# REGULAMENT
## PRIVIND ASIGURAREA SECURITĂȚII PRELUCRĂRII DATELOR CU CARACTER PERSONAL

IAȘI - 2025

CAPITOLUL I : DISPOZIŢII GENERALE

Art. 1(1):Regulamentului general privind protecția datelor ("GDPR") Regulamentul general privind protecția datelor, 679/2016, înlocuiește Directiva UE din 1995 privind protecția datelor și înlocuiește legislația fiecărui stat membru care a fost elaborată în conformitate cu Directiva 95/46/CE privind protecția datelor.

(2) :Scopul său este de a proteja "drepturile și libertățile" persoanelor fizice în viață și de a se asigura că datele cu caracter personal nu sunt prelucrate fără cunoștința lor și, ori de câte ori este posibil, că sunt prelucrate cu consimțământul lor.

(3) :Definițiile utilizate de organizație (extrase din GDPR) :

■- Domeniul material (articolul 2) - GDPR se aplică prelucrării datelor cu caracter personal, efectuată total sau parţial prin mijloace automatizate, precum şi prelucrării prin alte mijloace decât cele automatizate a datelor cu caracter personal care fac parte dintr-un sistem de evidenţă a datelor sau care sunt destinate să facă parte dintr-un sistem de evidenţă a datelor.

■-Domeniul de aplicare teritorial (articolul 3) - GDPR se aplică prelucrării datelor cu caracter personal în cadrul activităţilor unui sediu al unui operator sau al unei persoane împuternicite de operator pe teritoriul Uniunii, indiferent dacă prelucrarea are loc sau nu pe teritoriul Uniunii. Prezentul regulament se aplică prelucrării datelor cu caracter personal ale unor persoane vizate care se află în Uniune de către un operator sau o persoană împuternicită de operator care nu este stabilit(ă) în Uniune, atunci când activităţile de prelucrare sunt legate de:

a)- oferirea de bunuri sau servicii unor astfel de persoane vizate în Uniune, indiferent dacă se solicită sau nu efectuarea unei plăţi de către persoana vizată; sau

b)- monitorizarea comportamentului lor dacă acesta se manifestă în cadrul Uniunii. Prezentul regulament se aplică prelucrării datelor cu caracter personal de către un operator care nu este stabilit în Uniune, ci într-un loc în care dreptul intern se aplică în temeiul dreptului internaţional public.

■- "Sediul principal" - sediul principal al operatorului în UE va fi locul în care operatorul adoptă principalele decizii cu privire la scopul și mijloacele activităților sale de prelucrare a datelor. Sediul principal al unei persoane imputernicite în UE va fi centrul său administrativ.

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

■- "Categorii speciale de date cu caracter personal" - date cu caracter personal care dezvăluie originea rasială sau etnică, opinii politice, convingeri religioase sau filosofice sau apartenența sindicală și prelucrarea datelor genetice, date biometrice în scopul identificării unice a unei persoane fizice, date privind sănătatea sau date privind viața sexuală sau orientarea sexuală a unei persoane fizice.

■- "Operator" înseamnă persoana fizică sau juridică, autoritatea publică, agenţia sau alt organism care, singur sau împreună cu altele, stabileşte scopurile şi mijloacele de prelucrare a datelor cu caracter personal; atunci când scopurile şi mijloacele prelucrării sunt stabilite prin dreptul Uniunii sau dreptul intern, operatorul sau criteriile specifice pentru desemnarea acestuia pot fi prevăzute în dreptul Uniunii sau în dreptul intern;

■- "Persoana vizată" - orice persoană vie care face obiectul datelor cu caracter personal deținute de o organizație.

■- "Prelucrare" înseamnă orice operaţiune sau set de operaţiuni 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 dispoziţie în orice alt mod, alinierea sau combinarea, restricţionarea, ştergerea sau distrugerea;

■- "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 performanţa la locul de muncă, situaţia economică, sănătatea, preferinţele personale, interesele, fiabilitatea, comportamentul, locul în care se află persoana fizică respectivă sau deplasările acesteia.

■- "Incălcarea securităţii datelor cu caracter personal" înseamnă o încălcare a securităţii 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

■- "Consimţământ" al persoanei vizate înseamnă orice manifestare de voinţă liberă, specifică, informată şi lipsită de ambiguitate a persoanei vizate prin care aceasta acceptă, printr-o declaraţie sau printr-o acţiune fără echivoc, ca datele cu caracter personal care o privesc să fie prelucrate;

■- "Copil" - GDPR definește un copil drept orice persoană cu vârsta sub 16 ani, deși acest lucru poate fi redus la 13 de legislația statelor membre. Prelucrarea datelor cu caracter personal ale unui copil este legală numai dacă a fost obținut consimțământul părinților sau custozilor. Operatorul va depune eforturi rezonabile pentru a verifica, în astfel de cazuri, dacă titularul răspunderii părintești asupra copilului acordă sau autorizează acordul.

■- „Parte terţă" înseamnă o persoană fizică sau juridică, autoritate publică, agenţie sau organism altul decât persoana vizată, operatorul, persoana împuternicită de operator şi persoanele care, sub directa autoritate a operatorului sau a persoanei împuternicite de operator, sunt autorizate să prelucreze date cu caracter personal.

■- "Sistem de evidenţă a datelor" înseamnă orice set structurat de date cu caracter personal accesibile conform unor criterii specifice, fie ele centralizate, descentralizate sau repartizate după criterii funcţionale sau geografice;

CAPITOLUL II : POLITICA DE CONFIDENTIALITATE

Art. 2(1): Consiliul de Administrație și conducerea Universității , se angajează să respecte toate legile relevante ale UE și ale statelor membre cu privire la datele cu caracter personal și protecția "drepturilor și libertăților" persoanelor ale căror informații le colectează și proceseaza, în conformitate cu Regulamentul general privind protecția datelor (GDPR).

(2) :Conformitatea cu GDPR este descrisă de această politică și de alte politici relevante privind protecția datelor cu caracter personal, împreună cu procesele și procedurile conexe.

(3) :GDPR va fi aplicat de toate persoanele din cadrul Universității care prelucrează date cu caracter personal, ale clienților, angajaților, furnizorilor și partenerilor, precum și orice alte date personale pe care organizația le procesează din orice sursă.

(4) : COMISIA PENTRU SUPRAVEGHEREA PRELUCRĂRII DATELOR CU CARACTER PERSONAL constituită la nivelul Universității , este responsabilă pentru revizuirea anuală, sau atunci când este cazul, a tuturor documentațiilor de evidență, cartografiere și evaluare a activităților de prelucrare a datelor privind orice modificări ale activităților Universității .Aceste revizuiri pot fi determinate de schimbări înregistrate în procesele de prelucrare a datelor sau de orice cerințe suplimentare identificate prin evaluări ale impactului protecției datelor. Documentațiile trebuie să fie disponibile pentru verificare la cererea Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal

(5) :Această politică se aplică tuturor angajaților, personalului și părților interesate din cadrul Universitătii, cum ar fi furnizorii externalizați. Orice încălcare a GDPR va fi tratată conform politicii disciplinare a Universitătii și poate fi, de asemenea, o contraventie, caz în care problema va fi raportată cât mai curând posibil autorităților competente.

(6) :Se așteaptă ca partenerii și orice terțe părți care lucrează cu sau pentru Universitate și care au sau ar putea avea acces la date cu caracter personal, să respecte această politică. Nicio terță parte nu poate accesa datele cu caracter personal deținute de Universitate , fără să fi încheiat în prealabil un acord de confidențialitate a datelor și de prelucrare a acestora conform GDPR, acord prin care se vor impune terței părți obligații nu mai puțin oneroase decât cele pe care le respecta Universitatea și care-i conferă dreptul de a verifica respectarea acordului.

CAPITOLUL II : RESPONSABILITĂȚI ȘI ROLURI ÎN TEMEIUL REGULAMENTULUI GENERAL PRIVIND PROTECȚIA DATELOR

Art. 3(1):Universitatea poate fi, în context GDPR, atât operator de date cât și persoană împuternicită, rolul urmând a fi determinat prin analiza și cartografierea fiecărui proces de prelucrare de date cu caracter personal.

(2) :Managementul și toți cei cu roluri de conducere sau de supraveghere sunt responsabili pentru dezvoltarea și încurajarea practicilor de gestionare a informațiilor în cadrul societății. Sarcinile specifice și responsabilitățile sunt stabilite în fișele de post individuale.

(3) : COMISIA PENTRU SUPRAVEGHEREA PRELUCRĂRII DATELOR CU CARACTER PERSONAL se asigură de respectarea legislației în domeniu și a bunelor practici. Această responsabilitate include sesizarea de proceduri de lucru neconforme, inițierea de analize de impact în vederea gestionării securității și a riscurilor în ceea ce privește asigurarea unui nivel adecvat de protecție a datelor cu caracter personal. DPO, în cazul în care este numit, va fi sesizat obligatoriu la fiecare intenție de modificare a procedurilor de lucru ce presupun prelucrarea de date cu caracter personal, avizul lui fiind obligatoriu.

(4) : COMISIA PENTRU SUPRAVEGHEREA PRELUCRĂRII DATELOR CU CARACTER PERSONAL, are responsabilități specifice în ceea ce privește solicitările persoanelor vizate și reprezintă primul punct de contact pentru angajați sau orice persoane care solicită clarificări cu privire la orice aspect al respectării protecției datelor.

(5) :Prevederile prezentei politici se completează cu cele ale Regulamentului UE 2016/679 în ceea ce privește rolul DPO.

(6) :Conformitatea cu legislația privind protecția datelor este responsabilitatea tuturor angajaților din Universitătii care procesează datele cu caracter personal.

(7) :Politica de instruire internă a Universitătii stabilește cerințe specifice de formare și conștientizare a personalului în legătură cu rolurile specifice in domeniul protectiei datelor. Angajații cu rol în prelucrarea datelor cu caracter personal vor paricipa periodic la cursuri de instruire în acest sens.

(8) :Angajații organizației sunt responsabili pentru a se asigura că datele personale pe care le au furnizat către Universitate , sunt corecte și actualizate.

CAPITOLUL III : PRINCIPII LEGATE DE PRELUCRAREA DATELOR CU CARACTER PERSONAL

Art. 4(1):Prelucrarea datelor cu caracter personal trebuie să se desfășoare în conformitate cu principiile de protecție a datelor, prevăzute la articolul 5 din GDPR. Politicile și procedurile Universitătii vor fi concepute astfel încât să asigure respectarea acestor principii.

(2):Datele personale trebuie prelucrate în mod legal, echitabil şi transparent:

■- "Legal" – este identificată baza legală înainte de a putea prelucra datele personale. Acestea sunt adesea denumite "condițiile de procesare" și sunt Legea, Contractul sau Consimțământul.

■- "Echitabil" - pentru ca prelucrarea să fie echitabila, operatorul de date trebuie să pună la dispoziția persoanelor vizate anumite informații cât mai practic posibil. Aceasta se aplică dacă datele cu caracter personal au fost obținute direct de la persoanele vizate sau din alte surse.

■- "Transparență" - GDPR include reguli privind furnizarea catre persoanele vizate de informații privind confidențialitatea în articolele 12, 13 și 14. Acestea sunt detaliate și specifice, punând accentul pe faptul că notificările privind confidențialitatea sunt înțelese și accesibile. Informațiile trebuie comunicate persoanei vizate într-o formă inteligibilă, folosind un limbaj clar și simplu. Informațiile specifice care trebuie furnizate persoanei vizate trebuie să includă cel puțin:

•-identitatea și datele de contact ale operatorului și, dacă este cazul, ale reprezentantului operatorului;

•-datele de contact ale COMISIEI PENTRU SUPRAVEGHEREA PRELUCRĂRII DATELOR CU CARACTER PERSONAL cu protecția datelor;

•-scopul prelucrării pentru care sunt destinate datele cu caracter personal, precum și temeiul juridic al prelucrării;

•-perioada pentru care vor fi stocate datele cu caracter personal;

•-existența drepturilor de a solicita accesul, rectificarea, ștergerea sau opoziția față de prelucrare și condițiile (sau lipsa) de exercitare a acestor drepturi, cum ar fi afectarea legalității prelucrării anterioare;

•-categoriile de date cu caracter personal vizate;

•-destinatarii sau categoriile de destinatari ai datelor cu caracter personal, după caz;

•-dacă este cazul, că operatorul intenționează să transfere date cu caracter personal unui destinatar dintr-o țară terță și nivelul de protecție acordat datelor;

•-orice informații suplimentare necesare pentru a garanta o prelucrare corectă.

(3) :Datele personale pot fi colectate doar în scopuri specifice, explicite și legitime. Datele obținute în scopurile specificate nu trebuie utilizate într-un scop care diferă de cele care au fost notificate în mod oficial, atunci când e cazul, Autorității de Supraveghere.

(4) :Datele personale trebuie să fie adecvate, relevante și limitate la ceea ce este necesar pentru procesare. În acest sens:

(4.1)-Managementul Universitătii se va asigura că societatea nu colectează informații care nu sunt strict necesare pentru scopul pentru care sunt obținute.

(4.2)-În toate formularele de colectare a datelor (electronice sau pe suport de hârtie), inclusiv cererile de colectare a datelor în noile sisteme informatice, trebuie să fie inclusă o declarație de procesare echitabilă sau un link catre politica de confidențialitate în vigoare.

(4.3)-Managementul Universității se va asigura că toate metodele de colectare a datelor sunt revizuite, prin audit efectuat de experți interni sau externi, pentru a se asigura că datele colectate sunt în continuare adecvate, relevante și limitate.

(4.4)-Datele cu caracter personal care sunt inexacte, având în vedere scopurile pentru care sunt prelucrate, sunt șterse sau rectificate fără întârziere ("exactitate") :

■-Datele care sunt stocate de către operatorul de date trebuie revizuite și actualizate, după caz.

■-Managementul Universității are responsabilitatea de a se asigura că întreg personalul este instruit cu privire la importanța colectării și menținerii datelor exacte.

■- Totodată, este responsabilitatea persoanei vizate să se asigure că datele deținute de Universitate sunt exacte și actualizate. Completarea unui formular de înregistrare sau o cerere de către o persoană vizată va include o declarație conform căreia datele conținute în aceasta sunt corecte la data depunerii.

■- Angajații, clienții sau alte persoane interesate sunt obligați să notifice Universității orice schimbări, pentru a permite actualizarea în mod corespunzător a evidențelor personale. Este responsabilitatea Universitătii să se asigure că orice notificare privind modificările este înregistrată și operată.

■- Managementul Universității este responsabil de asigurarea aplicării procedurilor și politicilor adecvate pentru păstrarea datelor cu caracter personal corecte și actualizate, ținând cont de volumul de date colectate, de viteza cu care s-ar putea modifica și de orice alți factori relevanți.

■- Managementul Universității ,sau DPO dacă este numit, se va îngriji de examinarea anuală a datelor păstrate, prelucrate de societate pentru a identifica orice date care nu mai sunt necesare în contextul scopului înregistrat. Aceste date vor fi șterse sau distruse în siguranță, în conformitate cu procedura de stergere / distrugere a suporturilor de stocare.

■- Managementul Universității, sau DPO dacă este numit, are obligația de a răspunde solicitărilor de rectificare de la persoanele vizate în termen de 30 de zile. Acest termen poate fi extins, pentru solicitări complexe, cu informarea persoanei vizate. Dacă solicitarea este considerată abuzivă, acest lucru va fi adus la cunoștința persoanei vizate, motivând clasificarea și să o informeze cu privire la dreptul de a depune plângere Autorității de Supraveghere și de a solicita căi de atac.

■- Managementul Universității este responsabil de luarea măsurilor adecvate care, în cazul în care organizațiile terțe părți ar fi primit date cu caracter personal

inexacte sau neactualizate, să le informeze că acestea sunt inexacte și / sau expirate și nu trebuie să fie utilizate, sau pentru transmiterea oricărei corecții a datelor cu caracter personal părții terțe în cazul în care acest lucru este necesar.

(4.5)-Datele cu caracter personal trebuie păstrate într-o formă care să permită identificarea persoanei vizate numai atâta timp cât este necesar pentru prelucrare.

■- Dacă datele cu caracter personal sunt păstrate peste data prelucrării, acestea vor fi minimizate, criptate sau pseudonimizate, pentru a proteja identitatea persoanei vizate.

■- Datele cu caracter personal vor fi păstrate în conformitate cu termenele legale sau stabilite prin decizie internă și odată ce data de păstrare a fost depășită, aceste date vor fi distruse în siguranță.

■- Managementul Universitătii va aproba în mod specific orice păstrare a datelor care depășește perioadele de păstrare definite și trebuie să se asigure că justificarea este facuta în mod clar și în conformitate cu cerințele legale privind protecția datelor. Această aprobare se va face exclusiv în scris. 4.6 Datele personale trebuie prelucrate într-o manieră care să asigure securitatea corespunzătoare. Este obligatorie, de fiecare dată când se sesizează un posibil risc, efectuarea unei analize de impact, luând în considerare toate circumstanțele operațiunilor de procesare ale Universitătii . La determinarea caracterului adecvat, se vor lua în considerare, de asemenea, amploarea eventualelor daune sau pierderi care ar putea fi cauzate persoanelor (de exemplu, personalului sau clienților) în cazul unei încălcări a securității, efectul oricărei încălcări a securității asupra Universitătii și orice daune reputaționale posibile, inclusiv pierderea posibilă a încrederii clienților. La evaluarea măsurilor tehnice adecvate, se vor lua în considerare cel putin următoarele:

•-Protecția prin parolă;

•-Blocarea automată a terminalelor (calculator/laptop etc) cand nu sunt folosite (idle state);

•-Eliminarea drepturilor de acces pentru USB și alte suporturi de memorie;

•- Software de verificare a virușilor și firewall-uri;

•-Drepturile de acces in functie de roluri, inclusiv cele atribuite personalului temporar;

•-Criptarea dispozitivelor care părăsesc sediile organizației, cum ar fi laptopurile;

•-Securitatea rețelelor locale si WLAN;

•-Tehnologii de îmbunătățire a confidențialității, cum ar fi pseudonimizarea și anonimizarea; - Identificarea standardelor de securitate relevante pentru Universitate.La evaluarea măsurilor organizatorice adecvate, se vor lua în considerare si următoarele:

•-Nivelurile potrivite de instruire în cadrul UNIVERSITĂTII ;

•-Includerea atribuțiilor și responsabilităților privind protecția datelor în fișe de post ale persoanelor care prelucrează astfel de date;

•-Identificarea măsurilor de acțiune disciplinară pentru încălcarea datelor;

•-Monitorizarea personalului pentru respectarea standardelor de securitate relevante;

•-Controlul accesului fizic la înregistrările electronice și pe hârtie;

•-Stocarea datelor pe suport de hârtie în dulapuri securizate;

•- Restricționarea utilizării dispozitivelor electronice portabile în afara locului de muncă;

•-Restricționarea folosirii dispozitivelor personale ale angajatului la locul de muncă;

•- Adoptarea unor reguli clare despre parole;

• - Realizarea de copii de rezervă periodică a datelor;

•-Impunerea obligațiilor contractuale asupra altor organizații de a lua măsuri de securitate corespunzătoare atunci când transferă date în afara SEE. Se va acorda o atenție sporită riscurilor pe care le prezintă prelucrarea datelor, care pot duce la prejudicii aduse persoanelor fizice ale căror date sunt prelucrate.

(4.6)-Operatorul trebuie să poată demonstra conformitatea cu celelalte principii ale GDPR și cu prevederile care promovează responsabilitatea și guvernanța. Universitatea va demonstra conformitatea cu principiile protecției datelor prin implementarea politicilor de protecție a datelor, respectarea codurilor de conduită, punerea în aplicare a măsurilor tehnice și organizatorice, precum și adoptarea unor tehnici precum protecţia datelor începând cu momentul conceperii, DPIA, procedurile de notificare a încălcărilor și planurile de răspuns la incidente.

## CAPITOLUL IV : DREPTURILE PERSOANELOR VIZATE

Art. 5(1):Persoanele vizate au următoarele drepturi în ceea ce privește prelucrarea datelor și înregistrările acestor date:

(1.1)-Să solicite acces cu privire la informațiile deținute și referitoare la cei carora le-au fost dezvăluite.

(1.2)-Să se opună prelucrării, mai ales daca le-ar putea provoca daune sau prejudicii.

(1.3)-Să se opună prelucrării în scopul marketingul direct.

(1.4)-Să fie informați cu privire la procesul decizional individual automatizat, inclusiv crearea de profiluri.

(1.5)-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.

(1.6)-Să solicite despăgubiri în cazul în care suferă daune prin orice încălcare a GDPR;

(1.7)-Să ia măsuri pentru rectificarea, blocarea, ștergerea, inclusiv dreptul de a fi uitat sau distrugerea datelor inexacte.

(1.8)-Să solicite autorității de supraveghere să evalueze dacă o prevedere a GDPR a fost încălcată.

(1.9)-Persoana vizată are dreptul de a primi datele cu caracter personal care o privesc şi pe care le-a furnizat operatorului într-un format structurat, utilizat în mod curent şi care poate fi citit automat şi are dreptul de a transmite aceste date altui operator, fără obstacole din partea operatorului căruia i-au fost furnizate datele cu caracter personal.

(1.10)-Persoana vizată are dreptul de a se opune creării de profile fără existența unui consimțământ în acest sens.

(2):Universitatea asigură persoanele vizate ca isi pot exercita aceste drepturi:

(2.1)-Persoanele vizate pot face cereri de acces la date, conform Procedurii de solicitare a accesului persoanei vizate; această procedură descrie, de asemenea, modul în care Universitatea se asigură că răspunsul său la solicitarea de acces la date respectă cerințele GDPR.

(2.2)-Persoanele vizate au dreptul să depună o solicitare către Universitatea în legătură cu prelucrarea datelor lor personale. Toate solicitările din partea persoanelor vizate și modul în care au fost soluționate plângerile se vor face în conformitate cu procedura care le reglementează.

(2.3)-Persoana responsabilă pentru tratarea solicitărilor primite din partea persoanelor vizate este desemnată de Rectorul Universității;

Art. 6:Consimțământul :

(1)-Universitatea înțelege prin "consimțământul" persoanei vizate orice manifestare de voinţă liberă, specifică, informată şi lipsită de ambiguitate a persoanei vizate prin care aceasta acceptă, printr-o declaraţie sau printr-o acţiune fără echivoc, ca datele cu caracter personal care o privesc să fie prelucrate. Persoana vizată își poate retrage consimțământul în orice moment.

(2)-Universitatea înțelege că, prin "consimțământ", persoana vizată a fost pe deplin informată cu privire la prelucrarea datelor personale și a solicitat acordul în timp ce se află într-o stare de spirit adecvată pentru a face acest lucru și fără a se exercita presiuni asupra ei. Consimțământul obținut sub presiune sau pe baza unor informații înșelătoare nu va constitui o bază valabilă pentru procesare.

(3)-Trebuie să existe o comunicare activă între părți pentru a demonstra consimțământul activ. Consimțământul nu poate fi dedus din lipsa de răspuns la o

comunicare. Operatorul trebuie să poată demonstra obținerea consimțământului pentru operațiunea de procesare.

(4)-Pentru datele sensibile, trebuie obținut un acord scris explicit a persoanelor vizate, cu excepția cazului în care există o bază legală de procesare alternativă, contract sau obligație legală.

(5)-În majoritatea cazurilor, consimțământul de prelucrare a datelor personale și sensibile este obținut în mod obișnuit de Universitatea utilizând declaratiile de consimțământ standard avizate de Management.

(6)-În cazul în care Universitatea are acces la date cu caracter personal ale minorilor, pentru prelucrarea acestora este obligatoriu consimțământul părintelui sau al reprezentantului legal al copilului. Această cerință se aplică copiilor cu vârsta sub 16 ani (cu excepția cazului în care statul membru prevede o limită de vârstă mai mică, dar nu poate fi mai mică de 13).

## CAPITOLUL V : SECURITATEA DATELOR

Art. 7(1):Toți angajații sunt responsabili pentru a se asigura că toate datele personale pe care Universitateale deține și prelucrează sunt păstrate în siguranță, potrivit procedurilor și măsurilor de securitate interne și nu sunt divulgate în niciun fel unei terțe părți decât dacă acea terță parte a fost autorizată în mod specific să primească aceste informații și a încheiat un acord de confidențialitate.

(2)-Toate datele personale ar trebui să fie accesibile numai celor care au nevoie să le folosească și accesul poate fi acordat numai în conformitate cu Politica de control al accesului. Toate datele cu caracter personal trebuie procesate in siguranță și trebuie păstrate:

- - într-o cameră închisă cu acces controlat;
- - într-un sertar închis sau într-un dulap;
- - dacă sunt păstrate pe computere, protejate prin parolă în conformitate cu cerințele din politica IT sau politica de control a accesului și / sau stocate pe suporturi (detașabile) care sunt criptate.

(3)-Toate ecranele laptopurilor și terminalelor PC vor fi vizibile doar personalului autorizat al Universitatii . Toți angajații vor utiliza funcția idle (lock) ca modalitate de blocare a accesului neautorizat.

(4)-Înregistrările in format fizic nu pot fi lăsate acolo unde pot fi accesate de personal neautorizat sau vizitatori și nu pot fi înlăturate din sediu fără autorizație explicită scrisă. Imediat ce înregistrările în format fizic nu mai sunt necesare pentru activitatea curentă, acestea trebuie să fie arhivate sau distruse în siguranță.

(5)-Datele personale pot fi șterse sau eliminate numai în conformitate cu procedura de păstrare a înregistrărilor. Înregistrările în format fizic care au ajuns la

scadență, trebuie să fie mărunțite și aruncate ca "deșeuri confidențiale", iar procedura consemnată într-un proces verbal.

(6)-Prelucrarea datelor cu caracter personal "în afara sediului" este interzisă și prezintă un risc potențial mai mare decat pierderea, furtul sau deteriorarea datelor cu caracter personal. Personalul trebuie să fie autorizat în mod specific să proceseze datele în afara sediului.

(7)-Orice încălcare a securității datelor cu caracter personal va fi notificată imediat persoanei / persoanelor vizate, pentru a putea lua măsuri de precauție necesare. În notificare se va descrie natura încălcării securității datelor cu caracter personal și se vor transmite recomandări pentru persoana fizică în scopul atenuării eventualelor efecte negative.

(8)-Încălcarea securității datelor se notifică în termen de 72 de ore Autorității de Supraveghere prin formularul pus la dispoziție pe www.dataprotection.ro. Atunci când notificarea nu poate fi realizată în acest termen, ea va trebui să fie transmisă de îndată ce este posibil, împreună cu motivele întârzierii.

(9)-Notificările nu sunt necesare atunci când se poate demonstra, în conformitate cu principiul responsabilității, că încălcarea securității datelor cu caracter personal nu este susceptibilă să genereze un risc pentru drepturile și libertățile persoanelor fizice.

## CAPITOLUL VI : DIVULGAREA DATELOR

Art. 8(1):Universitatea trebuie să se asigure că datele cu caracter personal nu sunt divulgate terților neautorizați, care includ membri ai familiei, prieteni, organisme guvernamentale și, în anumite circumstanțe, chiar și organele de control. Toți angajații trebuie să fie atenți atunci când sunt rugați să dezvăluie datele personale deținute de o altă persoană unei terțe părți. Este important să se țină seama de relevanța divulgării informațiilor este sau nu relevantă pentru desfășurarea activității.

(2)-Regulamentul UE 2016/679 permite anumite cazuri în care dezvăluirea este posibilă fără consimțământ, atunci când informațiile sunt solicitate pentru unul sau mai multe din următoarele scopuri:

(2.1)-protejarea securității naționale;

(2.2)-prevenirea sau depistarea infracțiunilor, inclusiv reținerea sau urmărirea penală a infractorilor;

(2.3)-îndeplinirea funcțiilor de reglementare (include sănătatea, siguranța și bunăstarea persoanelor la locul de muncă);

(2.4)-pentru a preveni vătămarea gravă a unui terț;

(2.5)-pentru a proteja interesele vitale ale individului în situații de viață și de moarte.

(3)-Toate solicitările de furnizare a datelor pentru unul dintre aceste motive trebuie să fie susținute de o documentație adecvată, iar toate aceste dezvăluiri trebuie să fie autorizate în mod specific de către Management sau DPO în cazul în care este numit.

CAPITOLUL VII : PĂSTRAREA ȘI ELIMINAREA DATELOR

Art. 9(1):Universitatea nu va păstra datele cu caracter personal într-o formă care să permită identificarea persoanelor vizate pentru o perioadă mai lungă decât este necesar, în raport cu scopul / scopurile pentru care datele au fost colectate inițial.

(2)-Universitatea poate stoca date pentru perioade mai lungi în cazul în care datele cu caracter personal vor fi prelucrate exclusiv în scopuri de arhivare în interes public, în scopuri științifice sau istorice de cercetare sau în scopuri statistice, sub rezerva punerii în aplicare a măsurilor tehnice și organizatorice adecvate pentru protejarea drepturilor și libertăților persoanei vizate.

(3)-Perioada de păstrare pentru fiecare categorie de date cu caracter personal va fi stabilită expres, împreună cu criteriile utilizate pentru stabilirea acestei perioade, inclusiv obligațiile legale ale societății care trebuie să păstreze datele.

(4)-Termenele de păstrare a datelor și procedurile de ștergere a datelor prelucrate și stocate de Universitatease vor aplica în toate cazurile.

(5)-Datele cu caracter personal trebuie să fie eliminate în siguranță, în conformitate cu al șaselea principiu al GDPR - prelucrate într-un mod adecvat pentru a menține securitatea, protejând astfel "drepturile și libertățile" persoanelor vizate. Orice eliminare a datelor se va face în conformitate cu procedura de ștergere.

CAPITOLUL VIII : TRANSFERURI DE DATE

Art. 10(1):Toate transferurile de date din Spațiul Economic European (SEE) către țările din Spațiul Economic Neeuropean (menționate în GDPR ca "țări terțe") sunt ilegale, cu excepția cazului în care există un "nivel adecvat de protecție a drepturilor fundamentale ale persoanele vizate". Transferul de date cu caracter personal în afara SEE este interzis, cu excepția cazului în care se aplică una sau mai multe garanții sau excepții specificate:

(1.1)-*O decizie de adecvare* - Transferul de date cu caracter personal către o ţară terţă sau o organizaţie internaţională se poate realiza atunci când Comisia a decis că ţara terţă, un teritoriu ori unul sau mai multe sectoare specificate din acea ţară terţă sau organizaţia internaţională în cauză asigură un nivel de protecţie adecvat. Transferurile realizate în aceste condiţii nu necesită autorizări speciale. Țările care sunt membre ale Spațiului Economic European (SEE), dar nu și ale UE sunt acceptate ca îndeplinind condițiile unei decizii de adecvare. O listă a țărilor care îndeplinesc în prezent cerințele de adecvare ale Comisiei este publicată în Jurnalul Oficial al Uniunii Europene. http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm

(1.2)-*Privacy Shield* - Dacă Universitateadorește să transfere date personale din UE unei organizații din Statele Unite, ar trebui să verifice dacă organizația este înscrisă în cadrul Privacy Shield la Departamentul de Comerț al S.U.A. Obligația aplicabilă societăților inscrise in Privacy Shield este inclusă în Principiile privind confidentialitatea datelor. Departamentul de Comerț din S.U.A este responsabil pentru gestionarea și administrarea Privacy Shield și pentru asigurarea faptului că organizatiile își respectă angajamentele. Pentru a se putea certifica, companiile trebuie să aibă o politică de confidențialitate în conformitate cu principiile de confidențialitate, de ex. utilizare, stocare și transfer de date personale în conformitate cu un set puternic de reguli și garanții de protecție a datelor. Protecția datelor cu caracter personal se aplică indiferent dacă datele cu caracter personal au legătură cu un rezident al UE sau nu. Organizațiile trebuie să-și reînnoiască "statutul de membru" in cadrul Privacy Shield în fiecare an. Dacă nu, ele nu mai pot primi și utiliza datele cu caracter personal din UE. Evaluarea adecvării de către operatorul de date La evaluarea adecvării, operatorul care transfera date ar trebui să țină seama de următorii factori:

- natura informațiilor transferate;
- țara sau teritoriul de origine și destinația finală a informațiilor;
- modul în care informațiile vor fi utilizate și pentru cât timp;
- legile și practicile țării cesionarului, inclusiv practicile în materie de protecţie a datelor cu caracter personal relevante și obligațiile internaționale.

(1.3)- *Reguli corporatiste obligatorii* : Universitateapoate adopta reguli corporatiste obligatorii aprobate pentru transferul de date în afara UE. Acest lucru necesită prezentarea către Autoritatea de Supraveghere competentă spre aprobare a regulilor pe care încearcă să se bazeze.

(1.4)-*Clauze de contract standard* :Universitatea poate adopta clauze contractuale standard aprobate pentru transferul de date în afara SEE. Dacă se adoptă astfel de clauze, atunci există o recunoaștere automată a gradului de adecvare.

(1.5)- *Excepţii :* În lipsa unei decizii de adecvare, a calitatii de membru a Privacy Shield, a regulilor corporatiste obligatorii și / sau a clauzelor de contract standard, transferul datelor cu caracter personal într-o țară terță sau într-o organizație internațională are loc numai în următoarele condiții:

- persoana vizată și-a dat acordul în mod explicit cu privire la transferul propus, după ce a fost informată cu privire la riscurile posibile ale unor astfel de transferuri, din cauza lipsei unei decizii de adecvare și a garanțiilor adecvate;
- transferul este necesar pentru executarea unui contract între persoana vizată și operator sau implementarea măsurilor precontractuale luate la cererea persoanei vizate;
- transferul este necesar pentru încheierea sau executarea unui contract încheiat în interesul persoanei vizate între operator și o altă persoană fizică sau juridică;

■- transferul este necesar din motive importante de interes public;

■- transferul este necesar pentru stabilirea, exercitarea sau apărarea revendicărilor legale; - transferul este necesar pentru a proteja interesele vitale ale persoanei vizate sau ale altor persoane, în cazul în care persoana vizată nu este capabilă din punct de vedere fizic sau legal să-și dea consimțământul.

CAPITOLUL IX : SISTEM DE EVIDENŢĂ A ACTIVITĂŢILOR DE PRELUCRARE SI CARTOGRAFIEREA DATELOR

Art. 11(1):Universitateaa stabilit un sistem de evidenţă a activităţilor de prelucrare și cartografiere a datelor, ca parte a strategiei sale de abordare a riscurilor și a oportunităților în cadrul proiectului său de conformitate GDPR. Sistemul de evidenţă a activităţilor de prelucrare și cartografierea datelor se refera la:

■- procesele care utilizează date cu caracter personal;

■- sursa datelor personale; - volumul de date corespunzatoare persoanelor vizate;

■- descrierea fiecărui element de date cu caracter personal;

■- activitățile de prelucrare;

■- menținerea inventarului de categorii de date prelucrate;

■- documentarea scopului (scopurilor) pentru care se utilizează fiecare categorie de date cu caracter personal;

■- destinatarii și potențialii beneficiari ai datelor cu caracter personal;

■- rolul Universitătii pe întregul flux de date;

■- sisteme de stocare;

■- orice transfer de date;

■- toate cerințele privind păstrare și stergerea datelor cu caracter personal.

(2)-Managementul Universitătii este conștient de orice riscuri asociate procesării anumitor tipuri de date cu caracter personal.

(2.1)-Universitatea evaluează nivelul riscului pentru procesarea datelor cu caracter personal ale persoanelor vizate. Evaluările impactului privind protecția datelor (DPIA) se efectuează ținând seama de prelucrarea datelor cu caracter personal de către Universitate și de prelucrarea efectuată de alte organizații în numele societății.

(2.2)-Universitatea trebuie să gestioneze, prin luarea de măsuri de protecție rezonabile, orice riscuri identificate de evaluarea riscurilor pentru a reduce probabilitatea neconformității cu această politică.

(2.3)-Având în vedere natura, domeniul de aplicare, contextul şi scopurile prelucrării, 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 şi libertăţile

persoanelor fizice, operatorul efectuează, înaintea prelucrării, o evaluare a impactului operaţiunilor de prelucrare prevăzute asupra protecţiei datelor cu caracter personal. O evaluare unică poate aborda un set de operaţiuni de prelucrare similare care prezintă riscuri ridicate similare.

(2.4)-În cazul în care, rezultatul DPIA releva faptul că Universitatea este pe cale să inițieze o prelucrare a datelor cu caracter personal care ar putea cauza daune și / sau prejudicii persoanelor vizate, decizia de a începe procesarea și de a-și asuma riscurile revine Managementului.

(2.4)-DPO, dacă este numit, sau persoana desemnată intern, este obligat să anunțe către Autoritatea de Supraveghere astfel de situații în cazul în care există motive de îngrijorare semnificative, fie în legătură cu daune și / sau prejudicii, fie în legătură cu volumul de date.

(2.6)-Universitatea are în vedere implementarea de standarde de securitate adecvate [ex: ISO 27001, etc.] și aplicarea lor, pentru a reduce nivelul de risc asociat procesării datelor individuale la un nivel acceptabil.

**REPREZENTANT F.D.M. :**

Prof. univ. dr. Nicolae Postavaru