarea de date cu caracter personal 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 cu caracter personal și care sunt eventualele consecințe ale nerespectării acestei obligații;

(f) existența unui proces decizional automatizat incluzând crearea de profiluri,

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

Capitolul XII. DREPTURILE PERSOANELOR VIZATE

Art. 13. Dreptul de acces al persoanei vizate

Persoana vizată are dreptul de a obține din partea UAB o confirmare că se prelucrează sau nu date cu caracter personal care o privesc și, în caz afirmativ, acces la datele respective și la următoarele informații:

(a) scopurile prelucrării;

(b) categoriile de date cu caracter personal vizate;

(c) destinatarii sau categoriile de destinatari cărora datele cu caracter personal le-au fost sau urmează să le fie divulgate, în special destinatari din țări terțe sau organizații internaționale;

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

(e) existența dreptului de a solicita UAB rectificarea sau ștergerea datelor cu caracter personal ori restricționarea prelucrării datelor cu caracter personal referitoare la persoana vizată sau a dreptului de a se opune prelucrării;

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

(g) în cazul în care datele cu caracter personal nu sunt colectate de la persoana vizată, orice informații disponibile privind sursa acestora;

(h) existența unui proces decizional automatizat incluzând crearea de profiluri.

Art. 14. Rectificare și ștergere

Dreptul la rectificare Persoana vizată are dreptul de a obține de la operator, fără întârzieri nejustificate, rectificarea datelor cu caracter personal inexacte care o privesc. Ținându-se seama de scopurile în care au fost prelucrate datele, persoana vizată are dreptul de a obține completarea datelor cu caracter personal care sunt incomplete, inclusiv prin furnizarea unei declarații suplimentare.

Dreptul la ștergerea datelor („dreptul de a fi uitat") (1) Persoana vizată are dreptul de a obține din partea UAB ștergerea datelor cu caracter personal care o privesc, fără întârzieri nejustificate, iar UAB are obligația de a șterge datele cu caracter personal fără întârzieri nejustificate în cazul în care se aplică unul dintre următoarele motive:

(a) datele cu caracter personal nu mai sunt necesare pentru îndeplinirea scopurilor pentru care au fost colectate sau prelucrate

(b) persoana vizată își retrage consimțământul pe baza căruia are loc prelucrarea

(c) persoana vizată se opune prelucrării

(d) datele cu caracter personal au fost prelucrate ilegal;

(e) datele cu caracter personal trebuie șterse pentru respectarea unei obligații legale care revine UAB în temeiul dreptului Uniunii sau al dreptului intern sub incidența căruia se află UAB;

(f) datele cu caracter personal au fost colectate în legătură cu oferirea de servicii ale societății informaționale menționate la articolul 8 alineatul (1) din Regulamentul UE.

Art. 15. Dreptul la restricționarea prelucrării

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

(a) persoana vizată contestă exactitatea datelor, pentru o perioadă care îi permite UAB 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) UAB 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; sau

(d) persoana vizată s-a opus prelucrării în conformitate cu articolul 21 alineatul (1) din Regulamentul UE, pentru intervalul de timp în care se verifică dacă drepturile legitime ale UAB prevalează asupra celor ale persoanei vizate.

Art. 16. Obligația de notificare privind rectificarea sau ștergerea datelor cu caracter personal sau restricționarea prelucrării

UAB 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 cu excepția cazului în care acest lucru se dovedește imposibil sau presupune eforturi disproporționate. UAB informează persoana vizată cu privire la destinatarii respectivi dacă persoana vizată solicită acest lucru.

Art. 17. 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 UAB într-un format structurat, utilizat în mod curent și care poate fi citit automat și are dreptul de a transmite aceste date altui operator, fără obstacole din partea UAB căruia i-au fost furnizate datele cu caracter personal, în cazul în care:

(a) prelucrarea se bazează pe consimțământ în temeiul articolului 6 alineatul (1) litera (a) sau al

articolului 9 alineatul (2) litera (a) sau pe un contract în temeiul articolului 6 alineatul (1) litera (b) din Regulament; și

(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.

Art. 18. Dreptul la opoziție și procesul decizional individual automatizat

În orice moment, persoana vizată are dreptul de a se opune, din motive legate de situația particulară în care se află, prelucrării în temeiul articolului 6 alineatul (1) litera (e) sau (f) sau al articolului 6 alineatul (1) a datelor cu caracter personal care o privesc, inclusiv creării de profiluri pe baza respectivelor dispoziții.

Procesul decizional individual automatizat, inclusiv crearea de profiluri

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.

Capitolul XIII. OPERATORUL ȘI PERSOANA ÎMPUTERNICITĂ DE OPERATOR

Art. 19. Responsabilitatea Operatorului

(1) Ținând seama de natura, domeniul de aplicare, contextul și scopurile prelucrării, costurile implementării precum și de riscurile cu grade diferite de probabilitate și gravitate pentru drepturile și libertățile persoanelor fizice, **UAB 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 legislația specifică.**

(2) De asemenea, măsurile tehnice și organizatorice adoptate de UAB sunt necesare protejării datelor cu caracter personal împotriva distrugerilor accidentale sau ilegale, pierderii, modificării, dezvăluirii sau accesului neautorizat. Respectivele masuri se revizuiesc și se actualizează dacă este necesar.

(3) **Pentru îndeplinirea cerințelor legale specifice protecției datelor cu caracter personal UAB implementează măsuri tehnice și organizatorice orientate pe diferite direcții de acțiune, precum: alocarea/stabilirea responsabilităților pentru Responsabilul de protecția datelor, alocarea/responsabilităților pentru angajații care prelucrează date cu caracter personal, elaborarea regulamentului privind protecția datelor, adaptarea activităților organizației la cerințele legale specifice, elaborarea/implementarea unor politici/proceduri IT adecvate pentru securitatea datelor personale, instruirea personalului, monitorizarea conformității, etc.**

Art. 20. Persoana împuternicită de Operator

(1) În cazul în care prelucrarea urmează să fie realizată în numele operatorului, acesta contractează exclusiv persoane împuternicite care oferă garanții suficiente pentru punerea în aplicare a unor măsuri tehnice și organizatorice adecvate, astfel încât prelucrarea să respecte cerințele prevăzute în prezentul regulament și să asigure protecția drepturilor persoanei vizate.

(2) Persoana împuternicită de operator nu recrutează o alta persoana împuternicită fără a primi în prealabil o autorizație scrisă, specifică sau generală, din partea operatorului.

(3) Prelucrarea de către o persoană împuternicită de un operator este reglementată printr-un contract sau alt act juridic în temeiul dreptului Uniunii sau al dreptului intern care are caracter

obligatoriu pentru persoana împuternicită de operator în raport cu operatorul și care stabilește obiectul și durata prelucrării, natura și scopul prelucrării, tipul de date cu caracter personal și categoriile de persoane vizate și obligațiile și drepturile operatorului.

Capitolul XIV. NOTIFICAREA AUTORITĂȚII DE SUPRAVEGHERE ÎN CAZUL ÎNCĂLCĂRII SECURITĂȚII DATELOR CU CARACTER PERSONAL

Art. 21. (1) În cazul în care are loc o încălcare a securității datelor cu caracter personal, UAB prin Responsabilul de protecția datelor, notifică acest lucru Autorității de supraveghere competente, fără întârzieri nejustificate și, daca este posibil, în termen de cel mult 72 de ore de la data la care a luat cunoștință de aceasta, cu excepția cazului în care este susceptibilă să genereze un risc pentru drepturile și libertățile persoanelor fizice. În cazul în care notificarea Autorității nu are loc în termen de 72 de ore, aceasta va fi însoțită de o explicație motivată a întârzierii în cauză.

(2)Persoana împuternicită de operator înștiințează operatorul (informează Responsabilul cu protecția datelor al operatorului) fără întârzieri nejustificate după ce ia la cunoștință de o încălcare a securității datelor cu caracter personal.

(3)Notificarea adresată Autorității cu privire la încălcarea securității datelor personale, conține cel puțin, următoarele elemente:

a) descrierea caracterului încălcării securității datelor cu caracter personal, 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) 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) descrierea consecințelor probabile ale încălcării securității datelor cu caracter personal;

d) descrierea masurilor luate sau propuse spre a fi luate de operator pentru a remedia problema încălcării securității datelor cu caracter personal, inclusiv, după caz, masurile pentru atenuarea eventualelor sale efecte negative.

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) Operatorul, prin Responsabilul de protecția datelor, păstrează documente referitoare la toate cazurile de încălcare a securității datelor cu caracter personal, care cuprind o descriere a situației de fapt în care a avut loc încălcarea securității datelor cu caracter personal, a efectelor acesteia și a măsurilor de remediere întreprinse. Aceasta documentație permite autorității de supraveghere să verifice conformitatea cu legislația specifică.

(5) Angajații UAB au obligația de a informa de îndată șeful ierarhic și Responsabilul cu protecția datelor (Ex: se va utiliza adresa de e-mail protectiadatelor@uab.ro) în cazul identificării unei situații de încălcare a securității datelor cu caracter personal.

Responsabilul cu protecția datelor analizează informațiile comunicate, iar dacă este cazul, solicită entităților funcționale date și informații suplimentare. În cazul în care situația de încălcare a securităţi datelor cu caracter personal este fundamentată rezonabil, Responsabilul cu protecția datelor întocmește Notificarea și solicită acordul conducerii pentru a fi transmisa la Autoritatea de Supraveghere. Notificarea se transmite către Autoritatea de Supraveghere pe suport de hârtie sau în format electronic, conform cerințelor stabilite de Autoritate.

Art. 22. Informarea Persoanei vizate cu privire la încălcarea securității datelor cu caracter personal

(1)În cazul în care încălcarea securității datelor cu caracter personal este susceptibilă să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice, operatorul, prin

Responsabilul de protecția datelor, informează persoana vizată fără întârzieri nejustificate cu privire la aceasta încălcare.

(2)În informarea transmisa persoanei vizate, prevăzută anterior, se include o descriere într-un limbaj clar și simplu a caracterului încălcării securității datelor cu caracter personal, precum și cel puțin următoarele informații și măsuri:

- numele și datele de contact ale responsabilului cu protecția datelor sau un alt punct de contact de unde se pot obține mai multe informații;
- descrierea consecințelor probabile ale încălcării securității datelor cu caracter personal;
- descrierea masurilor luate sau propuse spre a fi luate de operator pentru a remedia problema încălcării securității datelor cu caracter personal, inclusiv, după caz, măsurile pentru atenuarea eventualelor sale efecte negative.

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

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

b) operatorul a luat masuri ulterioare prin care se asigură că riscul ridicat pentru drepturile și libertățile persoanelor vizate nu mai este susceptibil sa 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.

Capitolul XV. TRANSFERURILE DE DATE CU CARACTER PERSONAL CĂTRE ȚĂRI TERȚE SAU ORGANIZAȚII INTERNAȚIONALE

Art. 23. (1) **Orice decizie de a transfera date în afara spațiului UE și al Zonei Economice-Europene va fi supusă, anterior transferului și în timp util, analizei Responsabilului de protecția datelor.**

(2)**Transferurile de date în afara spațiului UE și al Zonei Economice-Europene se pot face:**

- În temeiul unei decizii a Comisiei Europene privind caracterul adecvat al nivelului de protecție;
- În baza unor garanții adecvate oferite de UAB sau persoana împuternicită a UAB.

Garanțiile adecvate pot fi furnizate prin:

a) un instrument obligatoriu d.p.d.v. juridic și executoriu între autoritățile sau organismele publice;

b) reguli corporatiste obligatorii;

c) clauze standard de protecție a datelor adoptate de Comisia Europeană;

d) clauze standard de protecție a datelor adoptate de o autoritate de supraveghere și aprobate de Comisia Europeană;

e) un cod de conduita aprobat, însoțit de un angajament obligatoriu și executoriu din partea UAB sau a persoanei împuternicite de UAB din țara terță de a aplica garanții adecvate, inclusiv cu privire la drepturile persoanelor vizate; sau

f) un mecanism de certificare aprobat, însoțit de un angajament obligatoriu și executoriu din partea UAB sau a persoanei împuternicite de UAB din țara terță de a aplica garanții adecvate, inclusiv cu privire la drepturile persoanelor vizate.

(3) **Sub rezerva autorizării din partea autorității de supraveghere, garanțiile adecvate pot fi furnizate, în special, prin:**

a) clauze contractuale între UAB, persoana împuternicită de UAB și operatorul, persoana împuternicită de operator sau destinatarul datelor cu caracter personal din țara terță sau organizația internațională; sau

b) dispoziții care urmează să fie incluse în acordurile administrative dintre autoritățile sau organismele publice, care includ drepturi opozabile și efective pentru persoanele vizate.

(4) În absența unei decizii privind caracterul adecvat al nivelului de protecție sau a unor garanții adecvate, **un transfer de date către o țara terță sau o organizație internațională poate avea loc numai în una dintre condițiile următoare:**

a) persoana vizată și-a exprimat în mod explicit acordul cu privire la transfer, după ce a fost informată asupra posibilelor riscuri pe care transferurile le pot implica pentru persoana vizată;

b) transferul este necesar pentru executarea unui contract între persoana vizată și UAB sau pentru aplicarea unor masuri precontractuale adoptate la cererea persoanei vizate;

c) transferul este necesar pentru încheierea sau pentru executarea unui contract încheiat în interesul persoanei vizate între UAB și o alta persoană fizică sau juridică;

d) transferul este necesar din considerente importante de interes public;

e) transferul este necesar pentru stabilirea, exercitarea sau apărarea unui drept în instanță;

f) transferul este necesar pentru protejarea intereselor vitale ale persoanei vizate sau ale altor persoane, atunci când persoana vizata nu are capacitatea fizica sau juridica de a-și exprima acordul;

g) transferul se realizează dintr-un registru care, potrivit dreptului UE sau al dreptului intern, are scopul de a furniza informații publicului și care poate fi consultat de public în general, sau de orice persoană care poate face dovada unui interes legitim.

(5) În lipsa unei decizii a Comisiei, a unor garanții adecvate dar și în lipsa condițiilor precizate anterior, **un transfer către o țara terță sau o organizație internațională poate avea loc numai în cazul în care:**

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

Capitolul XVI. CĂI DE ATAC

Art. 24. Dreptul de a depune o plângere la o autoritate de supraveghere

(1) Fără a aduce atingere oricăror alte cai de atac administrative sau judiciare, orice persoană vizată are dreptul de a depune o plângere la o autoritate de supraveghere, în special în statul membru în care își are reședința obișnuită, în care se află locul sau de muncă sau în care a avut loc presupusa încălcare, în cazul în care consideră că prelucrarea datelor cu caracter personal care o vizează încălca prezentul regulament.

(2) Autoritatea de supraveghere la care s-a depus plângerea informează reclamantul cu privire la evoluția și rezultatul plângerii, inclusiv posibilitatea de a exercita o cale de atac judiciară în temeiul legislației specifice.

Art. 25. Dreptul la o cale de atac judiciară eficientă împotriva unei autorități de supraveghere

(1) Fără a aduce atingere oricăror alte căi de atac administrative sau nejudiciare, fiecare persoană vizată are dreptul de a exercită o cale de atac judiciară eficientă împotriva unei decizii obligatorii din punct de vedere juridic a unei autorități de supraveghere care o vizează.

(2) Fără a aduce atingere oricăror alte cai de atac administrative sau nejudiciare, fiecare persoană vizată are dreptul de a exercită o cale de atac judiciară eficientă în cazul în care autoritatea de supraveghere competentă nu tratează o plângere sau nu informează persoana vizată în termen de trei luni cu privire la progresele sau la soluționarea plângerii depuse.

(3) Acțiunile introduse împotriva unei autorități de supraveghere sunt aduse în fața instanțelor din statul membru în care este stabilită autoritatea de supraveghere.

Capitolul XVII. RESPONSABILITĂȚI ÎN CADRUL UNIVERSITĂȚII „1 DECEMBRIE 1918" DIN ALBA IULIA

Art. 26. (1) Cunoașterea și aplicarea corespunzătoare a prezentului Regulament reprezintă obligația întregului personal al UAB potrivit limitelor de autoritate aprobate;

(2) Responsabilitățile privind protecția datelor cu caracter personal revin gradual întregului personal al UAB;

(3)Responsabilitățile în ceea ce privește elaborarea, avizarea, aprobarea, implementarea, supravegherea și evaluarea aplicabilității prezentului Regulament, precum și dispunerea masurilor care se impun revin, după cum urmează:

Art. 27. UAB (cu toate structurile organizatorice), în calitate de Operator:

a) asigură implementarea legislației comunitare-UE și naționale privind protecția datelor cu caracter personal la nivelul UAB, prin prezentul regulament sau alte acte interne ;

b) asigură conformarea tuturor activităților de prelucrare cu prevederile legislației comunitare-UE și națională privind protecția datelor cu caracter personal;

c) asigură informarea persoanelor vizate și respectă drepturile acestora;

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

e) asigură respectarea prezentului regulament privind masurile de protecție a persoanelor cu privire la prelucrarea datelor cu caracter personal.

Art. 28. Organele de Conducere ale UAB și conducătorii structurilor sale organizatorice (direcții, servicii, birouri, compartimente etc.) sunt responsabili cu protecția datelor cu caracter personal pentru activitățile coordonate și au în acest sens următoarele responsabilități specifice:

a) stabilesc scopul și mijloacele de prelucrare a datelor cu caracter personal atunci când acestea sunt necesare în contextul derulării activității de învățământ sau evenimentele organizate de UAB în incinta imobilelor UAB, inclusiv desfășurării activității curente a UAB, precum și în contextul îndeplinirii obligațiilor legale;

b) asigură elaborarea/actualizarea procedurilor proprii și, după aprobarea acestora le pun în aplicare;

c) asigură implementarea și monitorizează respectarea actelor de reglementare internă și a legislației specifice, în materia prelucrării datelor cu caracter personal de către utilizatorii (angajații) din subordine;

d) coordonează și monitorizează activitatea personalului pe linia protecției datelor cu caracter personal la nivelul operatorului;

e) asigura desfășurarea pregătirii de specialitate și instruirea utilizatorilor în acest domeniu;

f) dispun masuri de completare sau, după caz, de modificare a fișei posturilor utilizatorilor;

g) analizează și dispun în ceea ce privește suspendarea sau revocarea dreptului de acces al utilizatorilor la sisteme de evidență a datelor cu caracter personal, în condițiile legii;

h) dispun masuri organizatorice pentru exercitarea drepturilor de către persoana vizată;

i) coordonează procesul de furnizare a datelor și informațiilor necesare în vederea soluționării cererilor persoanelor vizate;

j) analizează periodic activitatea utilizatorilor;

k) informează operativ Responsabilul de protecția datelor despre vulnerabilitățile și riscurile semnalate în sistemul de securitate a prelucrării datelor cu caracter personal al structurii și propune masuri pentru înlăturarea acestora;

l) informează operativ Responsabilul cu protecția datelor în legătură cu orice încălcare a normelor de protecție a datelor cu caracter personal de natură a prejudicia drepturile persoanei vizate, cu privire la masurile dispuse pentru identificarea persoanei responsabile și limitarea efectelor unei diseminări neautorizate a datelor, precum și cu privire la situațiile în care au fost emise recomandări sau aplicate sancțiuni de către Autoritatea națională de supraveghere sau când aceasta a dispus efectuarea unui control prealabil ori a unor investigații.

Art. 29. Utilizatorii, respectiv angajații UAB care prelucrează date cu caracter personal au următoarele responsabilități specifice:

a) să cunoască și să aplice prevederile actelor normative din domeniul prelucrării datelor cu caracter personal precum și ale prezentului regulament;

b) să informeze persoana vizată atunci când datele cu caracter personal sunt colectate direct de la aceasta, în condițiile legii, cu privire la: identitatea operatorului, scopul în care se face prelucrarea datelor, destinatarii sau categoriile de destinatari ai datelor, obligativitatea furnizării tuturor datelor cerute și consecințele refuzului de a le pune la dispoziție, drepturile prevăzute de lege, condițiile în care pot fi exercitate aceste drepturi etc.;

c) să prelucreze numai datele cu caracter personal necesare îndeplinirii atribuțiilor de serviciu și să acorde sprijin șefilor ierarhici, organelor de conducere ale UAB, pentru realizarea activităților specifice ale acestora;

d) să păstreze confidențialitatea datelor prelucrate, a contului de utilizator, a parolei/codului de acces la sistemele informatice/ baze de date prin care sunt gestionate date cu caracter personal;

e) să respecte masurile de securitate, precum și celelalte reguli stabilite la nivelul UAB

f) să informeze de îndată șeful ierarhic și Responsabilul de protecția datelor la adresa de e-mail: protectiadatelor@uab.ro) despre împrejurări de natura a conduce la o diseminare neautorizată de date cu caracter personal sau despre o situație în care au fost accesate/ prelucrate date cu caracter personal prin încălcarea normelor legale, despre care a luat la cunoștință.

Capitolul XVIII. EVIDENȚA ACTIVITĂȚILOR DE PRELUCRARE

Art. 30. UAB păstrează evidența activităților de prelucrare desfășurate. Evidențele se formulează în scris, inclusiv în format electronic. UAB pune evidențele la dispoziția autorității de supraveghere, la cererea acesteia.

Capitolul XIX. DISPOZIȚII FINALE ȘI TRANZITORII

Art. 31. Prezentul regulament a fost aprobat în ședința Senatului din data de 25.05.2018, modificat în ședința din data de 20.02.2019.

Prezentul regulament se completează cu prevederile legale în domeniul protecției datelor cu caracter personal.

Capitolul XX. ANEXE

Anexa nr. 1 *Nota de informare privind protecţia datelor personale pentru studenţi*
Anexa nr. 2 *Nota de informare privind protecţia datelor personale pentru angajaţi*
Anexa nr. 3 *Informare privind prelucrarea datelor personale prin intermediul sistemului de supraveghere video*
Anexa nr. 4 *Angajament de conformare*
Anexa nr. 5 *Cerere Acces*
Anexa nr. 6 *Cerere Rectificare*
Anexa nr. 7 *Cerere Ştergere*

Aprobat în Şedinţa Senatului Universităţii „1 Decembrie 1918" din Alba Iulia din 20 februarie 2019.

P R E Ş E D I N T E
Conf. univ. dr. Tamas-Szora Attila

AVIZAT
Oficiul Juridic
Consilier juridic Claudia Rotar