Anexa nr. 1 la HS nr. 12/10.4.2014
Preşedintele Senatului UDJG
prof. dr. ing. Lucian Georgescu

REGULAMENT

pentru asigurarea securităţii prelucrărilor datelor cu caracter personal de către Universitatea „Dunărea de Jos” din Galaţi

CAPITOLUL I. PREAMBUL

Art. 1. În vederea elaborării prezentului Regulament, s-a avut în vedere respectarea dispoziţiilor legale referitoare la protecţia dreptului la viaţa intimă, familială şi privată, în ceea ce priveşte prelucrarea datelor cu caracter personal, în conformitate cu dispoziţiile Legii nr. 677/2001, coroborate cu dispoziţiile Ordinului nr. 52/2002 privind aprobarea Cerinţelor minime de securitate a prelucrărilor de date cu caracter personal, precum şi în conformitate cu dispoziţiilor Legii 1/2011.

CAPITOLUL II: DISPOZIŢII GENERALE

A. SCOPUL ŞI SFERA DE APLICARE

Art. 2. Prezentul Regulament are drept principal obiectiv stabilirea unor norme de conduită pentru asigurarea unui nivel satisfăcător de protecţie a datelor cu caracter personal prelucrate de către Universitatea „Dunărea de Jos” din Galaţi.

Art. 3. Normele de conduită stabilesc exercitarea drepturilor şi obligaţiilor pe care Universitatea „Dunărea de Jos” din Galaţi le are în domeniul protecţiei persoanelor în privinţa datelor cu caracter personal, în relaţiile instituţiei cu persoanele vizate, cu alte instituţii de învăţământ, precum şi cu alte persoane fizice sau juridice.

Art. 4. Normele cuprinse în prezentul Regulament nu aduc atingere altor obligaţii legale imperative sau deontologice ce revin Universităţii „Dunărea de Jos” din Galaţi.

B. DEFINIREA TERMENILOR

Art. 5. Termenii folosiţi au următorul sens:

a) ***persoana vizată*** - persoana fizică ale cărei date cu caracter personal sunt prelucrate:
   - candidaţi la admitere în cadrul Universităţii „Dunărea de Jos" din Galaţi, pentru toate ciclurile de studii universitare – licenţă, masterat, doctorat.
   - studenţi declaraţi admişi şi înmatriculaţi la Universitatea „Dunărea de Jos" din Galaţi.
   - personalul didactic, personalul didactic auxiliar, precum şi personalul nedidactic angrenat în procesul educaţional.

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

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 şi în interiorul operatorului;

e) ***consimţământ*** - acordul neviciat al persoanei vizate de a-i fi prelucrate datele cu caracter personal, care trebuie să fie întotdeauna expres şi neechivoc;

f) ***nivel de protecţie şi de securitate adecvat al prelucrărilor de date cu caracter personal*** - nivelul de securitate proporţional riscului, pe care îl comport prelucrarea faţă de datele cu caracter personal respective şi faţă de drepturile şi libertăţile persoanelor şi conform cerinţelor minime de securitate a prelucrărilor de date cu caracter personal, elaborate de autoritatea de supraveghere şi actualizate corespunzător stadiului dezvoltării tehnologice şi costurilor implementarii acestor măsuri;

Art. 6. Termeni precum: *date cu caracter personal, prelucrarea datelor cu caracter personal, stocare, operator, terţ, destinatar, date anonime, autoritate de supraveghere, dreptul de informare, dreptul de acces, dreptul de intervenţie, dreptul de opoziţie* au sensurile definite de Legea nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date.

CAPITOLUL III. PRINCIPIILE ŞI CADRUL INSTITUŢIONAL PRIVIND PRELUCRAREA DE DATE CU CARACTER PERSONAL DE CĂTRE UNIVERSITATEA „DUNĂREA DE JOS" DIN GALAŢI

A. Legalitatea şi transparenta

Art. 7. Universitatea „Dunărea de Jos" din Galaţi recunoaşte şi respectă dreptul la viaţă intimă,

familială şi privată, prelucrarea datelor cu caracter personal desfăşurându-se în conformitate cu prevederile legale în vigoare, precizate la art. 1 din prezentul Regulament.

B. Responsabilitatea

Art. 8. Universitatea „Dunărea de Jos” din Galaţi utilizează datele cu caracter personal ale persoanelor vizate prin intermediul unei baze de date alcătuite din informaţii obţinute direct de la persoanele vizate prin consimţământul acestora şi informaţii furnizate de orice sursă externă autorizată de lege.

Art. 9. Universitatea „Dunărea de Jos” din Galaţi este responsabilă pentru datele cu caracter personal, aflate sub controlul său, precum şi pentru datele transferate către terţi.

Art. 10. Persoanele care vor răspunde pentru respectarea dispoziţiilor legale din domeniul protecţiei persoanelor şi a datelor cu caracter personal, precum şi a principiilor prevăzute în prezentul Regulament sunt numai persoane angajate în cadrul Universităţii „Dunărea de Jos” din Galaţi şi care au printre atribuţiile principale şi colectarea, utilizarea, prelucrarea, datelor cu caracter personal.

C. Legitimitatea scopului colectării

Art. 11. În Universitatea „Dunărea de Jos” din Galaţi colectarea de date cu caracter personal prin mijloace frauduloase, neloiale sau ilegale este interzisă.

Art. 12. Persoanele vizate vor fi informate asupra categoriilor de date care sunt prelucrate, scopul prelucrării, precum şi consecinţele refuzului acestora de a furniza Universităţii „Dunărea de Jos” din Galaţi datele solicitate.

Art. 13. Scopurile pentru care se colectează date se precizează în scris, într-un limbaj uşor accesibil pentru persoanele vizate.

D. Consimţământul

Art. 14. În cazul prelucrării datelor cu caracter personal, se cere consimţământul persoanelor vizate.

Art. 15. Consimţământul de colectare a datelor cu caracter personal se exprimă prin completarea de declaraţii/rubrici, însoţite de note de informare a persoanelor vizate în legătură cu prelucrarea datelor cu caracter personal.

Art. 16. Persoana vizată îşi poate retrage consimţământul în orice moment, sub condiţia avizării prealabile a operatorului. Acesta va informa persoana vizata în legatura cu procedura şi efectele retragerii consimţământului.

E. Legitimitatea dezvăluirii

Art. 17. Universitatea „Dunărea de Jos" din Galaţi va prelucra datele cu caracter personal numai pentru scopurile pentru care au fost colectate, cu excepţia cazului în care persoana vizata îşi da anterior consimţământul şi pentru prelucrarea în alte scopuri sau în alte cazuri permise de lege.

Art. 18. Accesul la datele prelucrate va fi permis numai angajaţilor Universităţii „Dunărea de Jos" din Galaţi, în îndeplinirea obligaţiilor de serviciu.

F. Legitimitatea stocării

Art. 19. Universitatea „Dunărea de Jos" din Galaţi se obligă să ia toate măsurile necesare pentru păstrarea datelor cu caracter personal de o manieră exactă, completată şi actualizată, pentru a îndeplinii scopurilor pentru care acestea au fost colectate.

Art. 20. Datele inexacte sau incomplete vor fi rectificate sau eliminate din evidenţa curentă.

Art. 21. 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 intervenţie şi de opoziţie.

Art. 22. În urma verificărilor periodice datele cu caracter personal deţinute de operator, care nu mai servesc realizării scopurilor sau îndeplinirii unor obligaţii legale, vor fi distruse sau transformate în date anonime într-un interval de timp rezonabil, potrivit procedurilor stabilite de lege.

G. Securitatea prelucrarilor

Art. 23. Universitatea „Dunărea de Jos" din Galaţi are obligaţia de a lua toate măsurile tehnice şi organizatorice necesare pentru asigurarea unui nivel de protecţie şi de securitate adecvat, în cadrul operaţiunilor 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.

H. Dreptul de informare

Art. 24. La cerere, atunci cand legea nu interzice, Universitatea „Dunărea de Jos" din Galaţi va comunica informaţii referitoare la: categoriile de date cu caracter personal pe care le prelucrează, sursele de la care au fost colectate datele cu caracter personal, scopurile prelucrării, precum şi dacă, respectiv unui terţ i-au fost dezvăluite aceste date.

Art. 25. În cazul în care dezvaluirea datelor este impusă de lege (de exemplu, în vederea executării unei hotărâri judecătoreşti), Universitatea „Dunărea de Jos" din Galaţi se va asigura ca terţul care solicita dezvaluirea acţionează în conformitate cu dispoziţiile legale incidente, iar cererea priveşte numai datele cu caracter personal neexcesive prin raportare la scopul prelucrării. Persoana vizata va

fi informată în legatura cu dezvaluirea, numai dacă legea permite.

I. Dreptul de acces

Art. 26. Persoanele vizate au dreptul să se informeze cu privire la datele personale proprii deţinute de Universitatea „Dunărea de Jos" din Galaţi, utilizând în acest scop diverse căi comunicare (email, fax, cerere scrisă).

Art. 27. O persoană vizată nu are dreptul de a accesa datele cu caracter personal ale altei persoane vizate.

J. Dreptul de intervenţie

Art. 28. Persoanele vizate au dreptul de a solicita verificarea exactităţii şi a caracterului complet al datelor cu caracter personal care le privesc, precum şi de a solicita rectificarea datelor inexacte.

Art. 29. Universitatea „Dunărea de Jos" din Galaţi va păstra o evidenţă a contestaţiilor privind caracterul exact sau complet al datelor, precum şi o evidenţă a datelor transferate către alţi operatori. Evidenţele vor conţine datele care au fost rectificate şi datele care au fost transferate.

Art. 30. Actualizarea bazelor de date se face prin intermediul informaţiilor transmise de persoanele vizate, precum şi prin informaţiile furnizate de orice sursă externă autorizată de lege.

K. Dreptul de opoziţie

Art. 31. Persoana vizată are dreptul de a se opune în orice moment, din motive întemeiate şi legitime legate de situaţia sa particulară, ca datele ce o vizează să facă obiectul unei prelucrări, cu excepţia cazurilor în care există dispoziţii legale contrare. În caz de opoziţie justificată prelucrarea nu mai poate viza datele în cauză.

Art. 32. Persoana vizată are dreptul de a se opune în orice moment, în mod gratuit şi fără nici o justificare, ca datele care o vizează să fie prelucrate în scop de marketing direct, în numele operatorului sau al unui terţ, sau să fie dezvăluite unor terţi într-un asemenea scop.

Art. 33. În vederea exercitării drepturilor prevăzute la art. 31 şi la art. 32 persoana vizată va înainta operatorului o cerere întocmită în formă scrisă, datată şi semnată. În cerere solicitantul poate arăta dacă doreşte ca informaţiile să îi fie comunicate la o anumită adresă, care poate fi şi de poştă electronică, sau printr-un serviciu de corespondenţă care să asigure că predarea i se va face numai personal.

Art. 34 . Operatorul este obligat să comunice persoanei vizate măsurile luate în temeiul art.31 sau art.32, precum şi, dacă este cazul, numele terţului 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 opţiuni a solicitantului exprimate potrivit art.33.

L. Soluţionarea plangerilor

Art. 35. Universitatea „Dunărea de Jos" din Galaţi este obligată să rezolve plângerile şi orice alte cereri legate de prelucrarea datelor cu caracter personal, în termenele şi condiţiile prevăzute de lege.

CAPITOLUL IV. CERINŢELE MINIME DE SECURITATE A PRELUCRĂRILOR DE DATE CU CARACTER PERSONAL

Art. 36. Identificarea şi autentificarea utilizatorului

(1) Prin utilizator se înţelege orice persoană care acţionează 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 şir 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 mulţi utilizatori nu trebuie să aibă acelaşi cod de identificare.

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

(5) Orice cont de utilizator este însoţit 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 şiruri de caractere. Cu cât şirul de caractere este mai lung, cu atât parola este mai greu de aflat. La introducerea parolelor acestea nu trebuie să fie afişate în clar pe monitor. Parolele trebuie schimbate periodic în funcţie de politicile de securitate ale entităţii (operator sau persoană împuternicită). Schimbarea periodică a parolelor se face numai de către utilizatori autorizaţi de operator.

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

(8) Orice utilizator care primeşte un cod de identificare şi un mijloc de autentificare trebuie să păstreze confidenţialitatea acestora şi să răspundă în acest sens în faţa operatorului.

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

(10) Operatorii autorizează anumiţi utilizatori pentru a revoca sau a suspenda un cod de identificare şi autentificare, dacă utilizatorul acestora şi-a dat demisia ori a fost concediat, şi-a încheiat contractul, a fost transferat la alt serviciu şi 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 entităţii.

Art. 37. Tipul de acces:

(1) Utilizatorii trebuie să acceseze numai datele cu caracter personal necesare pentru îndeplinirea atribuţiilor lor de serviciu. Pentru aceasta operatorii trebuie să stabilească tipurile de acces după funcţionalitate (cum ar fi: administrare, introducere, prelucrare, salvare etc.) şi după acţiuni aplicate asupra datelor cu caracter personal (cum ar fi: scriere, citire, ştergere), precum şi 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 excepţionale.

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

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

Art. 38. Colectarea datelor

(1) Operatorul desemnează utilizatori autorizaţi pentru operaţiile de colectare şi introducere de date cu caracter personal într-un sistem informaţional.

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

(3) Operatorul va lua măsuri pentru ca sistemul informaţional să înregistreze cine a făcut modificarea, data şi ora modificării. Pentru o mai bună administrare operatorul va lua măsuri ca sistemul informaţional să menţină datele şterse sau modificate.

Art. 39. Execuţia copiilor de siguranţă

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

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

Art. 40. Computerele şi terminalele de acces

(1) Computerele şi alte terminale de acces vor fi instalate în încăperi cu acces restricţionat. Dacă nu pot fi asigurate aceste condiţii, 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 acţionează o perioadă dată, stabilită de operator, sesiunea de lucru trebuie închisă automat. Mărimea acestei perioade se determină în funcţie de operaţiile care trebuie executate.

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

Art. 41. Fişierele de acces

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

- codul de identificare (numele utilizatorului pentru bazele de date cu caracter personal manuale);
- numele fişierului accesat (fişei);
- numărul înregistrărilor efectuate;

- tipul de acces;
- codul operaţiei executate sau programul folosit;
- data accesului (an, lună, zi);
- timpul (ora, minutul, secunda).

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

(3) Operatorul este obligat să păstreze fişierele de acces cel puţin 2 ani, pentru a fi folosite ca probe în cazul unor investigaţii. Dacă investigaţiile se prelungesc, aceste fişiere se vor păstra atât timp cât se va considera necesar.

(4) Fişierele 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 sancţiuni sau a sesizării organelor competente.

Art. 42. Sistemele de telecomunicaţii

(1) Operatorul este obligat să facă periodic controlul autentificărilor şi tipurilor de acces pentru detectarea unor disfuncţionalităţi în ceea ce priveşte folosirea sistemelor de telecomunicaţii.

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

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

Art. 43. Instruirea personalului

(1) În cadrul cursurilor de pregătire a utilizatorilor operatorul este obligat să facă informarea acestora cu privire la prevederile Legii nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date, la cerinţele minime de securitate a prelucrărilor de date cu caracter personal, precum şi cu privire la riscurile pe care le comportă prelucrarea datelor cu caracter personal, în funcţie de specificul activităţii utilizatorului.

(2) Utilizatorii care au acces la date cu caracter personal vor fi instruiţi de către operator asupra confidenţialităţii acestora şi vor fi avertizaţi prin mesaje care vor apărea pe monitoare în timpul

activităţii. Utilizatorii sunt obligaţi să îşi închidă sesiunea de lucru atunci când părăsesc locul de muncă.

Art. 44. Folosirea computerelor

(1) Pentru menţinerea securităţii prelucrării datelor cu caracter personal (în special împotriva viruşilor informatici) 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 privinţa pericolului privind viruşii informatici;
c) implementarea unor sisteme automate de devirusare şi de securitate a sistemelor informatice;
d) dezactivarea, pe cât posibil, a tastei "Print screen", atunci când sunt afişate pe monitor date cu caracter personal, interzicându-se astfel scoaterea la imprimantă a acestora.

Art. 45. Imprimarea datelor

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

(2) Fiecare entitate îşi va aproba propriul sistem de securitate, ţinând seama de aceste cerinţe minime de securitate a prelucrărilor de date cu caracter personal, iar în funcţie de importanţa datelor cu caracter personal prelucrate, îşi va impune măsuri de securitate suplimentare.

CAPITOLUL V. DISPOZIŢII FINALE ŞI TRANZITORII

Art. 46. Prezentul Regulament poate fi revizuit periodic, în funcţie de modificările şi completările legislative incidente, precum şi de nivelul de dezvoltare tehnologică.

Art. 47. Prezentul Regulament se completează cu prevederile legale în domeniul protecţiei datelor cu caracter personal.