APROBAT

la şedinţa Biroului Senatului Academiei „Ştefan cel Mare”. Proces-verbal nr. 1 din 14.08.2026

ACADEMIA „ŞTEFAN CEL MARE”
A MINISTERULUI AFACERILOR INTERNE

POLITICA DE PROTECȚIE A DATELOR CU CARACTER PERSONAL PRELUCRATE ÎN CADRUL ACADEMIEI „ŞTEFAN CEL MARE” A MINISTERULUI AFACERILOR INTERNE

Chişinău 2026

I. DISPOZIȚII GENERALE

1. Politica de protecție a datelor cu caracter personal prelucrate în cadrul Academiei „Ştefan cel Mare” a MAI (în continuare – Politica de protecție) instituie un cadru eficient, responsabil și transparent pentru a asigura conformitatea prelucrării datelor cu caracter personal cu principiile prevăzute de actele internaționale - Declaraţia universală a drepturilor omului, Convenția europeană a drepturilor omului, Convenţia pentru protecţia persoanelor referitor la prelucrarea automatizată a datelor cu caracter personal, 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 și ale celor naţionale: Constituţia Republicii Moldova, Legea nr. 195/2054 privind protecţia datelor cu caracter personal (în continuare – Legea nr. 195/2024), Legea nr. 148/2023 privind accesul la informaţiile de interes public și alte acte normative.

2. Academia „Ștefan cel Mare” a MAI (în continuare - Academia) se angajează să aplice principiile de protecție a datelor, bazându-se pe legalitate, transparență și integritate, astfel încât prelucrarea datelor cu caracter personal să fie desfășurată exclusiv pentru scopuri clare și legitime. În acest context, Academia va depune eforturile necesare pentru a asigura că toate persoanele implicate în prelucrarea datelor sunt conștiente de responsabilitățile lor și sunt instruite pentru a respecta măsurile și cerințele legale privind protecția datelor.

3. Politica de protecție se aplică activităților de prelucrare a datelor cu caracter personal efectuate de către personalul unităților structurale ale Academiei, care prelucrează datele cu caracter personal în numele Academiei.

4. Prezenta Politică de protecție asigură faptul că:

4.1. personalul Academiei cunoaște modul în care trebuie prelucrate datele cu caracter personal;

4.2. Academia oferă garanții de prelucrare a datelor personale cu respectarea drepturilor persoanelor vizate;

4.3. protejează împotriva riscurilor de încălcare a securității datelor cu caracter personal și a altor încălcări ale legislației privind protecția datelor.

5. Politica de protecție se aplică tuturor datelor cu caracter personal prelucrate în orice format, cu sau fără utilizarea de mijloace automatizate, prin operațiuni sau seturi de operațiuni precum 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.

6. Personalul Academiei, precum și terții, care prelucrează datele cu caracter personal în numele Academiei, trebuie să cunoască și să aplice regulile stabilite prin prezenta Politică de protecție. Conducătorii au responsabilitatea de a asigura că subalternii respectă Politica de protecție atunci când prelucrează datele cu caracter personal și de a urmări conformitatea activităților de prelucrare, care intră în responsabilitatea lor, cu procedurile, procesele, metodologiile implementate pentru asigurarea protecției datelor cu caracter personal.

7. Politica de protecție este aprobată de către Senatul Academiei, care activează în baza propriului regulament de organizare și funcționare, elaborat în conformitate cu regulamentul-cadru aprobat de Ministerul Educației, Culturii și Cercetării.

8. Politica de protecție este revizuită periodic și ori de câte ori apar modificări semnificative, inclusiv în următoarele situații:

8.1. adaptarea Politicii de protecție pentru a respecta noile reglementări naționale sau europene în cazul modificărilor legislative;

8.2. apariția unui incident de securitate major care afectează un număr semnificativ de date cu caracter personal;

8.3. aplicarea recomandărilor CNPDCP.

9. Politica de protecție, în mod obligatoriu, va fi adusă la cunoștință, sub semnătură, tuturor angajaților responsabili de prelucrarea datelor cu caracter personal, inclusiv la operarea modificărilor necesare asigurării nivelului adecvat de protecție a datelor cu caracter personal.

10. Termenii utilizați în Politica de protecție se definesc în felul următor:

10.1. *operator* - entitatea care, singură sau împreună cu altele, stabilește scopurile și mijloacele prelucrării ori căreia acestea îi sunt stabilite prin acte normative, în condițiile legii;

10.2. *operatori asociați* - atunci când doi sau mai mulți operatori stabilesc împreună scopurile și mijloacele prelucrării. Responsabilitățile acestora se stabilesc potrivit legislației aplicabile, dacă nu sunt deja prevăzute de acte normative;

10.3. *persoană împuternicită de operator* - entitatea care prelucrează date cu caracter personal în numele operatorului și numai în limitele instrucțiunilor documentate ale acestuia, cu excepția situațiilor în care actele normative impun o anumită prelucrare;

10.4. *utilizator* - persoana autorizată care, în exercitarea atribuțiilor de serviciu, efectuează operațiuni asupra datelor cu caracter personal prin intermediul unui sistem informațional, al unui sistem de evidență manual sau al altui mijloc autorizat de prelucrare.

II. PRINCIPIILE DE PRELUCRARE A DATELOR

11. Toate informațiile care conțin date cu caracter personal trebuie să fie protejate împotriva accesului neautorizat, a pierderii sau distrugerii accidentale, împotriva modificării sau dezvăluirii ilegale.

12. Prelucrarea datelor cu caracter personal se bazează pe următoarele principii:

12.1. **legalitatea, echitatea și transparența** – prelucrarea datelor cu caracter personal se realizează numai în baza unui temei legal, iar persoanele vizate sunt informate într-o manieră clară și transparentă despre scopul și modul în care datele lor vor fi utilizate, cu excepția cazurilor în care informarea este amânată sau omisă în conformitate cu legea.

12.2. **limitarea scopului de prelucrare** – colectarea urmează a fi realizată în scopuri determinate, explicite și legitime, iar ulterior să nu fie admisă prelucrarea într-un mod incompatibil cu aceste scopuri. Prelucrarea ulterioară a

datelor cu caracter personal în scopuri statistice, de cercetare istorică sau științifică nu este considerată incompatibilă cu scopul colectării dacă se efectuează cu respectarea prevederilor legale și cu respectarea garanțiilor privind prelucrarea datelor cu caracter personal, prevăzute de normele ce reglementează activitatea statistică, cercetarea istorică și cea științifică;

12.3. **reducerea la minimum a datelor** – datele colectate trebuie să fie adecvate, relevante și limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate;

12.4. **exactitatea datelor** – asigurarea colectării unor date exacte și, dacă este necesar, actualizării acestora. Datele cu caracter personal inexacte, având în vedere scopurile pentru care sunt prelucrate, se șterg sau rectifică fără întârziere;

12.5. **limitarea perioadei de stocare** – stocarea într-o formă care să permită identificarea persoanelor vizate pe o perioadă necesară îndeplinirii scopurilor în care sunt prelucrate. Datele cu caracter personal pot fi stocate pe perioade mai lungi în măsura în care acestea vor fi prelucrate exclusiv în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice, cu condiția existenței unor garanții adecvate, sub rezerva punerii în aplicare a măsurilor de ordin tehnic și organizatoric în vederea garantării drepturilor și libertăților persoanelor vizate (principiul limitării legate de stocare).

12.6. **integritatea și confidențialitatea** – prelucrarea datelor se realizează într-un mod care asigură securitatea adecvată a acestora, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, distrugerii sau deteriorării accidentale, prin luarea de măsuri tehnice sau organizatorice corespunzătoare.

III. RESPONSABILUL CU PROTECȚIA DATELOR

13. Operatorul și, după caz, persoana împuternicită de operator desemnează responsabilul cu protecția datelor, asigurând implicarea corespunzătoare și în timp util a responsabilului cu protecția datelor în chestiunile care privesc protecția datelor, accesul acestuia la informațiile și operațiunile necesare, resursele pentru îndeplinirea sarcinilor și posibilitatea menținerii cunoștințelor de specialitate.

14. Responsabilul cu protecția datelor își îndeplinește atribuțiile cu independența prevăzută de lege, având cel puțin următoarele sarcini:

14.1. informarea și consilierea conducerea și personalul operatorului sau a persoanei împuternicite de operator cu privire la obligațiile care le revin;

14.2. monitorizarea respectării Legii nr. 195/2024, a altor acte normative referitoare la protecția datelor, precum și a politicilor operatorului sau ale persoanei împuternicite de operator privind protecția datelor cu caracter personal;

14.3. acordarea de consiliere, la cerere, în ceea ce privește evaluarea impactului asupra protecției datelor și monitorizarea funcționării acesteia, în conformitate cu art. 35 din Legea nr. 195/2024;

14.4. participarea la analiza proiectelor de acte;

14.5. monitorizarea, prin verificări tematice sau prin sondaj, a legalității accesărilor și aplicării măsurilor de protecție a datelor, fără a substitui

competențele conducerii operatorului, administratorilor sistemelor sau ale altor structuri competente potrivit legislației;

14.6. oferirea de consiliere asupra obligațiilor de notificare și informare în cazul în care este informat cu privire la încălcările securității datelor;

14.7. participarea la instruirea personalului și la activitățile de conștientizare;

14.8. cooperarea cu CNPDCP, și îndeplinirea rolului de punct de contact în chestiunile privitoare la prelucrare, inclusiv consultarea prealabilă prevăzută la art.36 din Legea nr. 195/2024.

15. În îndeplinirea sarcinilor sale, responsabilul cu protecția datelor poate solicita unităților structurale informații și documente relevante pentru monitorizarea conformității.

16. Persoanele vizate pot contacta responsabilul cu protecția datelor cu privire la toate chestiunile legate de prelucrarea datelor lor cu caracter personal și de exercitarea drepturilor lor în temeiul Legii nr. 195/2024.

IV. EVIDENȚA ACTIVITĂȚILOR DE PRELUCRARE A DATELOR

17. Academia prelucrează date cu caracter personal în următoarele scopuri:

17.1. specifice domeniului de activitate:

17.1.1. prelucrarea datelor pentru furnizarea informațiilor de interes public;

17.1.2. colectarea datelor prin intermediul formularului de contact, prin e-mail, telefon și/sau fax referitoare la furnizarea serviciilor publice;

17.1.3. executarea unei operațiuni de plată;

17.1.4. soluționare petiții/sesizări, prelucrarea oricăror alte solicitări primite direct sau online, inclusiv formularea răspunsurilor la solicitări;

17.1.5. încheierea și executarea contractelor;

17.1.6. planificarea, organizarea și monitorizarea procedurilor legate de procesul de învățământ a studenților în cadrul Facultății DAOSP; evidența și monitorizarea reușitei academice a studenților Facultății DAOSP;

17.1.7. planificarea, organizarea și monitorizarea procedurilor legate de procesul de formare profesională inițială, continuă și managerială a funcționarilor publici cu statut special și carabinierilor;

17.1.8. organizarea și desfășurarea activităților de formare profesională tehnică;

17.1.9. asigurarea procesului de evaluare psihologică a candidaților și angajaților MAI;

17.1.10. promovarea unor acțiuni și evenimente;

17.1.11. protecția și securitatea persoanelor și a bunurilor;

17.1.12. protecție și asistență socială;

17.1.13. reprezentarea în instanțele judecătorești, autoritățile/instituțiile publice și alte organizații;

17.1.14. prestarea serviciilor medicale pacienților în vederea derulării programelor naționale de sănătate;

17.1.15. prelucrări statistice și în scop de cercetare științifică;

17.1.16. arhivare;

17.1.17. îndeplinirea altor obligații legale specifice domeniului de activitate;

17.2. administrative:

17.2.1. gestiune logistică, economică și financiară;

17.2.2. gestiunea resurselor umane (recrutare, salarizare, evaluare profesională etc.);

17.2.3. controlul activităților;

17.2.4. monitorizarea și supravegherea accesului în sediu și a securității bunurilor și persoanelor;

17.2.5. implicarea în diferite activități polițienești sub egida MAI și/sau IGP;

17.2.6. gestionarea sistemelor informaționale și a comunicațiilor interne.

18. Pentru asigurarea administrării eficiente și transparente a operațiunilor de prelucrare a datelor cu caracter personal, Academia, în calitate de operator, păstrează o evidență a activităților de prelucrare desfășurate sub responsabilitatea lor, care cuprinde următoarele informații:

18.1. numele și datele de contact ale Academiei, după caz, ale operatorului asociat, ale reprezentantului Academiei și ale responsabilului cu protecția datelor;

18.2. scopurile prelucrării;

18.3. o descriere a categoriilor de persoane vizate și a categoriilor de date cu caracter personal;

18.4. categoriile de destinatari cărora le-au fost sau le vor fi divulgate datele cu caracter personal, inclusiv destinatarii din alte state sau din organizații internaționale;

18.5. dacă este cazul, transferurile de date cu caracter personal către un alt stat sau către o organizație internațională, inclusiv identificarea acestui stat sau a organizației internaționale respective.

18.6. dacă este posibil, termenele-limită preconizate pentru ștergerea diferitelor categorii de date;

18.7. dacă este posibil, o descriere generală a măsurilor tehnice și organizatorice de securitate.

19. În calitate de persoană împuternicită de operator, Academia (după caz, reprezentantul Academiei) păstrează o evidență a tuturor categoriilor de activități de prelucrare desfășurate în numele operatorului, care cuprinde:

19.1. numele și datele de contact ale Academiei și ale fiecărui operator în numele căruia acționează Academia, precum și, după caz, ale reprezentantului operatorului sau ale reprezentantului Academiei;

19.2. categoriile activităților de prelucrare desfășurate în numele fiecărui operator;

19.3. dacă este cazul, transferurile da date cu caracter personal către un alt stat sau către o organizație internațională, inclusiv identificarea acestui stat sau a organizației internaționale respective;

19.4. dacă este posibil, o descriere generală a măsurilor tehnice și organizatorice de securitate.

20. Academia, după caz, reprezentantul Academiei, în calitate de operator sau persoană împuternicită de operator, țin în scris, inclusiv în format electronic, evidențele menționate la punctele 18 și 19 și le pun la dispoziția CNPDCP la cererea acestuia.

V. TRANSPARENȚA PRELUCRĂRII DATELOR

21. În calitate de operator, Academia ia măsuri adecvate pentru a furniza persoanei vizate orice informații menționate la punctele 23 și 24 și orice comunicări în temeiul art.art. 15–22 și 34 din Legea nr. 195/2024, referitoare la prelucrare, într-o formă concisă, transparentă, inteligibilă și ușor accesibilă, utilizând un limbaj clar și simplu, în mod gratuit, cu excepția cazurilor prevăzute în art. 12 alin. (5) din Legea nr. 195/2024. 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.

22. Academia furnizează persoanei vizate informații privind acțiunile întreprinse în urma unei cereri întemeiate pe art.art. 15–22 din Legea nr. 195/2024 cu privire la protecția datelor cu caracter personal, fără întârzieri nejustificate, dar în cel mult o lună de la primirea cererii. Această perioadă poate fi prelungită cu două luni atunci când este necesar, ținându-se cont de complexitatea și numărul cererilor. Academia 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 înaintează o cerere în format electronic, informațiile sunt furnizate în format electronic dacă este posibil, cu excepția cazului în care persoana vizată solicită un alt format.

23. Dacă nu ia măsuri cu privire la cererea persoanei vizate, Academia 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 la CNPDCP și de a depune o cerere de chemare în judecată.

24. În cazul în care datele cu caracter personal referitoare la o persoană vizată sunt colectate de la aceasta, Academia, în momentul obținerii acestor date, furnizează persoanei vizate următoarele informații:

24.1. identitatea și datele de contact ale Academiei și, după caz, ale reprezentantului acesteia;

24.2. datele de contact ale responsabilului cu protecția datelor, după caz;

24.3. scopurile în care sunt prelucrate datele cu caracter personal, precum și temeiul juridic al prelucrării;

24.4. interesele legitime urmărite de operator sau de o parte terță, în cazul în care 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, fapt care necesită protejarea datelor cu caracter personal.

24.5. destinatarii sau categoriile de destinatari ai datelor cu caracter personal;

24.6. Pe lîngă informațiile menționate la punctele 24.1. - 24.5., în momentul în care datele cu caracter personal sunt obținute, Academia furnizează persoanei vizate următoarele informații suplimentare necesare pentru a asigura o prelucrare echitabilă și transparentă:

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

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

24.6.3. dreptul de a depune o plângere la CNPDCP;

24.6.4. dacă furnizarea de date cu caracter personal reprezintă o obligație legală sau contractuală ori 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;

24.6.5. existența unui proces decizional automatizat, inclusiv crearea de profiluri, precum și, cel puțin în cazurile respective, informații pertinente privind logica utilizată și privind importanța și consecințele preconizate ale unei astfel de prelucrări pentru persoana vizată.

25. În cazul în care datele cu caracter personal nu au fost obținute de la persoana vizată, operatorul furnizează persoanei vizate următoarele informații:

25.1. identitatea și datele de contact ale operatorului și, după caz, ale reprezentantului acestuia;

25.2. datele de contact ale responsabilului cu protecția datelor, după caz;

25.3. scopurile în care sunt prelucrate datele cu caracter personal, precum și temeiul juridic al prelucrării;

25.4. categoriile de date cu caracter personal vizate;

25.5. destinatarii sau categoriile de destinatari ai datelor cu caracter personal, după caz.

25.6. Pe lângă informațiile menționate la punctele 24.1 – 24.5., operatorul furnizează persoanei vizate următoarele informații necesare pentru a asigura o prelucrare echitabilă și transparentă în ceea ce privește persoana vizată:

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

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

25.6.3. dreptul de a depune o plângere la Centru;

25.6.4. sursa din care provin datele cu caracter personal și, după caz, dacă acestea provin din surse disponibile public;

25.6.5. existența unui proces decizional automatizat, inclusiv crearea de profiluri, precum și, cel puțin în cazurile respective, informații pertinente privind logica utilizată și privind importanța și consecințele preconizate ale unei astfel de prelucrări pentru persoana vizată.

26. Operatorul furnizează informațiile menționate la punctele 24 și 25:

26.1. într-un termen rezonabil după obținerea datelor cu caracter personal, dar nu mai mare de o lună, ținând cont de circumstanțele specifice în care sunt prelucrate datele cu caracter personal;

26.2. dacă datele cu caracter personal urmează să fie utilizate pentru comunicarea cu persoana vizată – cel târziu în momentul primei comunicări cu persoana vizată respectivă;

sau

26.3. dacă se intenționează divulgarea datelor cu caracter personal către un alt destinatar – cel târziu la data la care acestea sunt divulgate pentru prima oară.

27. Prevederile punctelor 24 și 25 nu se aplică dacă și în măsura în care:

27.1. persoana vizată deține deja informațiile;

27.2. furnizarea acestor informații se dovedește a fi imposibilă sau ar implica eforturi disproporționate, în special în cazul prelucrării în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice;

27.3. obținerea sau divulgarea datelor este prevăzută în mod expres în actele normative care stabilesc măsuri adecvate pentru a proteja interesele legitime ale persoanei vizate; sau

27.4. în cazul în care datele cu caracter personal trebuie să rămână confidențiale în temeiul unei obligații legale de secret profesional reglementate de actele normative, inclusiv al unei obligații legale de a păstra secretul.

VI. PRELUCRAREA DATELOR CU CARACTER PERSONAL

28. Prelucrarea datelor cu caracter personal reprezintă orice operațiune sau serie de operațiuni care se efectuează asupra datelor cu caracter personal prin mijloace automatizate sau neautomatizate, cum ar fi colectarea, înregistrarea, organizarea, stocarea, păstrarea, restabilirea, adaptarea ori modificarea, extragerea, consultarea, utilizarea, dezvăluirea prin transmitere, diseminarea sau în orice alt mod, alăturarea ori combinarea, blocarea, ștergerea sau distrugerea.

29. Prelucrarea datelor cu caracter personal de către personalul Academiei se bazează pe un temei legal clar, identificat înainte de colectarea acestora. Serviciul responsabil de protecția datelor din cadrul Academiei evaluează baza legală și scopurile prelucrării pentru fiecare activitate, conform prevederilor Legii nr. 195/2024, iar personalul implicat în prelucrarea datelor cu caracter personal, înainte de inițierea oricărei prelucrări, va identifica temeiul legal corespunzător prelucrării.

30. Prelucrarea este legală numai dacă și în măsura în care se îndeplinește cel puțin una dintre următoarele condiții:

30.1. persoana vizată și-a dat consimțământul pentru prelucrarea datelor sale cu caracter personal pentru unul sau mai multe scopuri specifice;

30.2. prelucrarea este necesară pentru executarea unui contract la care persoana vizată este parte sau pentru luarea unor măsuri la cererea persoanei vizate înainte de încheierea unui contract;

30.3. prelucrarea este necesară în vederea îndeplinirii unei obligații legale care îi revine operatorului;

30.4. prelucrarea este necesară pentru a proteja interesele vitale ale persoanei vizate sau ale altei persoane fizice;

30.5. prelucrarea este necesară pentru îndeplinirea unei sarcini efectuate în interes public sau în exercitarea unei autorități oficiale cu care este învestit operatorul;

30.6. 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, fapt care necesită protejarea datelor cu caracter personal.

31. Datele cu caracter personal pot fi prelucrate în temeiul pct. 30.5. în cazul în care prelucrarea este necesară pentru:

31.1. îndeplinirea unei sarcini de interes public care reiese din actele normative;

31.2. exercitarea de către operator a funcțiilor sau atribuțiilor prevăzute de actele normative.

32. Prelucrarea categoriilor speciale de date cu caracter personal este interzisă, cu excepția cazurilor în care:

32.1. 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 actele normative prevăd că această interdicție nu poate fi înlăturată prin consimțământul persoanei vizate;

32.2. prelucrarea este necesară pentru îndeplinirea obligațiilor sau exercitarea drepturilor 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 actele normative ori de un contract colectiv de muncă care prevede garanții adecvate pentru drepturile fundamentale și interesele persoanei vizate;

32.3. 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;

32.4. prelucrarea este efectuată în cadrul activităților lor legitime și cu garanții adecvate de către un partid politic, sindicat, cult religios sau orice alt organism fără scop lucrativ cu specific politic, filozofic, religios sau sindical, cu condiția ca prelucrarea să se refere numai la membrii sau la foștii membri ai organismelor respective sau la persoane cu care acestea au contacte permanente în legătură cu scopurile lor, precum și ca datele cu caracter personal sa nu fie comunicate terților fără consimțământul persoanelor vizate;

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

32.6. prelucrarea este necesară pentru stabilirea, exercitarea sau apărarea unui drept într-o procedură administrativă, judiciară sau extrajudiciară ori când instanțele judecătorești acționează în exercițiul funcției lor judiciare;

32.7. prelucrarea este necesară din motive de interes public major, în temeiul actelor normative, care sunt proporționale cu obiectivul urmărit, respectă esența dreptului la protecția datelor și prevăd măsuri corespunzătoare și specifice pentru protejarea drepturilor fundamentale și a intereselor persoanei vizate;

32.8. prelucrarea este necesară în scopuri legate de medicina preventivă sau medicina muncii, de evaluarea capacității de muncă a angajatului, de stabilirea unui diagnostic medical, de prestarea asistenței medicale sau sociale ori a unui tratament medical sau de gestionarea sistemelor și serviciilor de sănătate ori de asistență socială, în temeiul actelor normative sau în temeiul unui contract încheiat cu un prestator de servicii de sănătate și cu condiția că datele respective sunt prelucrate de către sau sub responsabilitatea unui profesionist supus obligației de păstrare a secretului profesional în temeiul actelor normative sau de către o altă persoană supusă unei obligații de confidențialitate în temeiul actelor normative.

33. Prelucrarea datelor cu caracter personal referitoare la condamnări penale și infracțiuni sau la măsuri de securitate conexe în temeiul pct. 30 se efectuează numai sub controlul unei autorități publice sau atunci când prelucrarea este autorizată de actele normative care prevăd garanții adecvate pentru drepturile și libertățile persoanelor vizate.

34. În cazul în care scopurile pentru care un operator prelucrează date cu caracter personal nu necesită sau nu mai necesită identificarea de către operator a unei persoane vizate, operatorul nu are obligația de a păstra, a obține sau a prelucra informații suplimentare pentru a identifica persoana vizată, exclusiv în scopul respectării Legii nr. 195/2024.

35. Datele cu caracter personal sunt păstrate într-o formă care permite identificarea persoanelor vizate pe o perioadă ce nu depășește perioada necesară îndeplinirii scopurilor în care sunt prelucrate datele. Durata stocării este stabilită în conformitate cu normele legale și cerințele interne ale MAI.

36. La expirarea perioadei de stocare, datele vor fi șterse sau distruse în condiții de siguranță, utilizând metode corespunzătoare de securitate, fie prin ștergerea permanentă a înregistrărilor electronice, fie prin distrugerea fizică a suporturilor.

37. Datele cu caracter personal deținute de Academie pot fi dezvăluite în condițiile Legii nr. 148/2023 privind accesul la informațiile de interes public, cu excepția categoriilor de date cu caracter personal prevăzute la art. 9 alin. (1) din Legea nr. 195/2024, cu respectarea principiilor de protecție a datelor cu caracter personal. Toate dezvăluirile sunt documentate pentru a asigura trasabilitatea.

38. Datele cu caracter personal pot fi transmise către instituțiile competente ale altor state sau organisme de cooperare polițienească și juridică internațională în condițiile prevederilor cap. V din Legea nr. 195/2024.

VII. SECURITATEA DATELOR CU CARACTER PERSONAL

39. Academia prelucrează datele cu caracter personal astfel încât să asigure un nivel adecvat de securitate, raportat la riscurile asociate. Protecția împotriva prelucrării neautorizate sau ilegale, pierderii, distrugerii sau deteriorării accidentale este garantată prin implementarea unor măsuri tehnice și organizatorice adecvate pentru a garanta și a fi în măsură să demonstreze că prelucrarea se efectuează conform Legii nr. 195/2024, prin asigurarea:

39.1. pseudonimizării și criptării datelor cu caracter personal;

39.2. capacității de a asigura confidențialitatea, integritatea, disponibilitatea și reziliența sistemelor și serviciilor de prelucrare;

39.3. capacității de a restabili disponibilitatea datelor cu caracter personal și accesul la acestea în timp util în cazul în care are loc un incident de natură fizică sau tehnică;

39.4. unui proces necesar pentru testarea, evaluarea și aprecierea periodică a eficacității măsurilor tehnice și organizatorice pentru a garanta securitatea prelucrării.

40. Pseudonimizarea presupune prelucrarea datelor cu caracter personal astfel încât acestea să nu mai poată fi atribuite unei anumite 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.

41. Confidențialitatea datelor cu caracter personal se asigură prin următoarele măsuri:

41.1. controlul accesului la sistemele informatice, bazat pe conturi individuale de utilizator și autentificare strictă;

41.2. monitorizarea accesărilor și înregistrarea activităților care implică prelucrarea datelor cu caracter personal;

41.3. securitatea fizică a spațiilor unde se desfășoară activități de prelucrare a datelor, incluzând acces controlat și monitorizare video;

41.4. instruirea periodică a personalului în ceea ce privește normele de protecție a datelor cu caracter personal pentru a crește nivelul de conștientizare privind riscurile de securitate;

41.5. introducerea unor proceduri stricte de autorizare pentru transferul datelor către terți, incluzând acorduri contractuale clare cu aceștia.

42. Integritatea datelor cu caracter personal se asigură prin:

42.1. realizarea de backup-uri regulate și sigure ale bazelor de date;

42.2. implementarea unor soluții de protecție antivirus și de detectare a intruziunilor;

42.3. utilizarea aplicațiilor software testate înainte de implementare, în medii dedicate dezvoltării și testării;

42.4. protejarea echipamentelor tehnologiilor informaționale împotriva amenințărilor externe prin configurări de securitate, firewall-uri și actualizări regulate ale software-ului.

43. Disponibilitatea datelor cu caracter personal se asigură prin:

43.1. protejarea centrelor de date împotriva incendiilor, întreruperilor de curent electric și altor incidente tehnice;

43.2. restaurarea rapidă a bazelor de date care se realizează datorită existenței copiilor de rezervă și a procedurilor automate de recuperare;

43.3. existența sistemelor critice redundante, care asigură funcționarea lor continuă în caz de defecțiuni.

44. La evaluarea nivelului adecvat de securitate se ține cont, în special, de riscurile prezentate de prelucrare, generate în special, în mod accidental sau ilegal,

de distrugerea, pierderea, modificarea, divulgarea neautorizată sau accesul neautorizat la datele cu caracter personal transmise, stocate sau prelucrate într-un alt mod.

45. Operatorul și persoana împuternicită de operator iau măsuri pentru a asigura faptul că orice persoană fizică care acționează sub autoritatea operatorului sau a persoanei împuternicite de operator și care are acces la date cu caracter personal nu le prelucrează decât în baza instrucțiunilor operatorului, cu excepția cazului în care actele normative impun prelucrarea datelor cu caracter personal.

46. Pentru a preveni riscurile de acces neautorizat la date, Academia aplică măsuri stricte privind utilizarea stațiilor de lucru și a aplicațiilor informatice:

46.1. stațiile de lucru și aplicațiile informatice care gestionează date cu caracter personal sunt protejate prin parole complexe și autentificare multifactorială;

46.2. angajații sunt instruiți să nu lase stațiile de lucru nesupravegheate atunci când au date cu caracter personal deschise și să folosească ecrane de protecție pentru a preveni vizualizarea datelor de către persoane neautorizate;

46.3. toate acțiunile utilizatorilor sunt logate și monitorizate pentru a asigura trasabilitatea activităților și pentru a identifica eventuale încălcări ale politicilor de securitate.

47. Supravegherea prin mijloace video este realizată de Academie pentru a asigura securitatea și controlul accesului în spațiile gestionate (securitatea bunurilor, siguranța persoanelor – angajați ai Academiei sau vizitatori, precum și a proprietăților și informațiilor deținute) și nu se folosește pentru monitorizarea activității angajaților sau prezenței acestora la locul de muncă, iar datele înregistrate nu sunt destinate dezvăluirii terților.

VIII. EVALUAREA IMPACTULUI ASUPRA PROTECȚIEI DATELOR CU CARACTER PERSONAL. CONSULTAREA PREALABILĂ

48. Având în vedere natura, domeniul de aplicare, contextul și 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 și libertățile persoanelor fizice, operatorul efectuează, înaintea prelucrării, o evaluare a impactului operațiunilor de prelucrare preconizate asupra protecției datelor cu caracter personal. O singură evaluare poate aborda un set de operațiuni de prelucrare similare care prezintă riscuri ridicate similare.

49. La realizarea unei evaluări a impactului asupra protecției datelor cu caracter personal, operatorul solicită avizul responsabilului cu protecția datelor.

50. Evaluarea conține cel puțin:

50.1. o descriere sistematică a operațiunilor de prelucrare preconizate și a scopurilor prelucrării, inclusiv, după caz, interesul legitim urmărit de operator;

50.2. o evaluare a necesității și proporționalității operațiunilor de prelucrare în legătură cu aceste scopuri;

50.3. o evaluare a riscurilor pentru drepturile și libertățile persoanelor vizate menționate la pct. 48; și

50.4. măsurile preconizate în vederea abordării riscurilor, inclusiv garanțiile, măsurile de securitate și mecanismele menite să asigure protecția datelor cu caracter personal și să demonstreze conformitatea cu dispozițiile Legii nr. 195/2024, luând în considerare drepturile și interesele legitime ale persoanelor vizate și ale altor persoane interesate.

51. Operatorul consultă CNPDCP, conform art. 36 din Legea nr. 195/2024, înainte de prelucrare atunci când evaluarea impactului asupra protecției datelor cu caracter personal indică faptul că prelucrarea ar genera un risc ridicat în absența unor măsuri luate de operator pentru atenuarea riscului.

IX. GESTIONAREA INCIDENTELOR DE SECURITATE

52. Persoana împuternicită de operator informează operatorul fără întârzieri nejustificate după ce ia cunoștință de o încălcare, potrivit obligațiilor legale și contractuale aplicabile. Respectiva notificare cel puțin:

52.1. descrie caracterul încălcării securității datelor cu caracter personal, inclusiv, atunci când 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;

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

52.3. descrie consecințele probabile ale încălcării securității datelor cu caracter personal;

52.4. descrie măsurile 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 efecte negative.

53. Operatorul evaluează încălcarea cu participarea, a structurii în care s-a produs evenimentul, a responsabilului cu protecția datelor, a STI/administratorului sistemului, a structurii de securitate și după caz a altor specialiști relevanți.

54. Decizia privind notificarea Centrului și informarea persoanelor vizate aparține operatorului, iar responsabilul cu protecția datelor oferă consiliere și monitorizează respectarea cerințelor, fără a substitui decizia operatorului. Dacă este posibil, notificarea se face în termen de cel mult 72 de ore de la data la care a luat cunoștință de aceasta, cu excepția cazului în care încălcarea este puțin susceptibilă să genereze un risc pentru drepturile și libertățile persoanelor fizice. În cazul în care nu se face în termen de 72 de ore, notificarea este însoțită de o explicație motivată a întârzierii.

55. 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.

56. Operatorul 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.

57. În cazul în care încălcarea securității datelor cu caracter personal este susceptibilă să genereze un risc ridicat pentru drepturile și libertățile persoanelor

fizice, operatorul informează persoana vizată, fără întârzieri nejustificate cu privire la această încălcare.

58. Informarea menționată la pct. 57 include: o descriere, într-un limbaj clar și simplu, a caracterului încălcării securității datelor cu caracter personal, precum și, cel puțin, informațiile și măsurile prevăzute la pct. 52.2 – 52.4.

59. Informarea persoanei vizate prevăzută la pct. 57 nu este necesară în cazul în care este îndeplinită una dintre următoarele condiții:

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

59.2. operatorul a luat măsuri ulterioare prin care se asigură că riscul ridicat pentru drepturile și libertățile persoanelor vizate menționat la pct. 57 nu mai este susceptibil să se materializeze;

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

60. În cazul în care operatorul nu a informat persoana vizată despre încălcarea securității datelor cu caracter personal, CNPDCP, după ce a luat în considerare probabilitatea ca încălcarea securității datelor cu caracter personal să genereze un risc ridicat, poate să îi solicite operatorului informarea persoanei vizate sau poate decide că una dintre condițiile menționate la pct. 59 este îndeplinită.

X. RESPONSABILITĂȚI

61. Toți angajații și utilizatorii din cadrul Academiei care au acces la datele cu caracter personal sunt obligați să respecte prevederile prezentei Politici de protecție.

62. Nerespectarea prevederilor Politicii de securitate atrage după sine răspunderea disciplinară, contravențională, civilă ori penală, în raport cu gravitatea faptei, potrivit legislației.

63. Orice operator implicat în operațiunile de prelucrare este răspunzător pentru prejudiciul cauzat de operațiunile sale de prelucrare, în conformitate cu prevederile art. 76 din Legea nr. 195/2024. Persoana împuternicită de operator este răspunzătoare pentru prejudiciul cauzat de prelucrare numai în cazul în care nu a respectat obligațiile din Legea nr. 195/2024 care revin în mod specific persoanelor împuternicite de operator sau a acționat în afara ori în contradicție cu instrucțiunile legale ale operatorului.