



Regulament pentru asigurarea securității prelucrării datelor cu caracter personal de către Universitatea "Apollonia" din Iași

Prezentul Regulament are la bază prevederile Regulamentului U.E. nr. 679/2016 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date.

CAPITOLUL I. Dispoziții generale

Scopul și sfera de aplicare

Art. 1.

(1) Prezentul Regulament are drept scop stabilirea unor norme de conduită pentru asigurarea unui nivel satisfăcător de protecție a datelor cu caracter personal prelucrate de către Universitatea "Apollonia" din Iași, denumită în continuare UAI, operator.

(2) Normele de conduită stabilesc exercitarea drepturilor și obligațiilor pe care UAI le are în domeniul protecției persoanelor în privința datelor cu caracter personal, în relațiile instituției cu persoanele vizate, cu alte instituții de învățământ, precum și cu alte persoane fizice sau juridice.

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

Definirea termenilor

Art. 2.

(1) Termenii folosiți au următorul sens:

a) **persoana vizată** - persoana fizică ale cărei date cu caracter personal sunt prelucrate:

- candidați la admitere în cadrul UAI (pentru ciclurile de studii universitare de licență);
- studenți declarați admiși și înmatriculați la UAI;
- personalul didactic, personalul didactic auxiliar, precum și personalul nedidactic angrenat în procesul educațional.

b) **a colecta** - a strânge, a aduna, a primi date cu caracter personal de la persoanele prevăzute la lit. a) din prezentul articol prin intermediul secretariatelor facultăților.

c) **a dezvălui** - a transmite, a disemina, a face disponibile în orice alt mod date cu caracter personal, în afara operatorului;





d) **a utiliza** - a se folosi datele cu caracter personal de către și în interiorul operatorului;
e) **consimțământ** - acordul neviciat al persoanei vizate de a-i fi prelucrate datele cu caracter personal, care trebuie să fie întotdeauna expres și neechivoc;

f) **nivel de protecție și de securitate adecvat al prelucrărilor de date cu caracter personal** - nivelul de securitate proporțional riscului, pe care îl comportă prelucrarea față de datele cu caracter personal respective și față de drepturile și libertățile persoanelor și conform cerințelor minime de securitate a prelucrărilor de date cu caracter personal, elaborate de autoritatea de supraveghere și actualizate corespunzător stadiului dezvoltării tehnologice și costurilor implementării acestor măsuri.

(2) Termeni precum: date cu caracter personal, prelucrarea datelor cu caracter personal, stocare, operator, terț, destinatar, date anonime, autoritate de supraveghere, dreptul de informare, dreptul de acces, dreptul de intervenție, dreptul de opoziție au sensurile definite de Legea nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date.

Adoptarea și modificarea regulamentului

Art. 3. Prezentul Regulament a fost adoptat în ședința Senatului UAI din data de 24.05.2018, cu posibilitatea revizuirii periodice, în funcție de modificările și completările legislative aplicabile, precum și de nivelul de dezvoltare tehnologică.

CAPITOLUL II. Principiile și cadrul instituțional privind prelucrarea datelor cu caracter personal de către Universitatea "Apollonia" din Iași

Legalitatea și transparența

Art. 4. UAI recunoaște și respectă dreptul la viață intimă, familială și privată, prelucrarea datelor cu caracter personal desfășurându-se în conformitate cu prevederile legale în vigoare și cu respectarea cerințelor minime de securitate a prelucrărilor de date cu caracter personal, prevăzute de lege.





Responsabilitatea

Art. 5.

(1) UAI utilizează datele cu caracter personal ale persoanelor vizate prin intermediul unei baze de date alcătuite din informații obținute direct de la persoanele vizate prin consimțământul acestora și informații furnizate de orice sursă externă autorizată de lege.

(2) UAI este responsabilă pentru datele cu caracter personal, aflate sub controlul său, precum și pentru datele transferate către terți.

(3) Persoanele care vor răspunde pentru respectarea dispozițiilor legale din domeniul protecției persoanelor și a datelor cu caracter personal, precum și a principiilor prevăzute în prezentul Regulament sunt numai persoane angajate în cadrul UAI și care au printre atribuțiile principale și colectarea, utilizarea, prelucrarea, datelor cu caracter personal.

Legitimitatea scopului colectării

Art. 6.

(1) Colectarea de date cu caracter personal prin mijloace frauduloase, neloiale sau ilegale este interzisă în cadrul UAI.

(2) Persoanele vizate vor fi informate asupra categoriilor de date care sunt prelucrate, scopul prelucrării, precum și consecințele refuzului acestora de a furniza UAI datele solicitate.

(3) Scopurile pentru care se colectează date se precizează în scris, într-un limbaj ușor accesibil pentru persoanele vizate.

Consimțământul

Art. 7.

(1) În cazul prelucrării datelor cu caracter personal, se cere consimțământul persoanelor vizate.

(2) Consimțământul de colectare a datelor cu caracter personal se exprimă prin completarea de declarații (anexe). În această anexă sunt prezentate declarația și nota de informare pentru principalele tipuri de situații. După caz, UAI, va utiliza și alte variante de declarații concepute în aceeași manieră cu prezentul regulament (anexe).

(3) Persoana vizată își poate retrage consimțământul în orice moment, sub condiția avizării prealabile a operatorului. Acesta va informa persoana vizată în legătură cu procedura și efectele retragerii consimțământului.





Legitimitatea dezvăluirii

Art. 8

(1) UAI va prelucra datele cu caracter personal numai pentru scopurile pentru care au fost colectate, cu excepția cazului în care persoana vizată își dă anterior consimțământul și pentru prelucrarea în alte scopuri sau în alte cazuri permise de lege.

(2) Accesul la datele prelucrate va fi permis numai angajaților din cadrul UAI, în îndeplinirea obligațiilor de serviciu.

Legitimitatea stocării

Art. 9

(1) UAI se obligă să ia toate măsurile necesare pentru păstrarea datelor cu caracter personal de o manieră exactă, completată și actualizată, pentru a îndeplini scopurilor pentru care acestea au fost colectate.

(2) Datele inexacte sau incomplete vor fi rectificate sau eliminate din evidența curentă.

(3) Datele cu caracter personal vor fi păstrate numai pe perioada necesară îndeplinirii scopurilor stabilite, cu respectarea drepturilor persoanei vizate, în special a dreptului de acces, de intervenție și de opoziție.

(4) În urma verificărilor periodice, datele cu caracter personal deținute de operator care nu mai servesc realizării scopurilor sau îndeplinirii unor obligații legale, vor fi distruse sau transformate în date anonime într-un interval de timp rezonabil, potrivit procedurilor stabilite de lege.

Securitatea prelucrărilor

Art. 10

(1) UAI are obligația de a lua toate măsurile tehnice și organizatorice necesare pentru asigurarea unui nivel de protecție și de securitate adecvat, în cadrul operațiunilor efectuate asupra datelor cu caracter personal, în acest scop la bazele de date vor avea acces numai persoane autorizate, iar copierea datelor se va putea face numai la locul în care sunt gestionate.

Dreptul de informare

Art. 11

(1) La cerere, atunci când legea nu interzice, UAI va comunica informații referitoare la: categoriile de date cu caracter personal pe care le prelucreză, sursele de la care au fost colectate datele cu caracter personal, scopurile prelucrării, precum și dacă, respectiv unui terț i-au fost dezvăluite aceste date.





(2) În cazul în care dezvaluirea datelor este impusă de lege (de exemplu, în vederea executării unei hotărâri judecătorești), UAI se va asigura ca terțul care solicită dezvaluirea acționează în conformitate cu dispozițiile legale incidente, iar cererea privește numai datele cu caracter personal neexcesive prin raportare la scopul prelucrării. Persoana vizată va fi informată în legătură cu dezvaluirea, numai dacă legea permite.

Dreptul de acces

Art. 12

(1) Persoanele vizate au dreptul să se informeze cu privire la datele personale proprii deținute de UAI, utilizând în acest scop diverse căi de comunicare (email, fax, solicitare scrisă).

(2) persoana vizată nu are dreptul de a accesa datele cu caracter personal ale altei persoane vizate.

Dreptul de intervenție

Art. 13

(1) Persoanele vizate au dreptul de a solicita, la cerere, verificarea exactității și a caracterului complet al datelor cu caracter personal care le privesc, precum și rectificarea datelor inexacte sau incomplete.

(2) UAI va păstra o evidență a contestațiilor privind caracterul exact sau complet al datelor, precum și o evidență a datelor transferate către alți operatori. Evidențele vor conține datele care au fost rectificate și datele care au fost transferate.

(3) Actualizarea bazelor de date se face prin intermediul informațiilor transmise de persoanele vizate, precum și prin informațiile furnizate de orice sursă externă autorizată de lege.

Dreptul de opoziție

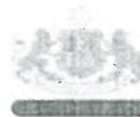
Art. 14

(1) Persoana vizată are dreptul de a se opune în orice moment, din motive întemeiate și legitime legate de situația sa particulară, ca date care o vizează să facă obiectul unei prelucrări, cu excepția cazurilor în care există dispoziții legale contrare. În caz de opoziție justificată, prelucrarea nu mai poate viza datele în cauză.

(2) Persoana vizată are dreptul de a se opune în orice moment, în mod gratuit și fără nici o justificare, ca datele care o vizează să fie prelucrate în scop de marketing direct, în numele operatorului sau al unui terț, sau să fie dezvăluite unor terți într-un asemenea scop.

(3) În vederea exercitării drepturilor prevăzute la art. 14 alin. (1) și (2), persoana vizată va înainta operatorului o cerere întocmită în formă scrisă, datată și semnată. În cerere solicitantul





poate arăta dacă dorește ca informațiile să îi fie comunicate la o anumită adresă, care poate fi și de poștă electronică, sau printr-un serviciu de corespondență care să asigure că predarea i se va face numai personal.

(4) Operatorul este obligat să comunice persoanei vizate măsurile luate în temeiul art. 14 alin.1 (1) sau (2), precum și, dacă este cazul, numele terțului căruia i-au fost dezvăluite datele cu caracter personal referitoare la persoana vizată, în termen de 15 zile de la data primirii cererii, cu respectarea eventualei opțiuni a solicitantului exprimate potrivit art. 14, alin. (3).

Soluționarea plângerilor

Art. 15

(1) UAI este obligată să rezolve plângerile și orice alte solicitări legate de prelucrarea datelor cu caracter personal, în termenele și condițiile prevăzute de lege.

CAPITOLUL III. Cerințe minime de securitate a prelucrărilor de date cu caracter personal

Identificarea și autentificarea utilizatorului

Art. 16.

(1) Prin utilizator se înțelege orice persoană care acționează sub autoritatea operatorului, a persoanei împuternicite sau a reprezentantului, cu drept recunoscut de acces la bazele de date cu caracter personal.

(2) Utilizatorii, pentru a căpăta acces la o bază de date cu caracter personal, trebuie să se identifice. Identificarea se poate face prin mai multe metode, cum ar fi: introducerea codului de identificare de la tastatură (un șir de caractere), folosirea unei cartele cu cod de bare, folosirea unei cartele inteligente (smart card) sau a unei cartele magnetice.

(3) Fiecare utilizator are propriul său cod de identificare. Niciodată mai mulți utilizatori nu trebuie să aibă același cod de identificare.

(4) Codurile de identificare (sau conturi de utilizator) nefolosite o perioadă mai îndelungată trebuie dezactivate și distruse după un control prealabil intern al operatorului. Perioada după care codurile trebuie dezactivate și distruse se stabilește de operator.

(5) Orice cont de utilizator este însoțit de o modalitate de autentificare. Autentificarea poate fi făcută prin introducerea unei parole sau prin mijloace biometrice: amprenta dactiloscopică, amprenta vocală, angiografia retiniană etc.

(6) Parolele sunt șiruri de caractere. Cu cât șirul de caractere este mai lung, cu atât parola este mai greu de aflat. La introducerea parolelor acestea nu trebuie să fie afișate în clar pe





monitor. Parolele trebuie schimbate periodic în funcție de politicile de securitate ale entității (operator sau persoană împuternicită). Schimbarea periodică a parolelor se face numai de către utilizatori autorizați de operator.

(7) Operatorul trebuie să solicite realizarea unui sistem informațional care să refuze automat accesul unui utilizator după 5 introduceri greșite ale parolei.

(8) Orice utilizator care primește un cod de identificare și un mijloc de autentificare trebuie să păstreze confidențialitatea acestora și să răspundă în acest sens în fața operatorului.

(9) Fiecare entitate va stabili o procedură proprie de administrare și gestionare a conturilor de utilizator.

(10) Operatorii autorizează anumiți utilizatori pentru a revoca sau a suspenda un cod de identificare și autentificare, dacă utilizatorul acestora și-a dat demisia ori a fost concediat, și-a încheiat contractul, a fost transferat la alt serviciu și noile sarcini nu îi solicită accesul la date cu caracter personal, a abuzat de codurile primite sau dacă va absenta o perioadă îndelungată stabilită de entitate.

(11) Accesul utilizatorilor la bazele de date cu caracter personal efectuate manual se va face pe baza unei liste aprobate de conducerea entității.

Tipul de acces

Art. 17.

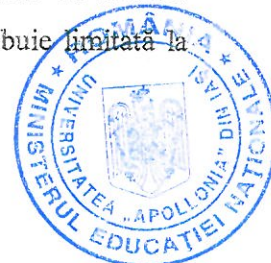
(1) Utilizatorii trebuie să acceseze numai datele cu caracter personal necesare pentru îndeplinirea atribuțiilor lor de serviciu. Pentru aceasta operatorii trebuie să stabilească tipurile de acces după funcționalitate (cum ar fi: administrare, introducere, prelucrare, salvare etc.) și după acțiuni aplicate asupra datelor cu caracter personal (cum ar fi: scriere, citire, ștergere), precum și procedurile privind aceste tipuri de acces.

(2) Programatorii sistemelor de prelucrare a datelor cu caracter personal nu vor avea acces la datele cu caracter personal. Operatorul va permite accesul programatorilor la datele cu caracter personal după ce acestea au fost transformate în date anonime.

(3) Compartimentul care asigură suportul tehnic poate avea acces la datele cu caracter personal pentru rezolvarea unor cazuri excepționale.

(4) Pentru activitatea de pregătire a utilizatorilor sau pentru realizarea de prezentări se vor folosi date anonime. Angajații care predau cursurile de pregătire vor folosi date cu caracter personal pe parcursul propriei lor pregătiri.

(5) Operatorul va stabili modalitățile stricte prin care se vor distruge datele cu caracter personal. Autorizarea pentru această prelucrare de date cu caracter personal trebuie limitată la câțiva utilizatori.





Colectarea datelor

Art. 18

(1) Operatorul desemnează utilizatori autorizați pentru operațiile de colectare și introducere de date cu caracter personal într-un sistem informațional

(2) Orice modificare a datelor cu caracter personal se poate face numai de către utilizatori autorizați desemnați de operator.

(3) Operatorul va lua măsuri pentru ca sistemul informațional să înregistreze cine a făcut modificarea, data și ora modificării. Pentru o mai bună administrare operatorul va lua măsuri ca sistemul informațional să mențină datele șterse sau modificate.

Execuția copiilor de siguranță

Art. 19.

(1) Operatorul va stabili intervalul de timp la care se vor executa copiile de siguranță ale bazelor de date cu caracter personal, precum și ale programelor folosite pentru prelucrările automatizate. Utilizatorii care execută aceste copii de siguranță vor fi numiți de operator, într-un număr restrâns. Copiile de siguranță se vor stoca în alte camere, în fișete metalice cu sigiliu aplicat, și, dacă este posibil, chiar în camere din altă clădire.

(2) Operatorul va lua măsuri ca accesul la copiile de siguranță să fie monitorizat.

Computerele și terminalele de acces

Art. 20.

(1) Computerele și alte terminale de acces vor fi instalate în încăperi cu acces restricționat. Dacă nu pot fi asigurate aceste condiții, computerele se vor instala în încăperi care se pot încuia sau se vor lua măsuri ca accesul la computere să se facă cu ajutorul unor chei ori cartele magnetice.

(2) Dacă pe ecran apar date cu caracter personal asupra cărora nu se acționează o perioadă dată, stabilită de operator, sesiunea de lucru trebuie închisă automat. Mărimea acestei perioade se determină în funcție de operațiile care trebuie executate.

(3) Terminalele de acces folosite în relația cu publicul, pe care apar date cu caracter personal, vor fi poziționate astfel încât să nu poată fi văzute de public și după o perioadă scurtă, stabilită de operator, în care nu se acționează asupra lor, acestea trebuie ascunse.





Fișierele de acces

Art. 21.

(1) Operatorul este obligat să ia măsuri ca orice accesare a bazei de date cu caracter personal să fie înregistrată într-un fișier de acces (numit log la prelucrările automate) sau într-un registru pentru prelucrările manuale de date cu caracter personal, stabilit de operator. Informațiile înregistrate în fișierul de acces sau în registru vor fi:

- codul de identificare (numele utilizatorului pentru bazele de date cu caracter personal manuale); numele fișierului accesat (fișei);
- numărul înregistrărilor efectuate; tipul de acces;
- codul operației executate sau programul folosit; data accesului (an, lună, zi);
- timpul (ora, minutul, secunda).

(2) Pentru prelucrările automate aceste informații vor fi stocate într-un fișier de acces general sau în fișiere separate pentru fiecare utilizator. Orice încercare de acces neautorizat va fi, de asemenea, înregistrată.

(3) Operatorul este obligat să păstreze fișierele de acces cel puțin 2 ani, pentru a fi folosite ca probe în cazul unor investigații. Dacă investigațiile se prelungesc, aceste fișiere se vor păstra atât timp cât se va considera necesar.

(4) Fișierele de acces trebuie să facă posibilă identificarea de către operator sau de către persoana împuternicită a persoanelor care au accesat date cu caracter personal fără un motiv anume, în vederea aplicării unor sancțiuni sau a sesizării organelor competente.

Sistemele de telecomunicații

Art. 22.

(1) Operatorul este obligat să facă periodic controlul autentificărilor și tipurilor de acces pentru detectarea unor disfuncționalități în ceea ce privește folosirea sistemelor de telecomunicații.

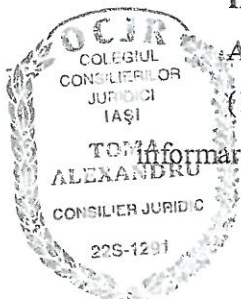
(2) Operatorii sunt obligați să conceapă sistemul de telecomunicații astfel încât datele cu caracter personal să nu poată fi interceptate sau transmise de oriunde. Dacă sistemul de telecomunicații nu poate fi astfel securizat, operatorul este obligat să impună folosirea metodei de criptare pentru transmiterea datelor cu caracter personal.

(3) Prin sistemele de telecomunicații se vor transmite numai datele cu caracter personal strict necesare.

Instruirea personalului

Art. 23.

(1) În cadrul cursurilor de pregătire a utilizatorilor operatorul este obligat să facă informarea acestora cu privire la prevederile Legii nr. 677/2001 pentru protecția persoanelor cu





privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date, la cerințele minime de securitate prelucrărilor de date cu caracter personal, precum și cu privire la riscurile pe care le comportă prelucrarea datelor cu caracter personal, în funcție de specificul activității utilizatorului.

(2) Utilizatorii care au acces la date cu caracter personal vor fi instruiți de către operator asupra confidențialității acestora și vor fi avertizați prin mesaje care vor apărea pe monitoare în timpul activității. Utilizatorii sunt obligați să își încheie sesiunea de lucru atunci când părăsesc locul de muncă.

Folosirea computerelor

Art. 24.

(1) Pentru menținerea securității prelucrării datelor cu caracter personal (în special împotriva virusurilor informatice) operatorul va lua măsuri care vor consta în:

- a) interzicerea folosirii de către utilizatori a programelor software care provin din surse externe sau dubioase;
- b) informarea utilizatorilor în privința pericolului privind virusii informatici;
- c) implementarea unor sisteme automate de devirusare și de securitate a sistemelor informatice;
- d) dezactivarea, pe cât posibil, a tastei "Print screen", atunci când sunt afișate pe monitor date cu caracter personal, interzicându-se astfel scoaterea la imprimantă a acestora.

Imprimarea datelor

Art. 25.

(1) Scoaterea la imprimantă a datelor cu caracter personal se va realiza numai de utilizatori autorizați pentru această operațiune de către operator. Operatorii sunt obligați să aprobe proceduri interne specifice privind folosirea și distrugerea acestor materiale.

(2) Fiecare entitate își va aproba propriul sistem de securitate, ținând seama de aceste cerințe minime de securitate a prelucrărilor de date cu caracter personal, iar în funcție de importanța datelor cu caracter personal prelucrate, își va impune măsuri de securitate suplimentare.





CAPITOLUL IV. Dispoziții finale și tranzitorii

(1) Regulamentul pentru asigurarea securității prelucrării datelor cu caracter personal de către Universitatea „Apollonia” din Iași va putea fi adaptat conform prevederilor legislative care vor urma momentului aprobării Regulamentului, prin decizia rectorului Universității „Apollonia” din Iași.

RECTOR,

Prof. univ. dr. Rodica CHIPURU



Secretar Șef,

Delia Cristina CHIPERU

Vizat juridic,

Jr. Alexandru TOMA

Prezentul Regulament a fost aprobat de Senatul Universității Apollonia din Iași prin Hotărârea nr. 34 din 24.05.2018.

Președinte Senatului,

Prof. univ. dr. Dumitru POPA

