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. 1 din 22.07.2015
Aprobat:	Senatul UVT	Hotărâre nr. 63 din 28.07.2015
Ediția 1		
Intrat în vigoare la data de …28.07.2015…..		
Retras la data de ……..…..		

CAPITOLUL I: DISPOZIŢII GENERALE

Scopul și sfera de aplicare

Art. 1

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

(2) Exercitarea drepturilor prevăzute în prezentul Regulament nu poate fi restrânsă decât în cazuri expres şi 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 şi prelucrării prin alte mijloace decât cele automate a datelor cu caracter personal care fac parte dintr-un sistem de evidenţă 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 peroanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date, modificată)

a) **date cu caracter personal** - orice informaţii 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 mulţi factori specifici identităţii sale fizice, fiziologice, psihice, economice, culturale sau sociale;
b) **prelucrarea datelor cu caracter personal** - orice operaţiune sau set de operaţiuni 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 terţi prin transmitere, diseminare sau în orice alt mod, alăturarea ori combinarea, blocarea, ştergerea sau distrugerea;

c) **stocarea -** păstrarea pe orice fel de suport a datelor cu caracter personal culese;
d) **sistem de evidenţă 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 funcţionale ori geografice;
e) **operator** - orice persoană fizică sau juridică, de drept privat ori de drept public, inclusiv autorităţile publice, instituţiile şi structurile teritoriale ale acestora, care stabileşte scopul şi mijloacele de prelucrare a datelor cu caracter personal; dacă scopul şi 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 autorităţile publice, instituţiile şi structurile teritoriale ale acestora, care prelucrează date cu caracter personal pe seama operatorului;
g) **terţ** - orice persoană fizică sau juridică, de drept privat ori de drept public, inclusiv autorităţile publice, instituţiile şi 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 autorităţile publice, instituţiile şi structurile teritoriale ale acestora, căreia îi sunt dezvăluite date, indiferent dacă este sau nu terţ; autorităţile publice cărora li se comunică date în cadrul unei competenţe speciale de anchetă nu vor fi considerate destinatari;
i) **date anonime** - date care, datorită originii sau modalităţii 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) candidaţi la admitere în cadrul UVT (pentru toate ciclurile de studiiuniversitare – licenţă, masterat, doctorat),

ii) studenţi declaraţi admişi şi înmatriculaţi la UVT (pentru toate ciclurile de studii universitare – licenţă, 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 facultăţilor, 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 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 comportă 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.

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-credinţă** şi în conformitate cu dispoziţiile legale în vigoare;

b) **colectate** în scopuri determinate, explicite şi legitime; prelucrarea ulterioară a datelor cu caracter personal în scopuri statistice, de cercetare istorică sau ştiinţifică nu va fi considerată incompatibilă cu scopul colectării dacă se efectuează cu respectarea dispoziţiilor 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 ştiinţifică;

c) **adecvate, pertinente şi neexcesive** prin raportare la scopul în care sunt colectate şi ulterior prelucrate;

d) **exacte şi, 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 şi pentru care vor fi ulterior prelucrate, să fie şterse sau rectificate;

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

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

B. Condiţii de legitimitate privind prelucrarea datelor

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

(2) **Consimţământul** 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 vieţii, integrităţii fizice sau sănătăţii persoanei vizate ori a unei alte persoane ameninţate;

c) când prelucrarea este necesară în vederea îndeplinirii unei obligaţii 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 învestit operatorul sau terţul căruia îi sunt dezvăluite datele;

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

f) când prelucrarea priveşte date obţinute din documente accesibile publicului, conform legii;

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

(3) Prevederile alin. (2) nu aduc atingere dispoziţiilor legale care reglementează obligaţia UVT, în calitate de operator, de a respecta şi de a ocroti viaţa intimă, familială şi privată.

C. Încheierea operaţiunilor de prelucrare

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

a) distruse;

b) transferate unui alt operator, cu condiţia ca operatorul iniţial să garanteze faptul că prelucrările ulterioare au scopuri similare celor în care s-a făcut prelucrarea iniţială;

c) transformate în date anonime şi stocate exclusiv în scopuri statistice, de cercetare istorică sau ştiinţifică.

(2) În cazul operaţiunilor de prelucrare efectuate în condiţiile 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 condiţia asigurării unor măsuri corespunzătoare de protejare a acestora, după care va proceda la distrugerea lor dacă nu sunt aplicabile prevederile legale privind păstrarea arhivelor.

CAPITOLULV
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 apartenenţa

sindicală, precum şi a datelor cu caracter personal privind starea de sănătate sau viaţa sexuală este interzisă.

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

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

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

c) când prelucrarea este necesară pentru protecţia vieţii, integrităţii fizice sau a sănătăţii persoanei vizate ori a altei persoane, în cazul în care persoana vizată se află în incapacitate fizică sau juridică de a-şi da consimţământul;

d) când prelucrarea este efectuată în cadrul activităţilor sale legitime de către o fundaţie, asociaţie sau de către orice altă organizaţie cu scop nelucrativ şi cu specific politic, filozofic, religios ori sindical, cu condiţia ca persoana vizată să fie membră a acestei organizaţii sau să întreţină cu aceasta, în mod regulat, relaţii care privesc specificul activităţii organizaţiei şi ca datele să nu fie dezvăluite unor terţi fără consimţământul 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 justiţie;

g) când prelucrarea este necesară în scopuri de medicină preventivă, de stabilire a diagnosticelor medicale, de administrare a unor îngrijiri sau tratamente medicale pentru persoana vizată ori de gestionare a serviciilor de sănătate care acţionează în interesul persoanei vizate, cu condiţia 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 obligaţii echivalente în ceea ce priveşte secretul;

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

(3) Prevederile alin. (2) nu aduc atingere dispoziţiilor legale care reglementează obligaţia autorităţilor publice de a respecta şi de a ocroti viaţa intimă, familială şi privată.

B. Prelucrarea datelor cu caracter personal având funcţie de identificare

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

a) persoana vizată şi-a dat în mod expres consimţământul;

b) prelucrarea este prevăzută în mod expres de o dispoziţie 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 funcţie de identificare de aplicabilitate generală nu se aplică în privinţa prelucrării datelor privind starea de sănătate în următoarele cazuri:

a) dacă prelucrarea este necesară pentru protecţia sănătăţii publice;

b) dacă prelucrarea este necesară pentru prevenirea unui pericol iminent, pentru prevenirea săvârşirii 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 condiţia respectării secretului profesional, cu excepţia situaţiei în care persoana vizată şi-a dat în scris şi în mod neechivoc consimţământul atât timp cât acest consimţământ nu a fost retras, precum şi cu excepţia situaţiei în care prelucrarea este necesară pentru prevenirea unui pericol iminent, pentru prevenirea săvârşirii 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 excepţie, 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 contravenţii

Art. 11. - (1) Prelucrarea datelor cu caracter personal referitoare la săvârşirea de infracţiuni de către persoana vizată ori la condamnări penale, măsuri de siguranţă sau sancţiuni administrative ori contravenţionale, aplicate persoanei vizate, poate fi efectuată numai de către sau sub controlul autorităţilor publice, în limitele puterilor ce le sunt conferite prin lege şi în condiţiile stabilite de legile speciale care reglementează aceste materii.

CAPITOLULVI

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 obţinute direct de la persoana vizată, UVT în calitate de operator este obligat să furnizeze persoanei vizate cel puţin următoarele informaţii, cu excepţia cazului în care această persoană posedă deja informaţiile respective:

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

b) scopul în care se face prelucrarea datelor;

c) informaţii suplimentare, precum: destinatarii sau categoriile de destinatari ai datelor; dacă furnizarea tuturor datelor cerute este obligatorie şi consecinţele refuzului de a le furniza; existenţa drepturilor prevăzute de prezenta lege pentru persoana vizată, în special a dreptului de acces, de intervenţie asupra datelor şi de opoziţie, precum şi condiţiile în care pot fi exercitate;

d) orice alte informaţii a căror furnizare este impusă prin dispoziţie a autorităţii de supraveghere, ţinând seama de specificul prelucrării.

(2) În cazul în care datele nu sunt obţinute direct de la persoana vizată, operatorul este obligat ca, în momentul colectării datelor sau, dacă se intenţionează dezvăluirea acestora

către terţi, cel mai târziu până în momentul primei dezvăluiri, să furnizeze persoanei vizate cel puţin următoarele informaţii, cu excepţia cazului în care persoana vizată posedă deja informaţiile respective:

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

b) scopul în care se face prelucrarea datelor;

c) informaţii suplimentare, precum: categoriile de date vizate, destinatarii sau categoriile de destinatari ai datelor, existenţa drepturilor prevăzute de prezenta lege pentru persoana vizată, în special a dreptului de acces, de intervenţie asupra datelor şi de opoziţie, precum şi condiţiile în care pot fi exercitate;

d) orice alte informaţii a căror furnizare este impusă prin dispoziţie a autorităţii de supraveghere, ţinând 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 ştiinţifică, ori în orice alte situaţii în care furnizarea unor asemenea informaţii se dovedeşte imposibilă sau ar implica un efort disproporţionat faţă de interesul legitim care ar putea fi lezat, precum şi în situaţiile în care înregistrarea sau dezvăluirea datelor este expres prevăzută de lege.

B. Dreptul de acces la date

Art. 13. - (1) Orice persoană vizată are dreptul de a obţine de la operator, la cerere şi 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 situaţia în care prelucrează date cu caracter personal care privesc solicitantul, să comunice acestuia, împreună cu confirmarea, cel puţin următoarele:

a) informaţii referitoare la scopurile prelucrării, categoriile de date avute în vedere şi destinatarii sau categoriile de destinatari cărora le sunt dezvăluite datele;

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

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

d) informaţii privind existenţa dreptului de intervenţie asupra datelor şi a dreptului de opoziţie, precum şi condiţiile în care pot fi exercitate;

e) informaţii asupra posibilităţii de a consulta registrul de evidenţă a prelucrărilor de date cu caracter personal, de a înainta plângere către autoritatea de supraveghere, precum şi de a se adresa instanţei pentru atacarea deciziilor operatorului, în conformitate cu dispoziţiile prezentei legi.

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

(3) Operatorul este obligat să comunice informaţiile solicitate, în termen de 15 zile de la data primirii cererii, cu respectarea eventualei opţiuni 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 ştiinţifică, dacă nu există, cel puţin aparent, riscul de a se aduce atingere drepturilor persoanei vizate şi dacă datele nu sunt utilizate pentru a lua decizii sau măsuri faţă de o anumită persoană, comunicarea prevăzută la alin. (3) se poate face şi 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 îşi fi dat în mod expres şi neechivoc consimţământul ca datele să fie prelucrate în scop de cercetare ştiinţifică, precum şi 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 intervenţie asupra datelor

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

a) după caz, rectificarea, actualizarea, blocarea sau ştergerea 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 terţii cărora le-au fost dezvăluite datele a oricărei operaţiuni efectuate conform lit. a) sau b), dacă această notificare nu se dovedeşte imposibilă sau nu presupune un efort disproporţionat faţă 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 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.

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

D. Dreptul de opoziţie

Art. 15. - (1) Persoana vizată are dreptul de a se opune în orice moment, din motive întemeiate şi legitime legate de situaţia sa particulară, ca date care 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.

(2) 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.

(3) În vederea exercitării drepturilor prevăzute la alin. (1) şi (2) 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.

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

E. Dreptul de a nu fi supus unei decizii individuale

Art. 16. - (1) Orice persoană are dreptul de a cere şi de a obţine:

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

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

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

a) decizia este luată în cadrul încheierii sau executării unui contract, cu condiţia 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-şi susţine 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.

CAPITOLULVII
Confidenţialitatea şi securitatea prelucrărilor

A. Confidenţialitatea prelucrărilor

Art. 17. - Orice persoană care acţionează 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 instrucţiunilor operatorului, cu excepţia cazului în care acţionează în temeiul unei obligaţii legale.

B. Securitatea prelucrărilor

Art. 18. - (1) Operatorul este obligat să aplice măsurile tehnice şi 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 transmisii de date în cadrul unei reţele, precum şi împotriva oricărei alte forme de prelucrare ilegală.

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

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

a) obligaţia persoanei împuternicite de a acţiona doar în baza instrucţiunilor primite de la operator;

b) faptul că îndeplinirea obligaţiilor prevăzute la alin. (1) revine şi persoanei împuternicite.

CAPITOLUL VIII

Notificarea către autoritatea de supraveghere

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

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

(3) Notificarea va cuprinde cel puţin următoarele informaţii:

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

b) scopul sau scopurile prelucrării;

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

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

e) garanţiile care însoţesc dezvăluirea datelor către terţi;

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

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

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

i) specificarea oricărui sistem de evidenţă a datelor cu caracter personal, care are legătură cu prelucrarea, precum şi a eventualelor legături cu alte prelucrări de date sau cu alte sisteme de evidenţă 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 situaţia în care prelucrarea datelor se face exclusiv în scopuri jurnalistice, literare sau artistice ori în scopuri statistice, de cercetare istorică sau ştiinţifică.

(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 şi alte informaţii, în special privind originea datelor, tehnologia de prelucrare automată utilizată şi detalii referitoare la măsurile de securitate. Dispoziţiile prezentului alineat nu se aplică în situaţia în care prelucrarea datelor se face exclusiv în scopuri jurnalistice, literare sau artistice.

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

a) categoriile de date care vor face obiectul transferului;

b) ţara de destinaţie 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 obligaţia respectivă şi va cuprinde numai următoarele elemente:

a) denumirea şi sediul operatorului;

b) scopul şi temeiul legal al prelucrării;

c) categoriile de date cu caracter personal supuse prelucrării.

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

a) atunci când, luând în considerare natura datelor destinate să fie prelucrate, prelucrarea nu poate afecta, cel puţin aparent, drepturile persoanelor vizate, cu condiţia 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 şi perioada pentru care datele pot fi stocate;

b)când prelucrarea este efectuată în cadrul activităţilor sale legitime de către o fundaţie, asociaţie sau de către orice altă organizaţie cu scop nelucrativ şi cu specific politic, filozofic, religios ori sindical, cu condiţia ca persoana vizată să fie membră a acestei organizaţii sau să întreţină cu aceasta, în mod regulat, relaţii care privesc specificul activităţii organizaţiei şi ca datele să nu fie dezvăluite unor terţi fără consimţământul persoanei vizate;

CAPITOLUL IX

Supravegherea şi controlul prelucrărilor de date cu caracter personal

Autoritatea de supraveghere

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

(2) Autoritatea de supraveghere îşi desfăşoară activitatea în condiţii de completă independenţă şi imparţialitate.

(3) Autoritatea de supraveghere monitorizează şi controlează sub aspectul legalităţii prelucrările de date cu caracter personal care cad sub incidenţa prezentei legi.

CAPITOLUL X

Transferul în străinătate al datelor cu caracter personal

Condiţiile 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 condiţiile în care nu se încalcă legea română, iar statul către care se intenţionează transferul asigură un nivel de protecţie adecvat.

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

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

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

CAPITOLUL XI

Soluționarea plângerilor

A. Plângeri adresate Autorităţii 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 incidenţa regulamentului, pot înainta plângere către autoritatea de supraveghere. Plângerea se poate face direct sau prin reprezentant. Persoana lezată poate împuternici o asociaţie sau o fundaţie să îi reprezinte interesele.

(2) Plângerea către autoritatea de supraveghere nu poate fi înaintată dacă o cerere în justiţie, având acelaşi obiect şi aceleaşi părţi, a fost introdusă anterior.

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

(4) În vederea soluţionării plângerii, dacă apreciază că este necesar, autoritatea de supraveghere poate audia persoana vizată, operatorul şi, dacă este cazul, persoana împuternicită sau asociaţia ori fundaţia care reprezintă interesele persoanei vizate. Aceste persoane au dreptul de a înainta cereri, documente şi 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. Interdicţia temporară a prelucrării poate fi instituită numai până la încetarea motivelor care au determinat luarea acestei măsuri.

(6) Decizia trebuie motivată şi se comunică părţilor 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 operaţiunilor de prelucrare până la soluţionarea plângerii în condiţiile alin. (5).

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

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

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

B. Contestarea deciziilor autorităţii de supraveghere

Art. 23. - (1) Împotriva oricărei decizii emise de autoritatea de supraveghere în temeiul dispoziţiilor prezentei legi operatorul sau persoana vizată poate formula contestaţie în termen de 15 zile de la comunicare, sub sancţiunea decăderii, la instanţa de contencios administrativ competentă. Cererea se judecă de urgenţă, cu citarea părţilor. Soluţia este definitivă şi irevocabilă.

C. Dreptul de a se adresa justiţiei

Art. 24. - (1) Fără a se aduce atingere posibilităţii de a se adresa cu plângere autorităţii de supraveghere, persoanele vizate au dreptul de a se adresa justiţiei 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 instanţei competente pentru repararea acestuia.

(3) Instanţa 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 28.04.2015

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

CERINŢELE MINIME DE SECURITATE a prelucrărilor de date cu caracter personal

Prezentele cerinţe minime de securitate a prelucrărilor de date cu caracter personal trebuie să stea la baza adoptării şi implementării de către operator a măsurilor tehnice şi organizatorice necesare pentru păstrarea confidenţialităţii şi integrităţii datelor cu caracter personal. În concordanţă cu acestea operatorii îşi vor stabili propriile politici şi proceduri de securitate.

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

1. Identificarea şi autentificarea utilizatorului

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.

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.

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

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.

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.

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.

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

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.

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

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.

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

2. Tipul de acces

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.

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 excepţionale.

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.

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.

3. Colectarea datelor

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

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

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.

4. Execuţia copiilor de siguranţă

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.

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

5. Computerele şi terminalele de acces

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.

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.

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.

6. Fişierele de acces

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).

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.

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.

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.

7. Sistemele de telecomunicaţii

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

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.

Prin sistemele de telecomunicaţii 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 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.

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.

9. Folosirea computerelor

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.

10. Imprimarea datelor

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.

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.

Anexa 2

DECLARAŢIE

Subsemnatul _____, în calitate de candidat la admitere/student declarat admis şi înmatriculat pentru ciclul de studii universitare[2]_____, anul universitar _____ declar că am luat la cunoştinţă de dispoziţiile legii nr. 677/2001 privind prelucrarea datelor cu caracter personal precum şi de conţinutul informării Universităţii de Vest din Timişoara cu privire la aceste date (informare aflată pe verso) şi declar că sunt de acord ca aceste date cu caracter personal sa fie stocate, prelucrate, utilizate şi publicate.

Declar, susţin şi semnez după ce am luat la cunoştinţă, sunt de acord cu întregul conţinut şi am completat personal datele din prezenta declaraţie.

Semnătura _____

Data _____

[2] Se va completa, dupa caz licenţă/masterat/doctorat, precum şi facultatea, respectiv domeniul de studii

Anexa 3

INFORMARE

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

Conform cerinţelor Legii nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date, modificată completată şi ale Legii nr. 506/2004 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul comunicaţiilor electronice UVT are obligaţia de a administra în condiţii de siguranţă şi 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 educaţie şi cultură,

în sensul iniţierii şi derulării de raporturi juridice între dumneavoastă şi UVT;

B) în vederea îmbuntătăţirii modului de comunicare cu studenţii, prin intermediul

poştei electronice, pentru comunicarea operativă şi eficientă a informaţiilor

necesare derulării raporturilor contractuale dintre dumneavoastră şi UVT.

Sunteţi obligat să furnizaţi datele enunţate, deoarece în cazul nefurnizării

corecte şi complete a acestora, UVT poate să refuze iniţierea de raporturi juridice cu dumneavoastră, întrucât poate fi pusă în imposibilitatea de a respecta cerinţele

reglementărilor speciale in domeniul educaţional.

Informaţiile înregistrate sunt destinate utilizării de către operator şi sunt

comunicate numai următorilor destinatari:

- persoana vizată
- partenerii contractuali ai operatorului
- instituţii de învăţământ şi educaţie

Conform Legii nr. 677/2001, beneficiaţi de dreptul de acces, de intervenţie

asupra datelor şi de dreptul de a nu fi supus unei decizii individuale. Totodată, aveţi dreptul să vă opuneţi prelucrării datelor personale care vă privesc şi să solicitaţi ştergerea datelor, cu excepţia situaţiilor prevăzute expres de lege, când prelucrarea datelor de către UVT este obligatorie. Pentru exercitarea acestor drepturi, vă puteţi adresa cu o cerere scrisă, datată şi semnată către Secretariatul General al UVT, care va înainta solicitarea dumneavoastră conducerii UVT.

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

Anexa 4

DECLARAŢIE

Subsemnatul _____, fiul lui _____

şi al _____, născut la data de _____ în localitatea _____, judeţul / 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 cunoştinţă de dispoziţiile legii nr. 677/2001 privind prelucrarea datelor cu caracter personal precum şi de conţinutul informării Universităţii de Vest din Timişoara cu privire la aceste date şi declar că sunt de acord ca aceste date cu caracter personal să fie stocate, prelucrate, utilizate şi publicate.

Declar, susţin şi semnez după ce am luat la cunoştinţă de întregul conţinut

şi am completat personal datele din prezenta declaraţie.

Semnătura _____

Data _____

[4] studii finanţate din Proiectul nr. ....., ID proiect ....., cu titlul ....., din cadrul Programului Operaţional Sectorial Dezvoltarea Resurselor Umane 2007-2013 nr. CCI 2007 RO051PO001, selectat în cadrul Programului Operaţional Sectorial Dezvoltarea Resurselor Umane (POS DRU) şi cofinanţat din „Fondul Social European" (FSE)

Anexa 5

INFORMARE

Universitatea de Vest din Timişoara cu sediul în Timişoara, 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 finanţate din Proiectul „Burse doctorale", ID, cu titlul „Racordarea programelor de studii doctorale la studiile doctorale europene, din cadrul Programului Operaţional Sectorial Dezvoltarea Resurselor Umane, selectat în cadrul Programului Operaţional Sectorial Dezvoltarea Resurselor Umane (POS DRU) şi cofinanţat din „Fondul Social European"(FSE), în conformitate cu prevederile Directivei CE/95/46 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date, transpusă în legislaţia naţională prin Legea nr.677/2001, precum şi prevederile Directivei 2002/58/CE privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul comunicaţiilor electronice, transpusă în legislaţia naţională 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 Operaţional Sector Dezvoltarea Resurselor Umane, selectat în cadrul Programului Operaţional Sectorial Dezvoltarea Resurselor Umane (POS DRU) şi cofinanţat din, Universitatea de Vest din Timișoara, în calitate de beneficiar al contractului de finanţare POSDRU are obligaţia de a transmite AMPOSDRU, informaţii privind participanţii în conformitate cu Regulamentul Comisiei (CE) nr.1828/2006 cu privire la implementarea Regulamentului Consiliului (CE) nr.1083/2006 privind dispoziţiile generale cu privire la Fondul European de Dezvoltare Regională, Fondul Social European şi Fondul de Coeziune şi al Regulamentului Parlamentului European şi al Consiliului nr.1080/2006 privind Fondul European de Dezvoltare Regională.

În acest sens, în calitate de beneficiar, Universitatea de Vest din Timişoara va centraliza şi transmite informaţii privind participanţii pentru fiecare an de implementare a proiectului, utilizând următoarele criterii: gen,statut ocupaţional, grupe de vârstă, apartenenţa la grup vulnerabil, nivel de educaţie, în baza

formularelor completate de către participanţi (doctoranzi), utilizând formatul

standard furnizat de AMPOSDRU.

În vederea realizării obiectivelor propuse şi îndeplinirii condiţiilor mai sus

menţionate, în calitate de doctorand, persoana din grupul ţintă al proiectului, are

obligaţia de a furniza datele personale, cu respectarea dispoziţiilor legale în

materie.

Anexa 6

COD DE CONDUITĂ

Preambul

Luând în considerare importanţa deosebită a garantării dreptului la viaţă intimă, familială şi privată, aşa cum este prevăzut la art. 26 din Constituţia României,

ţinând seama de necesitatea protejării acestui drept fundamental în cadrul activităţilor de prelucrare a datelor cu caracter personal, reglementate prin Legea nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date, precum şi prin Legea nr. 682/2001 privind ratificarea Convenţiei pentru protejarea persoanelor faţă de prelucrarea automatizată a datelor cu caracter personal, adoptată la Strasbourg la 28 ianuarie 1981.

CAPITOLUL I Dispoziţii generale

Scopul şi sfera de aplicare

Art. 1. -

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

(2) Normele de conduită stabilesc exercitarea drepturilor şi obligaţiilor în domeniul protecţiei persoanelor în privinţa datelor cu caracter personal, în relaţiile 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 obligaţii legale imperative sau deontologice care revin asociaţiilor profesionale.

Definirea termenilor

Art. 2. -

(1) Termenii folosiţi 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 şi 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 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 comportă 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 implementării acestor măsuri;

g) marketing direct - promovarea produselor şi a serviciilor, adresată direct clienţilor, persoane fizice, prin mijloace de genul poştei, inclusiv cea electronică, sau alte mijloace de marketing la distanţă, altele decât modalităţile promoţionale obişnuite (reclame).

(2) 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.

Cadrul legal al codurilor de conduită

Art. 3. -

Vor fi respectate dispoziţiile legale referitoare la protecţia dreptului la viaţă intimă, familială şi privată, în ceea ce priveşte prelucrarea datelor cu caracter personal. Se vor avea în vedere în mod special dispoziţiile Legii nr. 677/2001, precum şi ale Legii nr. 682/2001.

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

Legalitatea şi transparenţa

Art. 5. -

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

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

(3) Universitatea de Vest din Timișoaraeste obligată să asigure transparenţa prelucrărilor de date cu caracter personal.

Responsabilitatea

Art. 6. -

(1) Universitatea de Vest din Timișoaraeste responsabilă pentru datele cu caracter personal aflate sub controlul său, precum şi pentru datele transferate către terţi.

(2) Universitatea de Vest din Timișoara va desemna 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 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) Menţionarea scopurilor poate fi realizată în scris, oral sau în formă electronică, într-un limbaj uşor accesibil pentru persoanele vizate.

Consimţământul

Art. 8. -

(1) Consimţământul 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 şi pentru a solicita consimţământul acestora la momentul

colectării datelor cu caracter personal.

(3) Persoana vizată îşi poate retrage consimţământul în orice moment, sub condiţia avizării prealabile a operatorului. Acesta va informa persoana vizată în legătură cu procedura şi efectele retragerii consimţământului.

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 excepţia cazului în care persoana vizată îşi dă consimţământul pentru prelucrarea în alte scopuri sau în alte cazuri permise de lege.

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

Legitimitatea stocării

Art. 10. -

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

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

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

(4) Universitatea de Vest din Timișoarastabilește 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 intervenţie şi de opoziţie.

(5) 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.

Securitatea prelucrărilor

Art. 11. -

Universitatea de Vest din Timișoarava 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 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 circulaţie necontrolată a datelor.

Dreptul de informare

Art. 12. -

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

(2) Universitatea de Vest din Timișoara va comunica informaţii, 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 şi cărui terţ 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 judecătoreşti), Universitatea de Vest din Timișoara se va asigura că terţul care solicită dezvăluirea acţionează în conformitate cu dispoziţiile legale incidente, iar cererea priveşte 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 dispoziţie, în mod rezonabil.

(2) Accesul persoanei vizate nu poate fi permis, cu excepţia cazurilor prevăzute de lege, în următoarele situaţii: în cazul în care sunt solicitate date despre o altă persoană; în cazul în care ar putea fi afectate viaţa şi siguranţa altei persoane; în cazul în care sunt solicitate date care pot privi informaţii comerciale confidenţiale; în cazul în care s-ar aduce atingere soluţionării unui litigiu sau a unui proces penal.

(3) Universitatea de Vest din Timișoaraeste obligată să motiveze refuzul de a permite

accesul la anumite date cu caracter personal.

Dreptul de intervenţie

Art. 14. -

(1) 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 sau incomplete, prin formularea unor contestaţii.

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

(3) Dispoziţiile alin. (2) se aplică şi în cazul dezvăluirii de date către terţi, dacă este cazul.

(4) 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.

Colaborarea cu autoritatea de supraveghere

Art. 15. -

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

(2) Rapoartele şi sintezele la care se referă alin. (1) vor putea conţine şi alte informaţii privind aspecte din activitatea membrilor în domeniul protecţiei datelor cu caracter personal, precum şi propuneri de îmbunătăţire a activităţii 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 excepţia cazului în care aceste drepturi pot fi exercitate în mod

gratuit.

CAPITOLUL III Dispoziţii finale şi tranzitorii

Modul de aplicare

Art. 17. -

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

Modificarea şi completarea modelului de cod de conduită

Art. 18. -

(1) Modificările sau completările ale prezentuluide cod de conduit, vor fi trimise, în scris şi motivat, autorităţii de supraveghere.

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