



REGULAMENT privind protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date

*Regulation on the protection of individuals regarding
the processing of personal data and the circulation of these
data*

Elaborat:	Director IT, Dr. Marinel IORDAN	Semnătura 
Aviz juridic:	Consilier juridic: Nadia TOPAI	Semnătura 
Avizat:	Consiliul de Administrație al UVT	Hotărâre nr. 11/22.07.2015
Aprobat:	Senatul UVT	Hotărâre nr. 63/28.07.2015
Ediția 1		
Intrat în vigoare la data de 28.07.2015		
Retras la data de		

CAPITOLUL I: DISPOZIȚII GENERALE

Scopul și sfera de aplicare

Art. 1

(1) Prezentul Regulament are ca scop garantarea și protejarea drepturilor și libertăților fundamentale ale persoanelor fizice, în special a dreptului la viața intimă, familială și privată, cu privire la prelucrarea datelor cu caracter personal prelucrate de Universitatea de Vest din Timișoara, denumită în continuare UVT, operator.

(2) Exercițarea drepturilor prevăzute în prezentul Regulament nu poate fi restrânsă decât în cazuri expres și limitativ prevăzute de lege.

CAPITOLUL II: DOMENIU DE APLICARE

Art. 2. – Prezentul Regulament se aplică prelucrărilor de date cu caracter personal, efectuate, în tot sau în parte, prin mijloace automate, precum și prelucrării prin alte mijloace decât cele automate a datelor cu caracter personal care fac parte dintr-un sistem de evidență sau care sunt destinate să fie incluse într-un asemenea sistem.

CAPITOLUL III: DEFINIREA TERMENILOR

Art. 3. - Termenii folosiți se definesc după cum urmează: (au sensurile definite de Legea nr.677/2001 privind protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date, modificată)

- a) **date cu caracter personal** - orice informații referitoare la o persoană fizică identificată sau identificabilă; o persoană identificabilă este acea persoană care poate fi identificată, direct sau indirect, în mod particular prin referire la un număr de identificare ori la unul sau la mai mulți factori specifici identității sale fizice, fiziologice, psihice, economice, culturale sau sociale;

- b) **prelucrarea datelor cu caracter personal** - orice operațiune sau set de operațiuni care se efectuează asupra datelor cu caracter personal, prin mijloace automate sau neautomate, cum ar fi colectarea, înregistrarea, organizarea, stocarea, adaptarea ori modificarea, extragerea, consultarea, utilizarea, dezvăluirea către terți prin transmitere, diseminare sau în orice alt mod, alăturarea ori combinarea, blocarea, ștergerea sau distrugerea;
- c) **stocarea** - păstrarea pe orice fel de suport a datelor cu caracter personal culese;
- d) **sistem de evidență a datelor cu caracter personal** - orice structură organizată de date cu caracter personal, accesibilă potrivit unor criterii determinate, indiferent dacă această structură este organizată în mod centralizat ori descentralizat sau este repartizată după criterii funcționale ori geografice;
- e) **operator** - orice persoană fizică sau juridică, de drept privat ori de drept public, inclusiv autoritățile publice, instituțiile și structurile teritoriale ale acestora, care stabilește scopul și mijloacele de prelucrare a datelor cu caracter personal; dacă scopul și mijloacele de prelucrare a datelor cu caracter personal sunt determinate printr-un act normativ sau în baza unui act normativ, operator este persoana fizică sau juridică, de drept public ori de drept privat, care este desemnată ca operator prin acel act normativ sau în baza acelui act normativ;
- f) **persoană împuternicită de către operator** - o persoană fizică sau juridică, de drept privat ori de drept public, inclusiv autoritățile publice, instituțiile și structurile teritoriale ale acestora, care prelucrează date cu caracter personal pe seama operatorului;
- g) **terț** - orice persoană fizică sau juridică, de drept privat ori de drept public, inclusiv autoritățile publice, instituțiile și structurile teritoriale ale acestora, alta decât persoana vizată, operatorul ori persoana împuternicită sau persoanele care, sub autoritatea directă a operatorului sau a persoanei împuternicite, sunt autorizate să prelucreze date;
- h) **destinatar** - orice persoană fizică sau juridică, de drept privat ori de drept public, inclusiv autoritățile publice, instituțiile și structurile teritoriale ale acestora, căreia îi sunt dezvăluite date, indiferent dacă este sau nu terț; autoritățile publice cărora li se comunică date în cadrul unei competențe speciale de anchetă nu vor fi considerate destinatari;
- i) **date anonime** - date care, datorită originii sau modalității specifice de prelucrare, nu pot fi asociate cu o persoană identificată sau identificabilă.

Art.4 Alți termeni

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

i) candidați la admitere în cadrul UVT (pentru toate ciclurile de studii universitare – licență, masterat, doctorat),

ii) studenți declarați admiși și înmatriculați la UVT (pentru toate ciclurile de studii universitare – licență, masterat, doctorat),

iii) personalul angajat la UVT;

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, secretariatele de studii doctorale ale UVT, prin intermediul Departamentului de Resurse Umane;

- 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 nevicinat 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.

CAPITOLUL IV

Reguli generale privind prelucrarea datelor cu caracter personal

A. Caracteristicile datelor cu caracter personal în cadrul prelucrării

Art. 5. - (1) Datele cu caracter personal destinate a face obiectul prelucrării trebuie să fie:

- a) **prelucrate cu bună-credință** și în conformitate cu dispozițiile legale în vigoare;
- b) **colectate** în scopuri determinate, explicite și legitime; prelucrarea ulterioară a datelor cu caracter personal în scopuri statistice, de cercetare istorică sau științifică nu va fi considerată incompatibilă cu scopul colectării dacă se efectuează cu respectarea dispozițiilor legii, inclusiv a celor care privesc efectuarea notificării către autoritatea de supraveghere, precum și cu respectarea garanțiilor privind prelucrarea datelor cu caracter personal, prevăzute de normele care reglementează activitatea statistică ori cercetarea istorică sau științifică;
- c) **adecvate, pertinente și neexcesive** prin raportare la scopul în care sunt colectate și ulterior prelucrate;
- d) **exacte și, dacă este cazul, actualizate**, în acest scop se vor lua măsurile necesare pentru ca datele inexacte sau incomplete din punct de vedere al scopului pentru care sunt colectate și pentru care vor fi ulterior prelucrate, să fie șterse sau rectificate;

e) **stocate** într-o formă care să permită identificarea persoanelor vizate strict pe durata necesară realizării scopurilor în care datele sunt colectate și în care vor fi ulterior prelucrate; stocarea datelor pe o durată mai mare decât cea menționată, în scopuri statistice, de cercetare istorică sau științifică, se va face cu respectarea garanțiilor privind prelucrarea datelor cu caracter personal, prevăzute în normele care reglementează aceste domenii, și numai pentru perioada necesară realizării acestor scopuri.

(2) UVT în calitate de operator are obligația să respecte prevederile alin. (1) și să asigure îndeplinirea acestor prevederi de către persoanele împuternicite.

B. Condiții de legitimitate privind prelucrarea datelor

Art. 6. - (1) Orice prelucrare de date cu caracter personal, poate fi efectuată numai dacă persoana vizată **și-a dat consimțământul** în mod expres și neechivoc pentru acea prelucrare.

(2) **Consimțământul** persoanei vizate **nu este cerut** în următoarele cazuri:

a) când prelucrarea este necesară în vederea executării unui contract sau antecontract la care persoana vizată este parte ori în vederea luării unor măsuri, la cererea acesteia, înaintea încheierii unui contract sau antecontract;

b) când prelucrarea este necesară în vederea protejării vieții, integrității fizice sau sănătății persoanei vizate ori a unei alte persoane amenințate;

c) când prelucrarea este necesară în vederea îndeplinirii unei obligații legale a operatorului;

d) când prelucrarea este necesară în vederea aducerii la îndeplinire a unor măsuri de interes public sau care vizează exercitarea prerogativelor de autoritate publică cu care este investit operatorul sau terțul căruia îi sunt dezvăluite datele;

e) când prelucrarea este necesară în vederea realizării unui interes legitim al operatorului sau al terțului căruia îi sunt dezvăluite datele, cu condiția ca acest interes să nu prejudicieze interesul sau drepturile și libertățile fundamentale ale persoanei vizate;

f) când prelucrarea privește date obținute din documente accesibile publicului, conform legii;

g) când prelucrarea este făcută exclusiv în scopuri statistice, de cercetare istorică sau științifică, iar datele rămân anonime pe toată durata prelucrării.

(3) Prevederile alin. (2) nu aduc atingere dispozițiilor legale care reglementează obligația UVT, în calitate de operator, de a respecta și de a ocroti viața intimă, familială și privată.

C. Încheierea operațiunilor de prelucrare

Art. 7. - (1) La încheierea operațiunilor de prelucrare, dacă persoana vizată nu și-a dat în mod expres și neechivoc consimțământul pentru o altă destinație sau pentru o prelucrare ulterioară, datele cu caracter personal vor fi:

- a) distruse;
- b) transferate unui alt operator, cu condiția ca operatorul inițial să garanteze faptul că prelucrările ulterioare au scopuri similare celor în care s-a făcut prelucrarea inițială;
- c) transformate în date anonime și stocate exclusiv în scopuri statistice, de cercetare istorică sau științifică.

(2) În cazul operațiunilor de prelucrare efectuate în condițiile prevăzute la art. 7 alin. (1) lit. c) sau d), operatorul poate stoca datele cu caracter personal pe perioada necesară realizării scopurilor concrete urmărite, cu condiția asigurării unor măsuri corespunzătoare de protejare a acestora, după care va proceda la distrugerea lor dacă nu sunt aplicabile prevederile legale privind păstrarea arhivelor.

CAPITOLUL V

Reguli speciale privind prelucrarea datelor cu caracter personal

A. Prelucrarea unor categorii speciale de date

Art. 8. - (1) Prelucrarea datelor cu caracter personal legate de originea rasială sau etnică, de convingerile politice, religioase, filozofice sau de natură similară, de apartenența sindicală, precum și a datelor cu caracter personal privind starea de sănătate sau viața sexuală este interzisă.

(2) Prevederile alin. (1) nu se aplică în următoarele cazuri:

- a) când persoana vizată și-a dat în mod expres consimțământul pentru o astfel de prelucrare;

b) când prelucrarea este necesară în scopul respectării obligațiilor sau drepturilor specifice ale operatorului în domeniul dreptului muncii, cu respectarea garanțiilor prevăzute de lege; o eventuală dezvăluire către un terț a datelor prelucrate poate fi efectuată numai dacă există o obligație legală a operatorului în acest sens sau dacă persoana vizată a consimțit expres la această dezvăluire;

c) când prelucrarea este necesară pentru protecția vieții, integrității fizice sau a sănătății persoanei vizate ori a altei persoane, în cazul în care persoana vizată se află în incapacitate fizică sau juridică de a-și da consimțământul;

d) când prelucrarea este efectuată în cadrul activităților sale legitime de către o fundație, asociație sau de către orice altă organizație cu scop nelucrativ și cu specific politic, filozofic, religios ori sindical, cu condiția ca persoana vizată să fie membră a acestei organizații sau să întrețină cu aceasta, în mod regulat, relații care privesc specificul activității organizației și ca datele să nu fie dezvăluite unor terți fără consimțământul persoanei vizate;

e) când prelucrarea se referă la date făcute publice în mod manifest de către persoana vizată;

f) când prelucrarea este necesară pentru constatarea, exercitarea sau apărarea unui drept în justiție;

g) când prelucrarea este necesară în scopuri de medicină preventivă, de stabilire a diagnosticilor medicale, de administrare a unor îngrijiri sau tratamente medicale pentru persoana vizată ori de gestionare a serviciilor de sănătate care acționează în interesul persoanei vizate, cu condiția ca prelucrarea datelor respective să fie efectuate de către ori sub supravegherea unui cadru medical supus secretului profesional sau de către ori sub supravegherea unei alte persoane supuse unei obligații echivalente în ceea ce privește secretul;

h) când legea prevede în mod expres aceasta în scopul protejării unui interes public important, cu condiția ca prelucrarea să se efectueze cu respectarea drepturilor persoanei vizate și a celorlalte garanții prevăzute de prezenta lege.

(3) Prevederile alin. (2) nu aduc atingere dispozițiilor legale care reglementează obligația autorităților publice de a respecta și de a ocroti viața intimă, familială și privată.

B. Prelucrarea datelor cu caracter personal având funcție de identificare

Art. 9. - (1) Prelucrarea codului numeric personal sau a altor date cu caracter personal având o funcție de identificare de aplicabilitate generală poate fi efectuată numai dacă:

a) persoana vizată și-a dat în mod expres consimțământul;

b) prelucrarea este prevăzută în mod expres de o dispoziție legală.

C. Prelucrarea datelor cu caracter personal privind starea de sănătate

Art. 10. - (1) Prelucrarea codului numeric personal sau a altor date cu caracter personal având o funcție de identificare de aplicabilitate generală nu se aplică în privința prelucrării datelor privind starea de sănătate în următoarele cazuri:

a) dacă prelucrarea este necesară pentru protecția sănătății publice;

b) dacă prelucrarea este necesară pentru prevenirea unui pericol iminent, pentru prevenirea săvârșirii unei fapte penale sau pentru împiedicarea producerii rezultatului unei asemenea fapte ori pentru înlăturarea urmărilor prejudiciabile ale unei asemenea fapte.

(2) Prelucrarea datelor privind starea de sănătate poate fi efectuată numai de către, ori sub supravegherea unui cadru medical, cu condiția respectării secretului profesional, cu excepția situației în care persoana vizată și-a dat în scris și în mod neechivoc consimțământul atât timp cât acest consimțământ nu a fost retras, precum și cu excepția situației în care prelucrarea este necesară pentru prevenirea unui pericol iminent, pentru prevenirea săvârșirii unei fapte penale, pentru împiedicarea producerii rezultatului unei asemenea fapte sau pentru înlăturarea urmărilor sale prejudiciabile.

(3) Datele cu caracter personal privind starea de sănătate pot fi colectate numai de la persoana vizată. Prin excepție, aceste date pot fi colectate din alte surse numai în măsura în care este necesar pentru a nu compromite scopurile prelucrării, iar persoana vizată nu vrea ori nu le poate furniza.

D. Prelucrarea datelor cu caracter personal referitoare la fapte penale sau contravenții

Art. 11. - (1) Prelucrarea datelor cu caracter personal referitoare la săvârșirea de infracțiuni de către persoana vizată ori la condamnări penale, măsuri de siguranță sau sancțiuni administrative ori contravenționale, aplicate persoanei vizate, poate fi efectuată numai de către sau sub controlul autorităților publice, în limitele puterilor ce le sunt conferite prin lege și în condițiile stabilite de legile speciale care reglementează aceste materii.

CAPITOLUL VI

Drepturile persoanei vizate în contextul prelucrării datelor cu caracter personal

A. Informarea persoanei vizate

Art. 12. - (1) În cazul în care datele cu caracter personal sunt obținute direct de la persoana vizată, UVT în calitate de operator este obligat să furnizeze persoanei vizate cel puțin următoarele informații, cu excepția cazului în care această persoană posedă deja informațiile respective:

a) identitatea operatorului și a reprezentantului acestuia, dacă este cazul;

b) scopul în care se face prelucrarea datelor;

c) informații suplimentare, precum: destinatarii sau categoriile de destinatari ai datelor; dacă furnizarea tuturor datelor cerute este obligatorie și consecințele refuzului de a le furniza; existența drepturilor prevăzute de prezenta lege pentru persoana vizată, în special a dreptului de acces, de intervenție asupra datelor și de opoziție, precum și condițiile în care pot fi exercitate;

d) orice alte informații a căror furnizare este impusă prin dispoziție a autorității de supraveghere, ținând seama de specificul prelucrării.

(2) În cazul în care datele nu sunt obținute direct de la persoana vizată, operatorul este obligat ca, în momentul colectării datelor sau, dacă se intenționează dezvăluirea acestora către terți, cel mai târziu până în momentul primei dezvăluiri, să furnizeze persoanei vizate cel puțin următoarele informații, cu excepția cazului în care persoana vizată posedă deja informațiile respective:

a) identitatea operatorului și a reprezentantului acestuia, dacă este cazul;

b) scopul în care se face prelucrarea datelor;

c) informații suplimentare, precum: categoriile de date vizate, destinatarii sau categoriile de destinatari ai datelor, existența drepturilor prevăzute de prezenta lege pentru persoana vizată, în special a dreptului de acces, de intervenție asupra datelor și de opoziție, precum și condițiile în care pot fi exercitate;

d) orice alte informații a căror furnizare este impusă prin dispoziție a autorității de supraveghere, ținând seama de specificul prelucrării.

(3) Prevederile alin. (2) nu se aplică atunci când prelucrarea datelor se efectuează exclusiv în scopuri jurnalistice, literare sau artistice, dacă aplicarea acestora ar da indicii asupra surselor de informare.

(4) Prevederile alin. (2) nu se aplică în cazul în care prelucrarea datelor se face în scopuri statistice, de cercetare istorică sau științifică, ori în orice alte situații în care furnizarea unor asemenea informații se dovedește imposibilă sau ar implica un efort disproporționat față de interesul legitim care ar putea fi lezat, precum și în situațiile în care înregistrarea sau dezvoltarea datelor este expres prevăzută de lege.

B. Dreptul de acces la date

Art. 13. - (1) Orice persoană vizată are dreptul de a obține de la operator, la cerere și în mod gratuit pentru o solicitare pe an, confirmarea faptului că datele care o privesc sunt sau nu sunt prelucrate de acesta. Operatorul este obligat, în situația în care prelucrează date cu caracter personal care privesc solicitantul, să comunice acestuia, împreună cu confirmarea, cel puțin următoarele:

a) informații referitoare la scopurile prelucrării, categoriile de date avute în vedere și destinatarii sau categoriile de destinatari cărora le sunt dezvoltate datele;

b) comunicarea într-o formă inteligibilă a datelor care fac obiectul prelucrării, precum și a oricărei informații disponibile cu privire la originea datelor;

c) informații asupra principiilor de funcționare a mecanismului prin care se efectuează orice prelucrare automată a datelor care vizează persoana respectivă;

d) informații privind existența dreptului de intervenție asupra datelor și a dreptului de opoziție, precum și condițiile în care pot fi exercitate;

e) informații asupra posibilității de a consulta registrul de evidență a prelucrărilor de date cu caracter personal, de a înainta plângere către autoritatea de supraveghere, precum și de a se adresa instanței pentru atacarea deciziilor operatorului, în conformitate cu dispozițiile prezentei legi.

(2) Persoana vizată poate solicita de la operator informațiile prevăzute la alin. (1), printr-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.

(3) Operatorul este obligat să comunice informațiile solicitate, în termen de 15 zile de la data primirii cererii, cu respectarea eventualei opțiuni a solicitantului exprimate potrivit alin. (2).

(4) În cazul datelor cu caracter personal legate de starea de sănătate, cererea prevăzută la alin. (2) poate fi introdusă de persoana vizată fie direct, fie prin intermediul unui cadru medical care va indica în cerere persoana în numele căreia este introdusă. La cererea operatorului sau a persoanei vizate comunicarea prevăzută la alin. (3) poate fi făcută prin intermediul unui cadru medical desemnat de persoana vizată.

(5) În cazul în care datele cu caracter personal legate de starea de sănătate sunt prelucrate în scop de cercetare științifică, dacă nu există, cel puțin aparent, riscul de a se aduce atingere drepturilor persoanei vizate și dacă datele nu sunt utilizate pentru a lua decizii sau măsuri față de o anumită persoană, comunicarea prevăzută la alin. (3) se poate face și într-un termen mai mare decât cel prevăzut la acel alineat, în măsura în care aceasta ar putea afecta bunul mers sau rezultatele cercetării dar nu mai târziu de momentul în care cercetarea este încheiată. În acest caz persoana vizată trebuie să își fi dat în mod expres și neechivoc consimțământul ca datele să fie prelucrate în scop de cercetare științifică, precum și asupra posibilei amânări a comunicării prevăzute la alin. (3) din acest motiv.

(6) Prevederile alin. (2) nu se aplică atunci când prelucrarea datelor se efectuează exclusiv în scopuri jurnalistice, literare sau artistice, dacă aplicarea acestora ar da indicii asupra surselor de informare.

C. Dreptul de intervenție asupra datelor

Art. 14. - (1) Orice persoană vizată are dreptul de a obține de la operator, la cerere și în mod gratuit:

a) după caz, rectificarea, actualizarea, blocarea sau ștergerea datelor a căror prelucrare nu este conformă prezentei legi, în special a datelor incomplete sau inexacte;

b) după caz, transformarea în date anonime a datelor a căror prelucrare nu este conformă prezentei legi;

c) notificarea către terții cărora le-au fost dezvăluite datele a oricărei operațiuni efectuate conform lit. a) sau b), dacă această notificare nu se dovedește imposibilă sau nu presupune un efort disproporționat față de interesul legitim care ar putea fi lezat.

(2) Pentru exercitarea dreptului prevăzut la alin. (1) 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.

(3) Operatorul este obligat să comunice măsurile luate în temeiul alin. (1), 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 alin. (2).

D. Dreptul de opoziție

Art. 15. - (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 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 alin. (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 alin. (3).

E. Dreptul de a nu fi supus unei decizii individuale

Art. 16. - (1) Orice persoană are dreptul de a cere și de a obține:

a) retragerea sau anularea oricărei decizii care produce efecte juridice în privința sa, adoptată exclusiv pe baza unei prelucrări de date cu caracter personal, efectuată prin mijloace automate, destinată să evalueze unele aspecte ale personalității sale, precum competența profesională, credibilitatea, comportamentul său ori alte asemenea aspecte;

b) reevaluarea oricărei alte decizii luate în privința sa, care o afectează în mod semnificativ, dacă decizia a fost adoptată exclusiv pe baza unei prelucrări de date care întrunește condițiile prevăzute la lit. a).

(2) Respectându-se celelalte garanții prevăzute de prezenta lege, o persoană poate fi supusă unei decizii de natura celei vizate la alin. (1), numai în următoarele situații:

a) decizia este luată în cadrul încheierii sau executării unui contract, cu condiția ca cererea de încheiere sau de executare a contractului, introdusă de persoana vizată, să fi fost satisfăcută sau ca unele măsuri adecvate, precum posibilitatea de a-și susține punctul de vedere, să garanteze apărarea propriului interes legitim;

b) decizia este autorizată de o lege care precizează măsurile ce garantează apărarea interesului legitim al persoanei vizate.

CAPITOLUL VII

Confidențialitatea și securitatea prelucrărilor

A. Confidențialitatea prelucrărilor

Art. 17. - Orice persoană care acționează sub autoritatea operatorului sau a persoanei împuternicite, inclusiv persoana împuternicită, care are acces la date cu caracter personal, nu poate să le prelucreze decât pe baza instrucțiunilor operatorului, cu excepția cazului în care acționează în temeiul unei obligații legale.

B. Securitatea prelucrărilor

Art. 18. - (1) Operatorul este obligat să aplice măsurile tehnice și organizatorice adecvate pentru protejarea datelor cu caracter personal împotriva distrugerii accidentale sau ilegale, pierderii, modificării, dezvăluirii sau accesului neautorizat, în special dacă prelucrarea respectivă comportă transmitii de date în cadrul unei rețele, precum și împotriva oricărei alte forme de prelucrare ilegală.

(2) Aceste măsuri trebuie să asigure, potrivit stadiului tehnicii utilizate în procesul de prelucrare și de costuri, un nivel de securitate adecvat în ceea ce privește riscurile pe care le reprezintă prelucrarea, precum și în ceea ce privește natura datelor care trebuie protejate. Cerințele minime de securitate vor fi elaborate de autoritatea de supraveghere și vor fi actualizate periodic, corespunzător progresului tehnic și experienței acumulate.

(3) Efectuarea prelucrărilor prin persoane împuternicite trebuie să se desfășoare în baza unui contract încheiat în formă scrisă, care va cuprinde în mod obligatoriu:

- a) obligația persoanei împuternicite de a acționa doar în baza instrucțiunilor primite de la operator;
- b) faptul că îndeplinirea obligațiilor prevăzute la alin. (1) revine și persoanei împuternicite.

CAPITOLUL VIII

Notificarea către autoritatea de supraveghere

Art.19. (1) Operatorul este obligat să notifice autorității de supraveghere, personal sau prin reprezentant, înainte de efectuarea oricărei prelucrări ori a oricărui ansamblu de prelucrări având același scop sau scopuri corelate.

(2) Notificarea nu este necesară în cazul în care prelucrarea are ca unic scop ținerea unui registru destinat prin lege informării publicului și deschis spre consultare publicului în general sau oricărei persoane care probează un interes legitim, cu condiția ca prelucrarea să se limiteze la datele strict necesare ținerii registrului menționat.

(3) Notificarea va cuprinde cel puțin următoarele informații:

a) numele sau denumirea și domiciliul ori sediul operatorului și ale reprezentantului desemnat al acestuia, dacă este cazul;

b) scopul sau scopurile prelucrării;

c) o descriere a categoriei sau a categoriilor de persoane vizate și a datelor ori a categoriilor de date ce vor fi prelucrate;

d) destinatarii sau categoriile de destinatari cărora se intenționează să li se dezvăluie datele;

e) garanțiile care însoțesc dezvăluirea datelor către terți;

f) modul în care persoanele vizate sunt informate asupra drepturilor lor; data estimată pentru încheierea operațiunilor de prelucrare, precum și destinația ulterioară a datelor;

g) transferuri de date care se intenționează să fie făcute către alte state;

h) o descriere generală care să permită aprecierea preliminară a măsurilor luate pentru asigurarea securității prelucrării;

i) specificarea oricărui sistem de evidență a datelor cu caracter personal, care are legătură cu prelucrarea, precum și a eventualelor legături cu alte prelucrări de date sau cu alte sisteme de evidență a datelor cu caracter personal, indiferent dacă se efectuează, respectiv dacă sunt sau nu sunt situate pe teritoriul României;

j) motivele care justifică aplicarea prevederilor art. 12 alin. (3) sau (4) în situația în care prelucrarea datelor se face exclusiv în scopuri jurnalistice, literare sau artistice ori în scopuri statistice, de cercetare istorică sau științifică.

(4) Dacă notificarea este incompletă, autoritatea de supraveghere va solicita completarea acesteia.

(5) În limitele puterilor de investigare de care dispune, autoritatea de supraveghere poate solicita și alte informații, în special privind originea datelor, tehnologia de prelucrare automată utilizată și detalii referitoare la măsurile de securitate. Dispozițiile prezentului alineat nu se aplică în situația în care prelucrarea datelor se face exclusiv în scopuri jurnalistice, literare sau artistice.

(6) Dacă se intenționează ca datele care sunt prelucrate să fie transferate în străinătate, notificarea va cuprinde și următoarele elemente:

- a) categoriile de date care vor face obiectul transferului;
- b) țara de destinație pentru fiecare categorie de date.

(7) Notificarea se va transmite în termen de 15 zile de la intrarea în vigoare a actului normativ care instituie obligația respectivă și va cuprinde numai următoarele elemente:

- a) denumirea și sediul operatorului;
- b) scopul și temeiul legal al prelucrării;
- c) categoriile de date cu caracter personal supuse prelucrării.

(8) Autoritatea de supraveghere poate stabili și alte situații în care notificarea nu este necesară, în afara celei prevăzute la alin. (2), sau situații în care notificarea se poate efectua într-o formă simplificată, precum și conținutul acesteia, numai în unul dintre următoarele cazuri:

a) atunci când, luând în considerare natura datelor destinate să fie prelucrate, prelucrarea nu poate afecta, cel puțin aparent, drepturile persoanelor vizate, cu condiția să precizeze expres scopurile în care se poate face o asemenea prelucrare, datele sau categoriile de date care pot fi prelucrate, categoria sau categoriile de persoane vizate, destinatarii sau categoriile de destinatari cărora datele le pot fi dezvăluite și perioada pentru care datele pot fi stocate;

b) când prelucrarea este efectuată în cadrul activităților sale legitime de către o fundație, asociație sau de către orice altă organizație cu scop nelucrativ și cu specific politic, filozofic, religios ori sindical, cu condiția ca persoana vizată să fie membră a acestei organizații sau să întrețină cu aceasta, în mod regulat, relații care privesc specificul activității organizației și ca datele să nu fie dezvăluite unor terți fără consimțământul persoanei vizate;

CAPITOLUL IX

Supravegherea și controlul prelucrărilor de date cu caracter personal

Autoritatea de supraveghere

Art. 20. - (1) Autoritatea de supraveghere, în sensul prezentei legi, este Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal.

(2) Autoritatea de supraveghere își desfășoară activitatea în condiții de completă independență și imparțialitate.

(3) Autoritatea de supraveghere monitorizează și controlează sub aspectul legalității prelucrările de date cu caracter personal care cad sub incidența prezentei legi.

CAPITOLUL X

Transferul în străinătate al datelor cu caracter personal

Condițiile transferului în străinătate al datelor cu caracter personal

Art. 21. - (1) Transferul către un alt stat de date cu caracter personal care fac obiectul unei prelucrări ce sunt destinate să fie prelucrate după transfer poate avea loc numai în condițiile în care nu se încalcă legea română, iar statul către care se intenționează transferul asigură un nivel de protecție adecvat.

(2) Nivelul de protecție va fi apreciat de către autoritatea de supraveghere, ținând seama de totalitatea împrejurărilor în care se realizează transferul de date, în special având în vedere natura datelor transmise, scopul prelucrării și durata propusă pentru prelucrare, statul de origine și statul de destinație finală, precum și legislația statului solicitant. În cazul în care autoritatea de supraveghere constată că nivelul de protecție oferit de statul de destinație este nesatisfăcător, poate dispune interzicerea transferului de date.

(3) În toate situațiile transferul de date cu caracter personal către un alt stat va face obiectul unei notificări prealabile a autorității de supraveghere.

(4) Autoritatea de supraveghere poate autoriza transferul de date cu caracter personal către un stat a cărui legislație nu prevede un nivel de protecție cel puțin egal cu cel oferit de legea română atunci când operatorul oferă garanții suficiente cu privire la protecția drepturilor fundamentale ale persoanelor. Aceste garanții trebuie să fie stabilite prin contracte încheiate între operatori și persoanele fizice sau juridice din dispoziția cărora se efectuează transferul.

CAPITOLUL XI

Soluționarea plângerilor

A. Plângeri adresate Autorității de Supraveghere

Art. 22. - (1) În vederea apărării drepturilor prevăzute de regulament, persoanele ale căror date cu caracter personal fac obiectul unei prelucrări care cade sub incidența regulamentului, pot înainta plângere către autoritatea de supraveghere. Plângerea se poate face direct sau prin reprezentant. Persoana lezată poate împuternici o asociație sau o fundație să îi reprezinte interesele.

(2) Plângerea către autoritatea de supraveghere nu poate fi înaintată dacă o cerere în justiție, având același obiect și aceleași părți, a fost introdusă anterior.

(3) În afara cazurilor în care o întârziere ar cauza un prejudiciu iminent și ireparabil, plângerea către autoritatea de supraveghere nu poate fi înaintată mai devreme de 15 zile de la înaintarea unei plângeri cu același conținut către operator.

(4) În vederea soluționării plângerii, dacă apreciază că este necesar, autoritatea de supraveghere poate audia persoana vizată, operatorul și, dacă este cazul, persoana împuternicită sau asociația ori fundația care reprezintă interesele persoanei vizate. Aceste persoane au dreptul de a înainta cereri, documente și memorii. Autoritatea de supraveghere poate dispune efectuarea de expertize.

(5) Dacă plângerea este găsită întemeiată, autoritatea de supraveghere poate decide suspendarea provizorie sau încetarea prelucrării datelor, stergerea parțială ori integral a datelor prelucrate și poate să sesizeze organele de urmărire penală sau să intenteze acțiuni în justiție. Interdicția temporară a prelucrării poate fi instituită numai până la încetarea motivelor care au determinat luarea acestei măsuri.

(6) Decizia trebuie motivată și se comunică părților interesate în termen de 30 de zile de la data primirii plângerii.

(7) Autoritatea de supraveghere poate ordona, dacă apreciază necesar, suspendarea unora sau tuturor operațiunilor de prelucrare până la soluționarea plângerii în condițiile alin. (5).

(8) Autoritatea de supraveghere se poate adresa justiției pentru apărarea oricăror drepturi garantate de prezenta lege persoanelor vizate. Instanța competentă este Tribunalul Municipiului București. Cererea de chemare în judecată este scutită de taxa de timbru.

(9) La cererea persoanelor vizate, pentru motive întemeiate, instanța poate dispune suspendarea prelucrării până la soluționarea plângerii de către autoritatea de supraveghere.

(10) Prevederile alin. (4)-(9) se aplică în mod corespunzător și în situația în care autoritatea de supraveghere află pe orice altă cale despre săvârșirea unei încălcări a drepturilor recunoscute de prezenta lege persoanelor vizate.

B. Contestarea deciziilor autorității de supraveghere

Art. 23. - (1) Împotriva oricărei decizii emise de autoritatea de supraveghere în temeiul dispozițiilor prezentei legi operatorul sau persoana vizată poate formula contestație în termen de 15 zile de la comunicare, sub sancțiunea decăderii, la instanța de contencios administrativ competentă. Cererea se judecă de urgență, cu citarea părților. Soluția este definitivă și irevocabilă.

C. Dreptul de a se adresa justiției

Art. 24. - (1) Fără a se aduce atingere posibilității de a se adresa cu plângere autorității de supraveghere, persoanele vizate au dreptul de a se adresa justiției pentru apărarea oricăror drepturi garantate de prezentul regulament, care le-au fost încălcate.

(2) Orice persoană care a suferit un prejudiciu în urma unei prelucrări de date cu caracter personal, efectuată ilegal, se poate adresa instanței competente pentru repararea acestuia.

(3) Instanța competentă este cea în a cărei rază teritorială domiciliază pârâtul. Cererea de chemare în judecată este scutită de taxă de timbru.

DISPOZIȚII FINALE

Prezentul Regulament a fost adoptat în ședința Senatului UVT din data de

Temeiul legal în baza căruia a fost adoptat prezentul Regulament, Legea 677/2001 cu modificările și completările ulterioare.

LISTA ANEXELOR

Anexa 1 – Cerințe minime de Securitate a prelucrării datelor cu caracter personal

Anexa 2 – Declarație

Anexa 3 – Informare

Anexa 4 – Declarație

Anexa 5 – Informare

Anexa 6 – Cod de conduită

ANEXE la prezentul Regulament

Anexa 1

CERINȚELE MINIME DE SECURITATE a prelucrărilor de date cu caracter personal

Prezentele cerințe minime de securitate a prelucrărilor de date cu caracter personal trebuie să stea la baza adoptării și implementării de către operator a măsurilor tehnice și organizatorice necesare pentru păstrarea confidențialității și integrității datelor cu caracter personal. În concordanță cu acestea operatorii își vor stabili propriile politici și proceduri de securitate.

Cerințele minime de securitate a prelucrărilor de date cu caracter personal acoperă următoarele aspecte:

1. Identificarea și autentificarea utilizatorului

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.

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.

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

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.

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.

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.

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

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.

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

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.

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

2. Tipul de acces

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.

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.

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

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.

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.

3. Colectarea datelor

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

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

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.

4. Execuția copiilor de siguranță

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.

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

5. Computerele și terminalele de acces

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.

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.

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.

6. Fișierele de acces

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).

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.

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.

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.

7. Sistemele de telecomunicații

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

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 transmisia datelor cu caracter personal.

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

8. Instruirea personalului

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 a 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.

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 închidă sesiunea de lucru atunci când părăsesc locul de muncă.

9. Folosirea computerelor

Pentru menținerea securității prelucrării datelor cu caracter personal (în special împotriva virusilor 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 privința pericolului privind virușii 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.*

10. Imprimarea datelor

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.

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.

Anexa 2

DECLARAȚIE

Subsemnatul _____, în calitate de candidat la admitere/student declarat admis și înmatriculat pentru ciclul de studii universitare² _____, anul universitar _____ declar că am luat la cunoștință de dispozițiile legii nr. 677/2001 privind prelucrarea datelor cu caracter personal precum și de conținutul informării Universității de Vest din Timișoara cu privire la aceste date (informare aflată pe verso) și declar că sunt de acord ca aceste date cu caracter personal să fie stocate, prelucrate, utilizate și publicate.

Declar, susțin și semnez după ce am luat la cunoștință, sunt de acord cu întregul conținut și am completat personal datele din prezenta declarație.

Semnătura _____

Data _____

² Se va completa, după caz licență/masterat/doctorat, precum și facultatea, respectiv domeniul de studii

Anexa 3

INFORMARE

Universitatea de Vest din Timișoara, cu sediul în localitatea Timișoara, B-dul Vasile Pârvan, nr.4, Județul Timiș, denumită în continuare UVT, prelucrează datele dumneavoastră cu caracter personal.

Conform cerințelor Legii nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date, modificată completată și ale Legii nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice UVT are obligația de a administra în condiții de siguranță și numai pentru scopurile specificate, datele personale care îi sunt furnizate.

Datele dumneavoastră cu caracter personal, sunt necesare astfel:

A) pentru realizarea obiectului de activitate principal, respectiv educație și cultură,

în sensul inițierii și derulării de raporturi juridice între dumneavoastră și UVT;

B) în vederea îmbunătățirii modului de comunicare cu studenții, prin intermediul

poștei electronice, pentru comunicarea operativă și eficientă a informațiilor necesare derulării raporturilor contractuale dintre dumneavoastră și UVT.

Sunteți obligat să furnizați datele enunțate, deoarece în cazul nefurnizării corecte și complete a acestora, UVT poate să refuze inițierea de raporturi juridice cu dumneavoastră, întrucât poate fi pusă în imposibilitatea de a respecta cerințele reglementărilor speciale în domeniul educațional.

Informațiile înregistrate sunt destinate utilizării de către operator și sunt comunicate numai următorilor destinatari:

- persoana vizată
- partenerii contractuali ai operatorului
- instituții de învățământ și educație

Conform Legii nr. 677/2001, beneficiați de dreptul de acces, de intervenție

asupra datelor și de dreptul de a nu fi supus unei decizii individuale. Totodată, aveți dreptul să vă opuneți prelucrării datelor personale care vă privesc și să solicitați ștergerea datelor, cu excepția situațiilor prevăzute expres de lege, când prelucrarea datelor de către UVT este obligatorie. Pentru exercitarea acestor drepturi, vă puteți adresa cu o cerere scrisă, datată și semnată către Secretariatul General al UVT, care va înainta solicitarea dumneavoastră conducerii UVT.

De asemenea, vă este recunoscut dreptul de a vă adresa justiției.

Anexa 4

DECLARAȚIE

Subsemnatul _____, fiul lui _____
și al _____, născut la data de _____ în
localitatea _____, județul / sectorul _____, posesor al B.I./CI
seria _____ nr. _____, eliberat de
_____, la data de _____, în
calitate de doctorand UVT, înmatriculat ca student la studiile universitare
doctorale în I.O.S.U.D.-U.V.T.⁴, declar pe propria răspundere că am luat la
cunoștință de dispozițiile legii nr. 677/2001 privind prelucrarea datelor cu
caracter personal precum și de conținutul informării Universității de Vest din
Timișoara cu privire la aceste date și declar că sunt de acord ca aceste date cu
caracter personal să fie stocate, prelucrate, utilizate și publicate.

Declar, susțin și semnez după ce am luat la cunoștință de întregul conținut
și am completat personal datele din prezenta declarație.

Semnătura _____

Data _____

⁴ studii finanțate din Proiectul nr. _____, ID proiect _____, cu titlul _____, din cadrul Programului Operațional Sectorial

Dezvoltarea Resurselor Umane 2007-2013 nr. CCI 2007 RO051PO001, selectat în cadrul Programului Operațional Sectorial Dezvoltarea

Resurselor Umane (POS DRU) și cofinanțat din „Fondul Social European” (FSE)

Anexa 5

INFORMARE

Universitatea de Vest din Timișoara cu sediul în Timișoara, B-dul Vasile Pârvan, nr.4 , în calitate de I.O.S.U.D., prelucrează date cu caracter personal cu privire la doctoranzii ale căror studii sunt finanțate din Proiectul „Burse doctorale”, ID, cu titlul „Racordarea programelor de studii doctorale la studiile doctorale europene, din cadrul Programului Operațional Sectorial Dezvoltarea Resurselor Umane, selectat în cadrul Programului Operațional Sectorial Dezvoltarea Resurselor Umane (POS DRU) și cofinanțat din „Fondul Social European”(FSE), în conformitate cu prevederile Directivei CE/95/46 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date, transpusă în legislația națională prin Legea nr.677/2001, precum și prevederile Directivei 2002/58/CE privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice, transpusă în legislația națională prin Legea nr.506/2004.

Pe întreaga durată de implementare a proiectului, nr. „Burse doctorale”, ID proiect, cu titlul „Racordarea programelor de studii doctorale la studiile doctorale europene, din cadrul Programului Operațional Sectorial Dezvoltarea Resurselor Umane, selectat în cadrul Programului Operațional Sectorial Dezvoltarea Resurselor Umane (POS DRU) și cofinanțat din, Universitatea de Vest din Timișoara, în calitate de beneficiar al contractului de finanțare POSDRU are obligația de a transmite AMPOSDRU, informații privind participării în conformitate cu Regulamentul Comisiei (CE) nr.1828/2006 cu privire la implementarea Regulamentului Consiliului (CE) nr.1083/2006 privind dispozițiile generale cu privire la Fondul European de Dezvoltare Regională, Fondul Social European și Fondul de Coeziune și al Regulamentului

Parlamentului European și al Consiliului nr.1080/2006 privind Fondul European de Dezvoltare Regională.

În acest sens, în calitate de beneficiar, Universitatea de Vest din Timișoara va centraliza și transmite informații privind participanții pentru fiecare an de implementare a proiectului, utilizând următoarele criterii: gen, statut ocupațional, grupe de vârstă, apartenența la grup vulnerabil, nivel de educație, în baza

formularelor completate de către participanți (doctoranzi), utilizând formatul standard furnizat de AMPOSDRU.

În vederea realizării obiectivelor propuse și îndeplinirii condițiilor mai sus menționate, în calitate de doctorand, persoana din grupul țintă al proiectului, are obligația de a furniza datele personale, cu respectarea dispozițiilor legale în materie.

Anexa 6

COD DE CONDUITĂ

Preambul

Luând în considerare importanța deosebită a garantării dreptului la viață intimă, familială și privată, așa cum este prevăzut la art. 26 din Constituția României,

ținând seama de necesitatea protejării acestui drept fundamental în cadrul activităților de prelucrare a datelor cu caracter personal, reglementate prin Legea nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date, precum și prin Legea nr. 682/2001 privind ratificarea Convenției pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal, adoptată la Strasbourg la 28 ianuarie 1981.

CAPITOLUL I Dispoziții generale

Scopul și sfera de aplicare

Art. 1. -

(1) Prezentul cod de conduită are ca scop stabilirea unor norme de conduită pentru asigurarea unui nivel satisfăcător de protecție a datelor cu caracter personal prelucrate.

(2) Normele de conduită stabilesc exercitarea drepturilor și obligațiilor în domeniul protecției persoanelor în privința datelor cu caracter personal, în relațiile Universității de Vest din Timișoara cu persoanele vizate (în calitate de beneficiari ai serviciilor prestate, de utilizatori etc.).

(3) Normele cuprinse în prezentul model de cod de conduită nu aduc atingere altor obligații legale imperative sau deontologice care revin asociațiilor profesionale.

Definirea termenilor

Art. 2. -

(1) Termenii folosiți în prezentul cod de conduită au următorul sens:

- a) persoană vizată - persoana fizică ale cărei date cu caracter personal sunt prelucrate;*
- b) a colecta - a strânge, a aduna, a primi date cu caracter personal prin orice mijloace și din orice sursă;*
- 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 nevizat 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;*
- g) marketing direct - promovarea produselor și a serviciilor, adresată direct clienților, persoane fizice, prin mijloace de genul poștei, inclusiv cea electronică, sau alte mijloace de marketing la distanță, altele decât modalitățile promoționale obișnuite (reclame).*

(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.

Cadrul legal al codurilor de conduită

Art. 3. -

Vor fi respectate dispozițiile legale referitoare la protecția dreptului la viață intimă, familială și privată, în ceea ce privește prelucrarea datelor cu caracter personal. Se vor avea în vedere în mod special dispozițiile Legii nr. 677/2001, precum și ale Legii nr. 682/2001.

CAPITOLUL II Principiile prelucrărilor de date cu caracter personal efectuate de Universitatea de Vest din Timișoara

Legalitatea și transparența

Art. 5. -

(1) Universitatea de Vest din Timișoara recunoaște și respectă dreptul la viață intimă, familială și privată.

(2) Prelucrarea datelor cu caracter personal de către Universitatea de Vest din Timișoara se desfășoară în conformitate cu prevederile legale în vigoare.

(3) Universitatea de Vest din Timișoara este obligată să asigure transparența prelucrărilor de date cu caracter personal.

Responsabilitatea

Art. 6. -

(1) Universitatea de Vest din Timișoara este responsabilă pentru datele cu caracter personal aflate sub controlul său, precum și pentru datele transferate către terți.

(2) Universitatea de Vest din Timișoara va desemna 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 cod de conduită.

Legitimitatea scopului colectării

Art. 7. -

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

(2) Universitatea de Vest din Timișoara va comunica scopurile pentru care sunt colectate datele cu caracter personal fie înainte, fie cel mai târziu la momentul colectării.

(3) Menționarea scopurilor poate fi realizată în scris, oral sau în formă electronică, într-un limbaj ușor accesibil pentru persoanele vizate.

Consimțământul

Art. 8. -

(1) Consimțământul persoanelor vizate este cerut în cazul prelucrării datelor cu caracter personal, în afara cazurilor în care legea dispune altfel.

(2) Universitatea de Vest din Timișoara va folosi orice mijloace nedolosive, care necesită costuri financiare rezonabile, pentru a informa persoanele vizate în legătură cu prelucrarea datelor cu caracter personal și pentru a solicita consimțământul acestora la momentul colectării datelor cu caracter personal.

(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. 9. -

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

(2) Accesul la datele prelucrate va fi permis numai angajaților universității responsabili în acest scop și în îndeplinirea obligațiilor de serviciu.

Legitimitatea stocării

Art. 10. -

(1) Universitatea de Vest din Timișoara este obligată să păstreze datele cu caracter personal exacte, complete și actualizate, pentru realizarea scopurilor pentru care sunt utilizate.

(2) Datele inexacte sau incomplete vor fi șterse sau rectificate.

(3) *Datele cu caracter personal vor fi păstrate numai pentru perioada necesară atingerii scopurilor stabilite.*

(4) *Universitatea de Vest din Timișoara stabilește perioada necesară pentru păstrarea datelor colectate, numai pentru perioada necesară realizării scopului, urmărind totodată respectarea drepturilor persoanei vizate, în special a dreptului de acces, de intervenție și de opoziție.*

(5) *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. 11. -

Universitatea de Vest din Timișoara va 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 următoarele scopuri: pentru a limita accesul la bazele de date, care este permis numai persoanelor autorizate; pentru a interzice copierea datelor în afara locurilor în care sunt gestionate; în general, pentru a împiedica orice circulație necontrolată a datelor.

Dreptul de informare

Art. 12. -

(1) *Strategiile și procedurile folosite de Universitatea de Vest din Timișoara în legătură cu procesarea datelor cu caracter personal vor fi puse la dispoziție persoanelor vizate, sub formă de informații furnizate într-un limbaj accesibil, prin mijloace fizice (de exemplu, prin broșuri), telefonice sau electronice.*

(2) *Universitatea de Vest din Timișoara va comunica informații, la cerere, în legătură cu datele cu caracter personal, pe care le prelucrează, sursele din care au colectat datele cu caracter personal, scopurile prelucrării, dacă și cărui terț i-au fost dezvăluite aceste date, atunci când legea nu interzice.*

(3) *În cazul în care dezvăluirea datelor este impusă de lege (de exemplu, în vederea executării unei hotărâri judecătorești), Universitatea de Vest din Timișoara se va asigura că terțul care solicită dezvăluirea 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 dezvăluirea, numai dacă legea permite.*

Dreptul de acces

Art. 13. -

(1) Universitatea de Vest din Timișoara va permite accesul persoanelor vizate la datele cu caracter personal care le privesc, prin cele mai facile mijloace, pe care le pot pune la dispoziție, în mod rezonabil.

(2) Accesul persoanei vizate nu poate fi permis, cu excepția cazurilor prevăzute de lege, în următoarele situații: în cazul în care sunt solicitate date despre o altă persoană; în cazul în care ar putea fi afectate viața și siguranța altei persoane; în cazul în care sunt solicitate date care pot privi informații comerciale confidentiale; în cazul în care s-ar aduce atingere soluționării unui litigiu sau a unui proces penal.

(3) Universitatea de Vest din Timișoara este obligată să motiveze refuzul de a permite accesul la anumite date cu caracter personal.

Dreptul de intervenție

Art. 14. -

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

(2) Universitatea de Vest din Timișoara va păstra o evidență a contestațiilor privind caracterul exact sau complet al datelor, care nu au fost rezolvate, iar în cazul în care datele vor fi transferate către alți operatori, vor fi precizate datele care au fost rectificate sau în privința cărora există contestații nerezolvate.

(3) Dispozițiile alin. (2) se aplică și în cazul dezvăluirii de date către terți, dacă este cazul.

(4) 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.

Colaborarea cu autoritatea de supraveghere

Art. 15. -

(1) Anual sau ori de câte ori se va solicita Universitatea de Vest din Timișoara va prezenta autorității de supraveghere a prelucrărilor de date cu caracter personal, rapoarte sau sinteze cu privire la plângerile primite și la modul de soluționare a acestora.

(2) Rapoartele și sintezele la care se referă alin. (1) vor putea conține și alte informații privind aspecte din activitatea membrilor în domeniul protecției datelor cu caracter personal, precum și propuneri de îmbunătățire a activității acestora.

Cheltuielile suportate de către persoanele vizate

Art. 16. -

Universitatea de Vest din Timișoara va lua măsuri pentru asigurarea unui nivel rezonabil al cheltuielilor ocazionate de exercitarea drepturilor prevăzute de lege, cheltuieli care sunt în sarcina persoanei vizate, cu excepția cazului în care aceste drepturi pot fi exercitate în mod gratuit.

CAPITOLUL III Dispoziții finale și tranzitorii

Modul de aplicare

Art. 17. -

(1) Prezentul cod de conduită se completează cu prevederile legale în domeniul protecției datelor cu caracter personal.

Modificarea și completarea modelului de cod de conduită

Art. 18. -

(1) Modificările sau completările ale prezentului cod de conduită, vor fi trimise, în scris și motivat, autorității de supraveghere.

(2) Autoritatea de supraveghere va lua în considerare numai propunerile pertinente și concludente, în vederea modificării și completării prezentului cod de conduită.