UNIVERSITATEA SAPIENTIA DIN CLUJ-NAPOCA

REGULAMENT PRIVIND MANAGEMENTUL DATELOR DE CERCETARE

Art. 1. Scopul regulamentului

(1) Scopul prezentului Regulament privind managementul datelor de cercetare (denumit în continuare: Regulament) este de a stabili principii unitare și cerințe minime pentru întregul ciclu de viață al datelor de cercetare generate în cadrul activităților de cercetare-dezvoltare desfășurate la Universitatea Sapientia (denumită în continuare: Universitate).

Ciclul de viață al datelor:

> planificare → colectare → prelucrare → stocare → partajare → păstrare → arhivare → ștergere

(2) Regulamentul asigură integritatea, securitatea și trasabilitatea datelor de cercetare, promovează reutilizarea rezultatelor și transparența științifică, susținând totodată conformitatea cu cerințele finanțatorilor și cu prevederile legale (în special: protecția datelor, drepturile de autor, confidențialitatea, etica cercetării).

Art. 2. Domeniul de aplicare

(1) Domeniul de aplicare personal al Regulamentului vizează angajații Universității (cadre didactice, cercetători, personal administrativ), persoanele aflate în raporturi contractuale, cercetătorii invitați, precum și studenții Universității, în măsura în care gestionează date de cercetare în cadrul unui proiect de cercetare universitar sau prin utilizarea resurselor Universității.

(2) Domeniul de aplicare material al Regulamentului cuprinde toate datele de cercetare și documentația aferentă legate de activitatea de cercetare a Universității, incluzând în special:

- date brute și prelucrate;
- coduri și scripturi;
- baze de date;
- metadate;
- procese-verbale, chestionare, jurnale de măsurători;
- materiale audio și video;
- modele și seturi de date derivate.

Art. 3. Definiții

În sensul prezentului Regulament:

a) Date de cercetare: orice date care sunt colectate, create, prelucrate sau utilizate în cursul cercetării și care servesc la susținerea (validarea) rezultatelor cercetării.

b) Metadate: informații structurate despre date (descriere, metodologie, variabile, drepturi de acces, versiuni, marca temporală).

c) Date sensibile: date cu caracter personal, categorii speciale de date, secrete comerciale, materiale protejate de drepturi de autor sau orice alte date a căror divulgare prezintă riscuri juridice, etice sau de valorificare.

d) Plan de management al datelor (Data Management Plan, DMP): documentul elaborat la începutul proiectului, care stabilește modul de gestionare a datelor, responsabilitățile și regulile de partajare și păstrare a acestora.

Art. 4. § Principii

1) Gestionarea datelor de cercetare este guvernată de următoarele principii:

a) **Conformitatea legală și cu cerințele finanțatorilor:** respectarea GDPR, a drepturilor de autor, a confidențialității, a eticii cercetării și a condițiilor specifice ale proiectelor.

b) **Principiile FAIR (acolo unde este aplicabil):** datele trebuie să fie ușor de găsit (Findable), accesibile (Accessible), interoperabile (Interoperable) și reutilizabile (Reusable).

c) **Securitate și proporționalitate:** aplicarea unor măsuri tehnice și organizatorice adecvate și proporționale cu riscurile identificate.

d) **Integritate și trasabilitate:** asigurarea unui management corespunzător al versiunilor, al jurnalizării, al documentării și al metadatelor.

e) **„Deschidere – atât cât este posibil, închidere – atât cât este necesar”:** promovarea partajării, ținând cont de limitările juridice/etice/de valorificare.

Art. 5. Roluri și responsabilități

În cadrul managementului datelor de cercetare, se aplică următoarele roluri și responsabilități:

Rol	Responsabilități
Director de proiect (PI)	Elaborarea Planului de management al datelor (DMP), alocarea responsabilităților, asigurarea păstrării și partajării datelor.
Custodele datelor (Data Steward)	Responsabil pentru conținutul setului de date (de regulă PI-ul sau un cercetător desemnat).
Administrator de date / Responsabil operațional	Practica zilnică de gestionare a datelor: structură, versiuni, stocare, drepturi de acces.
Responsabil IT / Securitate	Asigurarea infrastructurii, gestionarea accesului, efectuarea copiilor de rezervă (backup) și gestionarea incidentelor.
Responsabil cu protecția datelor (DPO)	Gestionarea datelor cu caracter personal/sensibile, contracte, consimțăminte, acorduri de prelucrare a datelor.

Art. 6. Planul de management al datelor (DMP)

(1) Pentru toate proiectele de cercetare care beneficiază de finanțare externă sau care gestionează date cu caracter personal/sensibile, este obligatorie elaborarea unui Plan de management al datelor (DMP) la lansarea proiectului, acesta urmând să fie actualizat pe parcursul proiectului în funcție de necesități.

(2) Conținutul minim al DMP cuprinde:

- tipurile de date și metodele de colectare;
- formatele și structura fișierelor;
- regimul de stocare și de efectuare a copiilor de rezervă (backup);
- drepturile de acces;
- anonimizarea/pseudonimizarea;
- utilizarea datelor prelucrate în scopuri de publicare;
- partajarea și licențierea;
- perioada de păstrare și arhivarea;
- responsabilitățile și necesarul de resurse.

Art. 7. Colectarea, calitatea și documentarea datelor

(1) În procesul de colectare a datelor, trebuie asigurată documentarea descrierilor metodologice, a definițiilor variabilelor și a protocoalelor de măsurare.

(2) Etapele de prelucrare trebuie să fie reproductibile: codurile/scripturile, parametrii, versiunile software și setările de mediu trebuie consemnate.

(3) Standardizarea regulilor privind denumirea fișierelor și structura folderelor și directoarelor aferente datelor de cercetare este stabilită prin DMP-ul proiectului.

(4) În cazul în care colectarea datelor vizează comunitatea internă a Universității – incluzând în special studenții, cadrele didactice, personalul administrativ sau unitățile structurale ale Universității –, înainte de începerea cercetării, trebuie depusă o cerere de colectare a datelor la Comisia de Etică a Cercetării Științifice a Universității. Cererea trebuie să cuprindă: scopul și metodologia cercetării; categoria și numărul persoanelor vizate; tipul și volumul datelor ce urmează a fi colectate; temeiul juridic al prelucrării datelor și modalitatea de informare a persoanelor vizate; precum și măsurile privind securitatea și păstrarea datelor. Colectarea datelor poate fi inițiată exclusiv în urma aprobării de către Comisia de Etică a Cercetării Științifice.

Art. 8. Stocare, backup și gestionarea accesului

(1) Datele de cercetare vor fi stocate, în măsura posibilităților, pe infrastructura furnizată sau aprobată de Universitate (spațiu de stocare instituțional, soluții *cloud* securizate, spațiu de stocare dedicat proiectului).

(2) Efectuarea periodică a copiilor de rezervă (backup) și documentarea procedurii de recuperare a datelor sunt obligatorii; în cazul datelor sensibile, se va aplica criptarea.

(3) Accesul se asigură pe baza principiului „necesar și suficient”; nivelurile de autorizare sunt: citire – scriere – administrare.

(4) Încărcarea datelor cu caracter personal sau sensibile pe platforme externe este permisă numai în urma verificării de către DPO/serviciul juridic și după încheierea unui acord de prelucrare a datelor corespunzător.

Art. 9. Prelucrarea datelor cu caracter personal și a datelor sensibile

(1) Pentru prelucrarea datelor cu caracter personal este necesar un temei juridic (de exemplu: consimțământul, cercetarea de interes public cu garanții adecvate), iar persoanele vizate trebuie să primească o notă de informare cu privire la prelucrarea datelor.

(2) Trebuie aplicate măsuri de anonimizare sau pseudonimizare, în cazul în care scopul cercetării permite acest lucru.

(3) Accesul și partajarea pot avea loc exclusiv în conformitate cu prevederile GDPR și cu condițiile aprobării etice.

(4) Datele colectate despre studenții Universității nu pot fi divulgate unor părți terțe și nu pot fi transmise către organizații, persoane sau instituții externe, indiferent de scopul colectării datelor sau de identitatea solicitantului. Excepție de la această interdicție pot face exclusiv obligațiile legale sau solicitările din partea instanțelor judecătorești ori a autorităților competente. Rezultatele și concluziile cercetării pot fi publicate, însă datele brute sau datele cu caracter personal care stau la baza acestora nu pot fi transmise mai departe. În vederea publicării, cererea de colectare a datelor – în conformitate cu Art. 7, alin. (4) – trebuie depusă la Comisia de Etică a Cercetării Științifice, aceasta urmând să conțină:

- scopul și metodologia cercetării;
- categoriile și numărul persoanelor vizate;
- tipul și volumul datelor ce urmează a fi colectate;
- temeiul juridic al prelucrării datelor și modalitatea de informare a persoanelor vizate;
- măsurile privind securitatea și păstrarea datelor.

Fac excepție de la cele de mai sus datele colectate direct de la studenți în scopul elaborării lucrărilor de licență, a lucrărilor pentru Conferințele Cercurilor Științifice Studențești (CCȘS/TDK) etc., pentru care nu este necesară aprobarea Comisiei de Etică.

Art. 10. Partajare, publicare, licențiere

(1) Partajarea datelor de cercetare se realizează luând în considerare obiectivele proiectului, cerințele finanțatorilor și limitările juridice sau etice.

(2) În cazul partajării publice, sunt preferate identificatorii persistenți (de ex. DOI), metadatele corespunzătoare și licențierea clară (de ex. Creative Commons), în măsura în care drepturile permit acest lucru.

(3) În cazul în care se preconizează obținerea unei protecții prin proprietate industrială sau valorificarea rezultatelor, momentul partajării publice se va stabili în conformitate cu Regulamentul de proprietate intelectuală al Universității și cu deciziile structurii organizatorice competente a Universității.

Art. 11. Păstrarea, arhivarea și eliminarea datelor

(1) Perioada de păstrare a datelor este stabilită prin DMP-ul proiectului, luând în considerare obligațiile față de finanțatori și bunele practici specifice domeniului de cercetare.

(2) În procesul de arhivare, trebuie asigurată lizibilitatea pe termen lung a datelor (fiind preferate formatele deschise), precum și stabilirea clară a condițiilor de acces.

(3) Eliminarea sau ștergerea datelor se realizează în mod documentat, numai după îndeplinirea cerințelor legale și a obligațiilor față de finanțatori.

Art. 12. Gestionarea incidentelor

(1) În cazul în care există suspiciuni de breșă de securitate a datelor, acces neautorizat, pierdere de date sau compromitere a integrității acestora, trebuie notificați fără întârziere responsabilul IT/de securitate și – în cazul în care sunt vizate date cu caracter personal – responsabilul cu protecția datelor (DPO) la adresa de e-mail: dataprotect@sapientia.ro.

(2) Pentru fiecare incident trebuie întocmit un proces-verbal și trebuie luate măsurile necesare de remediere și de prevenire.

Art. 13. Instruire și suport

(1) Universitatea urmărește ca cercetătorii și studenții să beneficieze de informare și instruire periodică privind principiile managementului datelor, bunele practici și procedurile aferente.

(2) Șabloanele DMP și soluțiile recomandate (spațiu de stocare, controlul versiunilor, instrumente de anonimizare) trebuie puse la dispoziție la nivel instituțional.

Art. 14. Dispoziții finale

(1) Prezentul Regulament intră în vigoare la data publicării, după aprobarea acestuia de către Senatul Universității.

(2) Procedurile detaliate de implementare a Regulamentului (șablonul DMP, cererile de acces, ghidul privind stocarea datelor) pot fi emise ca documente separate.

(3) Revizuirea Regulamentului are loc cel puțin o dată la doi ani sau, în mod extraordinar, în cazul unor modificări legislative ori ale cerințelor finanțatorilor.

Prezentul regulament a fost aprobat prin Hotărârea Senatului nr. 3108 din data de 27.03.2026.

Conf. univ. dr. LÁZÁR Ede

Președintele Senatului

Avizat, ZSIGMOND Erika, consilier juridic