REGULAMENTUL INTERN PRIVIND PRELUCRAREA DATELOR CU CARACTER PERSONAL/GDPR

-As. -U.B.C.A.R.-

PITEȘTI,
2026

CAPITOLUL I – DISPOZIȚII GENERALE

TITLUL I – Cadrul juridic

Art. 1 – Baza legală

(1) Prezentul Regulament este adoptat în temeiul următoarelor acte normative aplicabile:

a) Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 (GDPR), cu aplicabilitate directă în toate statele membre ale Uniunii Europene;
b) Legea nr. 190/2018 privind măsuri de punere în aplicare a GDPR în România;
c) Legea nr. 363/2018 privind protecția persoanelor fizice față de prelucrarea datelor cu caracter personal în cadrul instituțiilor publice și private (după caz);
d) Legea nr. 102/2005 privind Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal;
e) Legea nr. 16/1996 privind Arhivele Naționale;
f) Legea contabilității nr. 82/1991, Codul muncii și alte reglementări incidente (fiscale, administrative, asociative).

(2) Regulamentul completează prevederile Statutului și ale Regulamentului de Organizare și Funcționare (ROF) ale U.B.C.A.R., având caracter normativ intern obligatoriu pentru toate structurile centrale și teritoriale, precum și pentru:

a) membrii înscriși în Asociație;
b) personalul angajat cu contract individual de muncă;
c) colaboratorii contractuali (inclusiv furnizori, parteneri și prestatori de servicii);
d) voluntarii și persoanele mandatate să acționeze în numele Asociației.

(3) Orice activitate de prelucrare a datelor cu caracter personal în cadrul U.B.C.A.R. se supune prezentului Regulament, indiferent de suportul utilizat (electronic, hârtie, audio-video, baze de date informatice).

Art. 2 – Obiect și scop

(1) Prezentul Regulament stabilește:

a) cadrul legal și organizatoric privind protecția datelor cu caracter personal în cadrul U.B.C.A.R.;
b) principiile de prelucrare a datelor;
c) responsabilitățile organelor centrale, teritoriale și ale persoanelor autorizate;
d) drepturile persoanelor vizate și modalitățile de exercitare a acestora;
e) măsurile tehnice și organizatorice de securitate și confidențialitate;
f) procedura de notificare și gestionare a incidentelor de securitate.

(2) Scopul adoptării prezentului Regulament este:

a) asigurarea unui nivel înalt de protecție a datelor membrilor, personalului și beneficiarilor;
b) prevenirea incidentelor și a riscurilor de sancțiuni legale sau prejudicii de imagine;
c) conformarea cu cerințele Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP) și cu standardele europene;
d) garantarea transparenței, integrității și responsabilității în cadrul U.B.C.A.R.

TITLUL II – Aplicabilitate

Art. 3 – Domeniu de aplicare

(1) Regulamentul se aplică:

a) la nivel central – CNC, CEN, SFN/AG și toate departamentele;
b) la nivel teritorial – filiale, comunități regionale, case de rugăciune, unități de cult afiliate;
c) în relația cu partenerii, colaboratorii și furnizorii care, în baza unui contract, prelucrează date în numele U.B.C.A.R. (împuterniciți).

(2) Prevederile prezentului Regulament se aplică **atât în mediul fizic, cât și în mediul digital**, inclusiv pentru:

- baze de date informatice și sisteme de arhivare electronică;
- comunicări prin e-mail, rețele sociale, aplicații de mesagerie;
- supraveghere video în spațiile deținute sau utilizate de Asociație;
- materiale foto-video realizate în cadrul evenimentelor religioase, sociale sau educaționale.

Art. 4 – Definiții
În sensul prezentului Regulament, termenii au înțelesul prevăzut de GDPR. În plus:

a) ***operator*** **–** U.B.C.A.R., prin structurile sale centrale și teritoriale, în calitate de entitate care stabilește scopurile și mijloacele de prelucrare;
b) ***persoană vizată*** **–** orice membru, angajat, voluntar, colaborator sau beneficiar ale cărui date sunt prelucrate;
c) ***împuternicit*** **–** orice persoană fizică sau juridică ce prelucrează date în numele U.B.C.A.R., în baza unui contract scris;
d) ***incident de securitate*** **–** orice încălcare a securității care duce la distrugerea, pierderea, modificarea, divulgarea neautorizată sau accesul neautorizat la datele personale.

Titlul III – Norme de interpretare și aplicare

Art. 5 – Principiul prevalenței legii
(1) În caz de conflict între prevederile prezentului Regulament și dispozițiile legale incidente, prevalează normele legale.
(2) În caz de conflict între Statut, ROF și prezentul Regulament, prevalează Statutul, iar în lipsa unor dispoziții clare – legislația aplicabilă și GDPR.

Art. 6 – Interpretare, adaptabilitate și confidențialitate
(1) Prezentul Regulament se interpretează în conformitate cu:

a) dispozițiile GDPR și legislația națională aplicabilă;
b) jurisprudența Curții de Justiție a Uniunii Europene și a Curții Europene a Drepturilor Omului;
c) principiile consacrate de Carta Drepturilor Fundamentale a Uniunii Europene și de Constituția României.

(2) În cazul în care una dintre dispozițiile prezentului Regulament devine inaplicabilă ca urmare a modificării cadrului legal, aceasta se consideră de drept completată și adaptată prin normele legale imperative în vigoare (clauză de adaptabilitate).
(3) U.B.C.A.R. are obligația de a demonstra conformitatea cu GDPR prin evidențe (registre de prelucrare, politici interne, traininguri și instruiri periodice), potrivit principiului responsabilității.
(4) Orice persoană care are acces la date cu caracter personal în baza unei funcții, atribuții sau contract (angajați, voluntari, colaboratori, împuterniciți) are obligația de confidențialitate, pe durata raportului juridic și ulterior încetării acestuia.
(5) Responsabilul cu protecția datelor (DPO), desemnat potrivit art. 37–39 GDPR, asigură monitorizarea aplicării prezentului Regulament și are independența necesară pentru a-și exercita atribuțiile.

Art. 6¹ – Principiul responsabilității proactive (accountability)
(1) U.B.C.A.R. își asumă responsabilitatea de a asigura și demonstra conformitatea cu GDPR și cu prezentul Regulament.
(2) Operatorul menține documentația necesară pentru a putea dovedi respectarea principiilor de prelucrare, inclusiv registre, politici, proceduri și rapoarte de audit.
(3) Dovada conformității este pusă la dispoziția ANSPDCP la solicitare.

CAPITOLUL II – PRINCIPII ȘI SCOPURI ALE PRELUCRĂRII

TITLUL I – Principii fundamentale

Art. 7 – Principii generale de prelucrare

(1) U.B.C.A.R. respectă următoarele principii fundamentale ale prelucrării datelor cu caracter personal, conform art. 5 GDPR:

a) **Legalitate, echitate și transparență** – datele sunt prelucrate în mod legal, corect și transparent față de persoana vizată;
b) **Limitarea scopului** – datele sunt colectate numai în scopuri determinate, explicite și legitime, fără a fi ulterior prelucrate într-un mod incompatibil cu aceste scopuri;
c) **Reducerea la minimum a datelor** – se colectează doar datele strict necesare realizării scopurilor;
d) **Exactitate** – datele sunt corecte și, dacă este necesar, actualizate, cu obligația de a rectifica sau șterge fără întârziere datele inexacte;
e) **Limitarea stocării** – datele se păstrează doar pe perioada necesară îndeplinirii scopurilor, cu respectarea termenelor legale de arhivare;
f) **Integritate și confidențialitate** – datele sunt protejate împotriva accesului neautorizat, distrugerii sau pierderii, prin măsuri tehnice și organizatorice adecvate;
g) **Responsabilitate (accountability)** – U.B.C.A.R. este responsabilă de respectarea principiilor și trebuie să poată demonstra această conformitate prin registre, proceduri și audituri interne.

(2) Încălcarea principiilor prevăzute la alin. (1) atrage răspunderea persoanelor implicate, disciplinară, civilă sau penală, după caz.

Titlul II – Scopuri legitime ale prelucrării

Art. 8 – Scopuri generale

(1) Datele cu caracter personal sunt prelucrate de U.B.C.A.R. în următoarele scopuri legitime:

a) evidența membrilor și a structurilor afiliate (filiale, comunități, case de rugăciune);
b) organizarea și desfășurarea activităților religioase, spirituale și comunitare;
c) gestionarea activităților sociale, educaționale, medicale și caritabile;
d) administrarea resurselor umane (angajați, voluntari, colaboratori);
e) gestionarea contractelor, parteneriatelor și furnizorilor de servicii;
f) respectarea obligațiilor legale în domeniile fiscal, contabil, arhivistic și al muncii;
g) comunicarea internă și externă, inclusiv prin materiale promoționale și mijloace digitale, cu respectarea dreptului la imagine și a normelor GDPR;
h) protecția intereselor vitale ale persoanelor vizate sau ale altor persoane (ex. situații medicale, de urgență).

(2) Orice prelucrare de date în alte scopuri decât cele menționate la alin. (1) necesită:

a) consimțământ explicit al persoanei vizate; sau
b) existența unui temei legal expres prevăzut de GDPR ori de legislația națională.

Titlul III – Prelucrarea categoriilor speciale de date

Art. 9 – Prelucrarea de date

(1) U.B.C.A.R. în virtutea identității sale religioase și confesionale, prelucrează în mod legitim date speciale, în sensul art. 9 GDPR (ex. convingeri religioase, date de sănătate).

(2) Aceste date sunt prelucrate numai în următoarele situații:

a) pe baza consimțământului explicit al persoanei vizate;
b) în temeiul obligațiilor legale (ex. protecția socială, raportări către autorități);
c) în cadrul activităților legitime desfășurate de U.B.C.A.R., cu garanții adecvate de confidențialitate și acces limitat doar la personalul autorizat.

(3) Datele speciale nu sunt dezvăluite către terți fără consimțământ sau fără o bază legală expresă.

Titlul IV – Legalitatea prelucrării

Art. 10 – Legalitate

(1) Prelucrarea datelor personale se face în baza unuia dintre temeiurile prevăzute de art. 6 GDPR, respectiv:

a) consimțământul persoanei vizate;
b) executarea unui contract;
c) respectarea unei obligații legale;
d) protejarea intereselor vitale ale persoanei vizate;
e) îndeplinirea unei sarcini de interes public;
f) interesul legitim al U.B.C.A.R., în măsura în care nu prevalează drepturile și libertățile fundamentale ale persoanei vizate.

(2) În cazul prelucrărilor bazate pe consimțământ, acesta este:

a) liber exprimat, specific, informat și lipsit de ambiguitate;
b) consemnat în scris sau printr-o declarație electronică;
c) revocabil oricând, fără a afecta legalitatea prelucrării realizate anterior.

Titlul V – Transparență și protecția minorilor

Art. 11 – Transparența prelucrării

(1) Persoanele vizate sunt informate în mod clar și accesibil cu privire la scopurile, temeiurile și condițiile de prelucrare a datelor, prin note de informare afișate la sediul central și la structurile teritoriale, precum și prin publicarea pe site-ul oficial.
(2) În cazul activităților publice (evenimente religioase, educaționale, sociale), informarea se face prin afișe vizibile și/sau anunțuri publice, iar consimțământul se obține în scris acolo unde este obligatoriu.

Art. 12 – Prelucrarea datelor minorilor

(1) În cadrul activităților educaționale și spirituale destinate copiilor și tinerilor, prelucrarea datelor personale ale minorilor se face exclusiv cu acordul părinților sau tutorilor legali.
(2) Datele minorilor beneficiază de un regim de protecție sporit, iar accesul la acestea este limitat la personalul autorizat.

Titlul VI – Transferuri și utilizarea imaginilor

Art. 13 – Transferul de date

(1) Datele pot fi transmise către furnizori de servicii, autorități publice sau parteneri contractuali numai în baza unui temei legal și cu respectarea principiului minimizării.
(2) În cazul transferurilor de date către state membre ale Uniunii Europene sau Spațiului Economic European (SEE), se aplică direct normele GDPR.
(3) Orice transfer către state terțe sau organizații internaționale se realizează numai în condițiile art. 44–49 GDPR, cu garanții adecvate de protecție.

Art. 14 – Fotografiile și înregistrările video

(1) În cadrul evenimentelor religioase, educaționale sau sociale, fotografierea și filmarea participanților se realizează cu respectarea dreptului la viață privată și la imagine.
(2) Publicarea fotografiilor și materialelor video se face numai cu consimțământul persoanelor vizate sau pe baza informării generale prealabile, în condițiile legii.

Titlul VII – Retenția și securitatea datelor

Art. 15 – Perioadele de stocare

(1) Datele personale se păstrează numai pe perioada strict necesară realizării scopurilor pentru care au fost colectate, cu respectarea termenelor prevăzute de lege.

(2) Exemple de termene de păstrare:

a) documente contabile și fiscale – 10 ani;
b) evidența membrilor – pe durata calității de membru + 3 ani după încetare;
c) arhivele cu valoare religioasă, istorică sau culturală – pe durată nedeterminată, cu respectarea Legii Arhivelor Naționale;
d) datele voluntarilor și colaboratorilor – pe durata contractului + 3 ani;
e) datele foto-video – maximum 2 ani, cu excepția materialelor cu caracter arhivistic sau istoric.

Art. 16 – Obligații interne și registre de prelucrare

(1) A.R.–U.B.CA.R, prin organele sale centrale și teritoriale, are obligația de a ține un **Registru al activităților de prelucrare**, conform art. 30 GDPR, care cuprinde:

a) scopurile prelucrării;
b) categoriile de persoane vizate și de date;
c) destinatarii datelor;
d) perioadele de stocare;
e) măsurile de securitate aplicate.

(2) Accesul la datele cu caracter personal se realizează pe **nivele de autorizare**, stabilite prin decizie internă, astfel încât doar persoanele strict necesare să aibă acces la anumite categorii de date (ex.: evidența membrilor, contabilitate, resurse umane, date medicale).

(3) Orice contract încheiat de U.B.C.A.R. cu persoane împuternicite (furnizori IT, contabili, avocați, arhivari, servicii de cloud, prestatori de servicii) trebuie să conțină **clauze privind protecția datelor** conform art. 28 GDPR, inclusiv obligații de confidențialitate și măsuri de securitate.

(4) În cazul în care U.B.C.A.R. prelucrează date în **responsabilitate comună** cu alte entități (de ex. evenimente comune, parteneriate internaționale), se va încheia un acord scris care stabilește responsabilitățile fiecărei părți și modalitatea prin care persoanele vizate își pot exercita drepturile (art. 26 GDPR).

(5) Datele cu caracter personal de natură religioasă sau care dezvăluie convingerile persoanelor vizate sunt prelucrate exclusiv în scopurile statutare ale U.B.C.A.R. și nu pot fi utilizate în scop comercial, discriminatoriu sau contrar libertății religioase.

(6) Datele prelucrate electronic sunt protejate prin:

a) sisteme informatice securizate (parole complexe, autentificare pe două niveluri, criptare);
b) copii de siguranță periodice (backup-uri);
c) controlul accesului la echipamente și aplicații informatice.

(7) Consimțământul persoanelor vizate se actualizează atunci când scopul inițial al prelucrării se modifică sau se extinde, iar lipsa unui consimțământ valabil atrage încetarea imediată a prelucrării respective.

Art. 16[1] – Decizii individuale automatizate

(1) U.B.C.A.R. nu ia decizii care produc efecte juridice sau similare exclusiv pe baza unei prelucrări automatizate, inclusiv prin profilare, cu excepția situațiilor permise de art. 22 GDPR.

(2) În cazul utilizării unor procese automatizate (ex.: selecție digitală, aplicații IT), persoana vizată este informată în prealabil și are dreptul de a solicita intervenție umană.

CAPITOLUL III – DREPTURILE PERSOANELOR VIZATE

TITLUL I – Dreptul la informare și acces

Art. 17 – Dreptul la informare

(1) Persoanele vizate au dreptul de a fi informate în mod concis, transparent și accesibil cu privire la prelucrarea datelor lor, conform art. 12–14 GDPR.

(2) Informarea se realizează prin note de informare, afișe la sediile U.B.C.A.R., formulare tipizate și prin publicarea pe site-ul oficial.

(3) Nota de informare include cel puțin: identitatea operatorului, scopurile și temeiurile prelucrării, destinatarii, perioada de stocare și drepturile persoanei vizate.

Art. 18 – Dreptul de acces

(1) Orice persoană vizată are dreptul de a obține confirmarea că datele sale sunt prelucrate de către U.B.C.A.R., precum și acces la acestea.

(2) La cerere, se furnizează gratuit o copie a datelor prelucrate; pentru copii suplimentare se poate percepe o taxă rezonabilă.

(3) Răspunsul la cererea de acces se transmite în termen de maximum 30 de zile calendaristice.

TITLUL II – Dreptul la corectare și ștergere

Art. 19 – Dreptul la rectificare

(1) Persoanele vizate pot solicita corectarea sau completarea datelor lor personale inexacte ori incomplete.

(2) Operatorul are obligația de a soluționa cererea în termen de 30 de zile și de a notifica persoana vizată cu privire la măsurile adoptate.

Art. 20 – Dreptul la ștergere („dreptul de a fi uitat”)

(1) Datele cu caracter personal se șterg la cererea persoanei vizate, în următoarele situații:

a) datele nu mai sunt necesare pentru scopurile colectării;

b) consimțământul a fost retras și nu există alt temei legal;

c) prelucrarea este ilegală;

d) datele trebuie șterse pentru respectarea unei obligații legale.

(2) Excepții: datele nu se șterg dacă sunt necesare pentru respectarea obligațiilor legale (fiscale, contabile, arhivistice), pentru constatarea sau apărarea unui drept în instanță ori pentru arhivare cu valoare religioasă sau istorică.

TITLUL III – Dreptul la restricționare și opoziție

Art. 21 – Dreptul la restricționarea prelucrării

(1) Persoanele vizate pot solicita restricționarea prelucrării în următoarele cazuri:

a) contestă exactitatea datelor, pe perioada verificării;

b) prelucrarea este ilegală, dar persoana nu dorește ștergerea;

c) operatorul nu mai are nevoie de date, dar persoana le solicită pentru apărarea unui drept;

d) persoana s-a opus prelucrării, pe perioada verificării interesului legitim.

(2) Datele restricționate se marchează distinct și nu pot fi prelucrate decât cu acordul persoanei vizate sau în scopuri legale.

Art. 22 – Dreptul la opoziție

(1) Persoanele vizate se pot opune, din motive legate de situația lor particulară, prelucrării datelor bazate pe interes legitim sau pe îndeplinirea unei sarcini de interes public.

(2) U.B.C.A.R. încetează prelucrarea, cu excepția cazului în care există motive legitime și imperioase care prevalează asupra drepturilor persoanei vizate.

TITLUL IV – Dreptul la portabilitate și căi de atac

Art. 23 – Dreptul la portabilitatea datelor

(1) Persoanele vizate pot solicita transferul datelor furnizate, într-un format structurat și utilizat curent, către un alt operator.

(2) Portabilitatea se aplică doar datelor prelucrate automat, pe baza consimțământului sau a unui contract.

Art. 24 – Dreptul de a formula plângeri

(1) Persoanele vizate pot depune plângere la Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP), dacă consideră că drepturile le-au fost încălcate.

(2) De asemenea, pot introduce acțiuni în instanță împotriva operatorului sau a împuterniciților.

(3) U.B.C.A.R. are obligația de a coopera deplin cu ANSPDCP și cu instanțele de judecată.

TITLUL V – Procedura de exercitare a drepturilor

Art. 25 – Modalitatea de exercitare a drepturilor

(1) Persoanele vizate își pot exercita drepturile prevăzute de prezentul Regulament prin cerere scrisă adresată U.B.C.A.R., transmisă la sediul central, la structurile teritoriale sau prin e-mail la adresa responsabilului cu protecția datelor (DPO).

(2) Operatorul are obligația de a răspunde cererii fără întârzieri nejustificate și, în orice caz, în termen de maximum 30 de zile calendaristice de la primirea acesteia.

(3) În cazuri complexe, termenul poate fi prelungit cu cel mult 30 de zile, cu informarea motivată a persoanei vizate.

Art. 26 – Notificarea terților și limitările legale

(1) În cazul în care datele cu caracter personal au fost dezvăluite către terți, operatorul are obligația de a-i informa despre orice rectificare, ștergere sau restricționare solicitată, cu excepția situației în care acest lucru se dovedește imposibil sau presupune eforturi disproporționate.

(2) Exercitarea drepturilor persoanelor vizate poate fi restricționată numai în măsura în care o astfel de restricționare este prevăzută de lege, în special pentru: securitatea națională, apărarea ordinii publice, prevenirea sau anchetarea infracțiunilor, respectarea obligațiilor fiscale sau de arhivare.

Art. 26¹ – Dreptul de a se opune marketingului direct

(1) Persoanele vizate au dreptul absolut de a se opune prelucrării datelor lor în scopuri de marketing direct, inclusiv profilării legate de acest scop.

(2) Orice material promoțional sau comunicare digitală se realizează numai pe baza consimțământului expres și documentat al persoanei vizate.

Art. 26² – Termenele de soluționare a cererilor

(1) Orice cerere a persoanei vizate este soluționată în termen de maximum 30 de zile.

(2) În cazuri justificate, termenul poate fi prelungit cu cel mult 30 de zile, cu notificarea prealabilă a persoanei vizate și prezentarea motivelor întârzierii.

CAPITOLUL IV – RESPONSABILITĂȚI ȘI ORGANIZARE INTERNĂ

TITLUL I – Roluri și responsabilități

Art. 27 – Operatorul (U.B.C.A.R.)

(1) U.B.C.A.R., în calitate de operator, asigură conformitatea cu GDPR și poate demonstra această conformitate (principiul responsabilității).

(2) Operatorul:

a) stabilește scopurile și mijloacele prelucrării;

b) adoptă politici interne, proceduri și registre (inclusiv ROPA/Registrul activităților de prelucrare – cf. Art. 16);

c) implementează **protecția datelor prin proiectare și în mod implicit** (*privacy by design & by default*), inclusiv minimizarea datelor și controlul accesului încă din faza de concepere a proceselor;

d) alocă resurse adecvate pentru protecția datelor (umane, financiare, tehnice);

e) desemnează și sprijină DPO, asigurând independența acestuia;

f) aprobă planul anual de conformitate GDPR și rapoartele de audit intern.

Art. 28 – Responsabilul cu protecția datelor (DPO)

(1) DPO este desemnat potrivit art. 37–39 GDPR și acționează independent, raportând direct către organul de conducere (C.E.N.).

(2) Atribuțiile DPO includ:

a) consilierea operatorului privind obligațiile GDPR;

b) monitorizarea conformității (politici, proceduri, training);

c) avizarea evaluărilor de impact (DPIA) și a testelor de interes legitim (LIA);

d) cooperarea cu ANSPDCP și rol de punct de contact;

e) consilierea privind incidentele/breșele și măsurile corective;

f) ținerea evidenței recomandărilor și măsurilor implementate.

(3) DPO nu primește instrucțiuni privind exercitarea atribuțiilor, nu este sancționat sau revocat pentru motive legate de acestea și nu se află în conflict de interese.

(4) Date de contact DPO: **ubcarromania@gmail.com**

Art. 29 – Conducerea executivă și structurile centrale

(1) BP/CNC asigură guvernanța și supravegherea conformității GDPR.

(2) Aprobă și revizuiește anual politicile și planul de conformitate; validează recomandările DPO; dispune măsuri corective.

(3) Numește un responsabil operațional GDPR (liaison) în fiecare departament central (ex.: Secretariat, Juridic & HR, Financiar-Contabil, IT).

Art. 30 – Structurile teritoriale și locale

(1) Fiecare filială/comunitate locală desemnează un **punct de contact GDPR** care colaborează cu DPO.

(2) Obligații:

a) aplică politicile;

b) menține registrele locale (prelucrări, acces, instruiri, incidente);

c) notifică DPO **în max. 24 ore** despre incidente și cereri ale persoanelor vizate;

d) asigură afișajul informativ și colectarea consimțămintelor acolo unde este necesar.

TITLUL II – Împuterniciți și aranjamente de prelucrare

Art. 31 – Selectarea și evaluarea împuterniciților

(1) Împuterniciții (furnizori IT, hosting/cloud, contabilitate, arhivare, HR, SSM/Medicina muncii etc.) sunt selectați în baza unor garanții suficiente privind măsurile tehnice și organizatorice.

(2) Se realizează **due diligence** înainte de contractare (politici de securitate, certificări, localizarea datelor, sub-procesatori).

Art. 32 – Contracte cu împuterniciții (art. 28 GDPR)
(1) Contractele includ cel puțin: obiectul, durata, natura și scopul prelucrării, tipurile de date, categoriile de persoane vizate, obligațiile și drepturile operatorului.
(2) Clauze minime: confidențialitate, instruirea personalului, asistența pentru drepturile persoanelor vizate, ștergerea/returnarea datelor la încetare, audit și inspecție, sub-procesare doar cu autorizarea operatorului, notificarea promptă a incidentelor.
(3) Operatorul își rezervă dreptul de **audit** al împuternicitului (direct sau prin terț independent).

Art. 33 – Operatorii asociați (art. 26 GDPR)
(1) Dacă U.B.C.A.R. stabilește împreună cu altă entitate scopurile și mijloacele prelucrării, părțile încheie un **acord de operatori asociați**.
(2) Acordul definește rolurile, punctul unic de contact și modul de exercitare a drepturilor persoanelor vizate; o sinteză se pune la dispoziția persoanelor vizate.

TITLUL III – Personal, voluntari și confidențialitate

Art. 34 – Confidențialitate și instruire
(1) Toate persoanele care prelucrează date semnează **angajamente de confidențialitate** înainte de a avea acces la date.
(2) U.B.C.A.R. asigură **instruire inițială** și **formare periodică** (cel puțin anual) privind protecția datelor, adaptată rolurilor.
(3) Evidențele trainingurilor se păstrează în registrul de conformitate.

Art. 35 – Acces pe roluri și ciclul de viață al accesului (JML)
(1) Accesul la date se acordă conform principiului **necesității de a cunoaște** (need-to-know) și minimizării.
(2) Se aplică proceduri **Joiners–Movers–Leavers**: acordare, modificare și revocare a accesului la angajare/mutare/încetare, cu documentare.
(3) Accesul este revizuit cel puțin anual.

Art. 36 – Măsuri disciplinare și raportare
(1) Încălcarea regulilor GDPR/ale prezentului Regulament atrage măsuri disciplinare conform ROF și legislației muncii/civile, fără a exclude răspunderea contravențională/penală.
(2) Orice persoană poate sesiza confidențial DPO cu privire la încălcări; se protejează avertizorii de integritate, potrivit legii.

TITLUL IV – Gestionarea temeiurilor: consimțământ, interes legitim, DPIA

Art. 37 – Consimțământ: colectare, dovadă, retragere
(1) Consimțământul este liber, specific, informat și lipsit de ambiguitate; nu se condiționează prestarea unui serviciu de consimțământ la prelucrări nenecesare.
(2) Se colectează separat de alți termeni/condiții, pe **formulare dedicate**, și se **evidențiază** în registrul consimțămintelor.
(3) Retragerea consimțământului este la fel de simplă ca acordarea și produce efecte pentru viitor; canalele de retragere sunt publicate (inclusiv e-mail DPO).

Art. 38 – Interes legitim și testul de balanță (LIA)
(1) Când temeiul este interesul legitim, se realizează **testul de balanță** documentat (scop legitim, necesitate, echilibrare drepturi).
(2) LIA este revizuit anual sau la schimbarea scopului.

Art. 39 – Evaluarea impactului (DPIA)
(1) Se efectuează DPIA atunci când un tip de prelucrare, în special prin utilizarea noilor tehnologii, este susceptibil să genereze un risc ridicat pentru drepturile și libertățile persoanelor (ex.: supraveghere video pe arii extinse, prelucrări de date sensibile la scară largă).
(2) DPO avizează DPIA; dacă riscul rezidual rămâne ridicat, se consultă ANSPDCP înainte de prelucrare (art. 36 GDPR).

TITLUL V – Registrul cererilor persoanelor vizate și gestionarea reclamațiilor

Art. 40 – Registrul cererilor (DSAR)
(1) A.R.– U.B.CA.R. menține un registru al cererilor persoanelor vizate (informare, acces, rectificare, ștergere, restricționare, opoziție, portabilitate), cu dată, canal, identitate verificată, acțiuni și termenul-limită.
(2) Identitatea solicitantului este verificată rezonabil înainte de soluționare; cererile vădit nefondate sau excesive pot fi refuzate sau taxate rezonabil, motivat, conform art. 12 alin. (5) GDPR.

Art. 41 – Gestionarea reclamațiilor
(1) Reclamațiile interne privind protecția datelor se înregistrează și se investighează prompt; DPO emite recomandări, iar conducerea dispune măsuri.
(2) Persoanele vizate sunt informate cu privire la dreptul de a se adresa ANSPDCP sau instanței (cf. Art. 24).

Art. 41¹ – Raportarea anuală a DPO
(1) DPO transmite anual un raport detaliat către conducerea centrală, cu privire la nivelul de conformitate, incidente și recomandări.
(2) Un rezumat al raportului este publicat pe site-ul oficial al U.B.C.A.R., în scop de transparență.

Art. 41² – Protecția avertizorilor
(1) Orice persoană care raportează încălcări GDPR este protejată împotriva represaliilor.
(2) Identitatea avertizorului este confidențială și nu poate fi divulgată decât dacă este impus prin lege.

TITLUL VI – Audit, control și actualizare

Art. 42 – Audit intern și verificări
(1) Se efectuează audituri interne de conformitate GDPR cel puțin anual, cu raport scris către conducere și recomandări de măsuri corective.
(2) Conducerea dispune implementarea măsurilor corective și monitorizează progresul.

Art. 43 – Raportarea incidentelor interne
(1) Orice persoană care observă un incident de securitate sau o potențială încălcare a protecției datelor are obligația de a raporta imediat punctului GDPR local sau DPO.
(2) Neraportarea incidentelor constituie abatere disciplinară.

Art. 44 – Transferuri interne între structuri
(1) Orice transfer de date între nivelul central și filialele teritoriale se realizează prin canale securizate (criptare, parole, plicuri sigilate).
(2) Responsabilitatea asigurării securității transferului revine structurii care transmite datele.

Art. 45 – Evidențe și probe de conformitate
(1) Toate activitățile GDPR (registre, consimțăminte, traininguri, audituri, DPIA, LIA) se documentează și se păstrează ca evidențe de conformitate.
(2) Evidențele se pun la dispoziția ANSPDCP la cerere.

Art. 46 – Actualizarea Regulamentului

(1) Prezentul Regulament se revizuiește cel puțin o dată la 2 ani sau ori de câte ori intervin modificări legislative ori tehnologice relevante.

(2) Propunerile de actualizare se fac de către DPO și se aprobă de conducerea centrală (BP/CNC).

CAPITOLUL V – MĂSURI TEHNICE ȘI ORGANIZATORICE DE SECURITATE

TITLUL I – Principii și responsabilități generale

Art. 47 – Principiul securității datelor

(1) U.B.C.A.R. asigură un nivel de securitate corespunzător riscurilor, conform art. 32 GDPR, prin măsuri tehnice și organizatorice adecvate.

(2) Nivelul de securitate se stabilește ținând cont de:

a) natura, volumul și categoriile de date prelucrate;

b) riscurile de acces neautorizat, distrugere, pierdere sau divulgare;

c) costurile implementării și tehnologia disponibilă;

d) impactul potențial asupra drepturilor și libertăților persoanelor vizate.

Art. 48 – Responsabilități de implementare

(1) Conducerea centrală (C.E.N./C.N.C.) adoptă politica de securitate și alocă resursele necesare.

(2) DPO monitorizează respectarea politicilor și emite recomandări.

(3) Responsabilii locali (filiale, comunități) aplică măsurile stabilite și raportează incidentele.

TITLUL II – Măsuri tehnice de securitate

Art. 49 – Controlul accesului

(1) Accesul la date se face pe bază de rol și autorizare, conform principiului necesității de a cunoaște.

(2) Se aplică autentificare pe două niveluri pentru accesul la sisteme informatice centrale.

(3) Parolele respectă standardele minime (min. 12 caractere, complexitate, rotație periodică).

Art. 50 – Protecția rețelelor și a echipamentelor

(1) Rețelele informatice sunt protejate prin firewall, antivirus actualizat și sisteme de detecție a intruziunilor.

(2) Laptopurile, telefoanele și dispozitivele mobile sunt securizate prin criptare și parole de acces.

(3) Echipamentele scoase din uz sunt distruse sau șterse securizat (wiping).

Art. 51 – Criptare și pseudonimizare

(1) Datele sensibile se stochează și transmit în formă criptată.

(2) Ori de câte ori este posibil, datele se pseudonimizează sau anonimizează pentru reducerea riscului.

Art. 52 – Copii de siguranță și continuitatea activității

(1) Backup-urile datelor se realizează cel puțin săptămânal și se stochează securizat.

(2) Se menține un plan de continuitate a activității și recuperare în caz de dezastru (BCP/DRP).

TITLUL III – Măsuri organizatorice și procedurale

Art. 53 – Politici și proceduri interne

(1) Se adoptă politici scrise privind accesul la date, gestionarea incidentelor, utilizarea echipamentelor și distrugerea documentelor.

(2) Angajații și voluntarii sunt informați și instruiți periodic cu privire la procedurile de securitate.

Art. 54 – Securitatea documentelor fizice

(1) Documentele pe suport hârtie se păstrează în spații cu acces restricționat, dulapuri încuiate și camere cu monitorizare.

(2) Documentele care nu mai sunt necesare se distrug prin tocătoare industriale sau prin servicii autorizate de distrugere.

Art. 55 – Gestionarea furnizorilor și a contractelor

(1) Toți furnizorii și colaboratorii care au acces la date semnează clauze contractuale de confidențialitate și securitate.

(2) Furnizorii sunt auditați periodic pentru verificarea respectării standardelor.

TITLUL IV – Securitatea comunicațiilor și a transferurilor

Art. 56 – E-mail și platforme digitale

(1) Comunicările prin e-mail care conțin date personale se fac prin canale securizate (criptare, acces pe bază de parolă).

(2) Utilizarea rețelelor sociale și a platformelor online respectă politica internă de securitate și nu implică publicarea de date fără consimțământ.

Art. 57 – Transferuri interne și internaționale

(1) Transferurile interne (central – filiale) se fac numai prin canale securizate (criptare, VPN, plicuri sigilate).

(2) Transferurile către state terțe respectă art. 44–49 GDPR, numai cu garanții adecvate (clauze standard, BCR, certificări).

TITLUL V – Monitorizare, testare și răspundere

Art. 58 – Monitorizarea securității

(1) Sistemele IT sunt monitorizate permanent pentru detectarea accesului neautorizat.

(2) Se păstrează log-uri de acces și activitate pentru minimum 6 luni.

Art. 59 – Testare și audit tehnic

(1) Se efectuează teste periodice de penetrare și vulnerabilitate, cel puțin o dată pe an.

(2) Rezultatele sunt analizate și integrate în planul de securitate.

Art. 60 – Răspunderea pentru securitate

(1) Fiecare angajat, voluntar sau colaborator are obligația de a respecta măsurile de securitate și confidențialitate.

(2) Încălcarea obligațiilor atrage sancțiuni disciplinare, civile sau penale, după caz.

Art. 60¹ – Testarea planurilor de continuitate

(1) Planurile de continuitate a activității și de recuperare în caz de dezastru sunt testate cel puțin o dată pe an.

(2) Rezultatele testării se documentează și se folosesc pentru îmbunătățirea procedurilor.

Art. 60² – Interdicția rețelelor nesecurizate

(1) Este interzis accesul la date cu caracter personal prin rețele Wi-Fi publice sau nesecurizate.

(2) În cazuri excepționale, se utilizează conexiuni VPN și criptare integrală.

TITLUL VI – Politici suplimentare de securitate și control

Art. 61 – Gestionarea dispozitivelor mobile și a muncii la distanță

(1) Utilizarea dispozitivelor mobile (laptopuri, telefoane, tablete) în scop profesional este permisă numai cu respectarea politicii interne BYOD și cu autorizarea expresă a operatorului.

(2) Accesul de la distanță (remote work/telemuncă) se face exclusiv prin conexiuni securizate (VPN, criptare end-to-end).

(3) Datele organizaționale trebuie stocate în medii separate de cele personale, cu parole distincte și soluții de securitate active.

Art. 62 – Clasificarea și etichetarea datelor

(1) A.R.– U.B.CA.R. instituie un sistem intern de clasificare a datelor:

a) publice;

b) interne;
c) confidențiale;
d) sensibile (inclusiv date speciale conform art. 9 GDPR).

(2) Fiecare categorie beneficiază de niveluri de protecție și acces corespunzătoare.
(3) Documentele confidențiale și sensibile se marchează vizibil și se transmit numai prin canale securizate.

Art. 63 – Securitatea fizică a infrastructurii
(1) Accesul la spațiile unde sunt localizate serverele, arhivele sau echipamentele de rețea se face doar cu autorizare specială.
(2) Se menține un registru al accesului fizic, verificat periodic de către responsabilul desemnat.
(3) Zonele critice sunt supravegheate video, cu respectarea legislației privind monitorizarea.

Art. 64 – Logarea și verificarea trasabilității
(1) Toate accesările bazelor de date și ale sistemelor informatice sunt logate automat.
(2) Log-urile sunt verificate de DPO sau responsabilul IT cel puțin o dată pe trimestru.
(3) Durata de păstrare a log-urilor este de minimum 12 luni, după care acestea se arhivează sau se distrug securizat.

Art. 65 – Politica de actualizare și suporturi externe
(1) Toate sistemele informatice sunt menținute actualizate (patch management), cu instalarea periodică a update-urilor de securitate.
(2) Utilizarea suporturilor externe (USB, HDD, DVD) se face exclusiv cu criptare și cu aprobare scrisă a responsabilului IT.
(3) Suporturile care nu mai sunt utilizate se distrug sau se șterg definitiv prin proceduri certificate.

CAPITOLUL VI – GESTIONAREA INCIDENTELOR ȘI NOTIFICAREA ÎNCĂLCĂRILOR DE DATE

TITLUL I – Definiții și clasificări

Art. 66 – Definiția incidentului de securitate

(1) Incident de securitate înseamnă orice situație care duce la distrugerea, pierderea, alterarea, divulgarea neautorizată sau accesul neautorizat la datele cu caracter personal, indiferent dacă este intenționată sau accidentală.
(2) Exemple: acces neautorizat, pierdere de documente, atac cibernetic, furt de echipamente, erori umane, transmiterea greșită de date.

Art. 67 – Clasificarea incidentelor

(1) Incidentele se clasifică în funcție de gravitate:
- *a)* minore – fără impact asupra drepturilor persoanelor vizate (ex.: erori corectate imediat);
- *b)* medii – pot afecta un număr limitat de persoane și necesită măsuri corective;
- *c)* majore – afectează un număr semnificativ de persoane sau implică date sensibile;
- *d)* critice – pot genera prejudicii grave pentru persoanele vizate și necesită notificare către ANSPDCP.

TITLUL II – Procedura internă de raportare și reacție

Art. 68 – Obligația de raportare

(1) Orice angajat, voluntar sau colaborator care constată un incident are obligația de a-l raporta imediat către DPO sau către responsabilul desemnat local.
(2) Raportarea se face în maximum 24 de ore de la constatare, pe formular tipizat sau prin canalele de raportare stabilite.

Art. 69 – Evaluarea incidentului

(1) DPO evaluează incidentul în termen de maximum 48 de ore, determinând natura, amploarea și impactul acestuia.
(2) Se documentează: descrierea incidentului, categoriile și numărul estimat de persoane afectate, categoriile și volumul datelor compromise, cauzele și riscurile asociate.

Art. 70 – Măsuri imediate

(1) Operatorul adoptă măsuri imediate pentru:
- *a)* limitarea accesului neautorizat;
- *b)* recuperarea datelor compromise;
- *c)* prevenirea escaladării incidentului.

(2) Toate măsurile se consemnează în registrul incidentelor.

TITLUL III – Notificarea Autorității și informarea persoanelor vizate

Art. 71 – Notificarea ANSPDCP

(1) În cazul unei încălcări de securitate care prezintă risc pentru drepturile și libertățile persoanelor, operatorul notifică ANSPDCP în termen de 72 de ore de la constatare (art. 33 GDPR).
(2) Notificarea include cel puțin:
- *a)* natura și descrierea incidentului;
- *b)* categoriile și numărul estimat de persoane vizate;
- *c)* categoriile și numărul estimat de înregistrări afectate;
- *d)* numele și datele de contact ale DPO;
- *e)* consecințele probabile;
- *f)* măsurile luate sau propuse.

(3) Dacă notificarea nu se face în termen, trebuie justificată întârzierea.

Art. 72 – Informarea persoanelor vizate
(1) Dacă încălcarea este susceptibilă să genereze un risc ridicat pentru drepturile și libertățile persoanelor vizate, acestea sunt informate fără întârzieri nejustificate.
(2) Informarea se face într-un limbaj clar și simplu, cuprinzând: natura incidentului, consecințele, măsurile de remediere și drepturile de care dispun.
(3) Informarea nu este necesară dacă:
a) datele au fost protejate prin măsuri tehnice (ex.: criptare);
b) au fost luate măsuri ulterioare care elimină riscul;
c) ar presupune un efort disproporționat – caz în care se recurge la o informare publică.

TITLUL IV – Evidențe, audit și îmbunătățire

Art. 73 – Registrul incidentelor
(1) Toate incidentele de securitate, indiferent de gravitate, se înregistrează într-un registru special gestionat de DPO.
(2) Registrul include: data incidentului, descrierea, persoana care a raportat, evaluarea impactului, măsurile adoptate și concluziile.

Art. 74 – Audit și lecții învățate
(1) Incidentele majore și critice sunt supuse unui audit intern pentru a identifica cauzele și măsurile preventive.
(2) Concluziile sunt integrate în planul anual de conformitate GDPR și în instruirile personalului.

Art. 75 – Răspundere și sancțiuni interne
(1) Neraportarea sau raportarea tardivă a incidentelor atrage sancțiuni disciplinare.
(2) Persoanele care încalcă obligațiile de securitate și confidențialitate răspund disciplinar, civil sau penal, după caz.

Art. 75¹ – Raport anual al incidentelor
(1) DPO întocmește anual un raport consolidat privind incidentele, tendințele identificate și măsurile corective.
(2) Raportul este prezentat conducerii centrale și integrat în planul de conformitate GDPR.

TITLUL V – Dispoziții suplimentare privind gestionarea incidentelor

Art. 76 – Documentarea incidentelor ne-notificate
(1) Toate incidentele de securitate, inclusiv cele care nu fac obiectul notificării către ANSPDCP, se documentează în registrul incidentelor.
(2) Documentația cuprinde evaluarea motivată a operatorului privind inexistența unui risc pentru drepturile și libertățile persoanelor vizate.
(3) Această documentație se păstrează minimum 5 ani și se pune la dispoziția ANSPDCP la cerere.

Art. 77 – Canale de alertă internă
(1) U.B.C.A.R. instituie un mecanism rapid de alertă internă (adresă de e-mail securizată, telefon dedicat, platformă digitală) pentru raportarea incidentelor.
(2) Datele de contact pentru raportare sunt comunicate tuturor angajaților, voluntarilor și colaboratorilor.
(3) Raportarea se poate face și anonim, iar operatorul garantează protecția avertizorilor de integritate.

Art. 78 – Rolul DPO în notificare
(1) DPO este responsabil pentru centralizarea, evaluarea și întocmirea notificării către ANSPDCP, cu aprobarea operatorului.

(2) DPO asigură menținerea corespondenței oficiale cu Autoritatea și arhivează toate notificările și răspunsurile.

Art. 79 – Obligațiile împuterniciților în caz de incident

(1) Împuterniciții au obligația contractuală de a informa imediat operatorul despre orice incident care afectează datele prelucrate în numele U.B.C.A.R., în maximum 24 de ore de la constatare.

(2) Neîndeplinirea acestei obligații constituie încălcare contractuală gravă și poate atrage sancțiuni sau rezilierea contractului.

(3) Operatorul verifică periodic procedurile împuterniciților prin audituri sau rapoarte de conformitate.

Art. 80 – Simulări și testări periodice

(1) U.B.C.A.R. organizează cel puțin anual simulări de răspuns la incidente („table-top exercises”) pentru testarea eficienței procedurilor.

(2) Rezultatele simulărilor se documentează și se folosesc pentru îmbunătățirea planului de gestionare a incidentelor.

(3) Simulările pot include scenarii de atac cibernetic, pierdere de documente, scurgeri accidentale de date sau incidente la nivelul împuterniciților.

CAPITOLUL VII – AUDIT, CONFORMITATE ȘI INSTRUIRE PERIODICĂ

TITLUL I – Audit intern și evaluări periodice

Art. 81 – Auditul GDPR intern

(1) U.B.C.A.R. efectuează audituri interne privind respectarea prezentului Regulament și a legislației GDPR cel puțin o dată pe an.
(2) Auditul include verificarea: registrelor de prelucrare, consimțămintelor, incidentelor, contractelor cu împuterniciți, instruirilor și nivelului de securitate tehnică.
(3) Rezultatele auditului se consemnează într-un raport scris, păstrat minimum 5 ani.

Art. 82 – Evaluări tematice și inopinate

(1) DPO poate dispune audituri tematice asupra unor departamente sau structuri teritoriale (ex.: HR, contabilitate, IT, filiale).
(2) Conducerea centrală, prin C.E.N., poate decide efectuarea de audituri inopinate, atunci când există suspiciuni de neconformitate sau în urma unor incidente.

TITLUL II – Conformitate continuă

Art. 83 – Revizuirea periodică a politicilor

(1) Politicile și procedurile GDPR se revizuiesc cel puțin anual sau ori de câte ori apar modificări legislative ori tehnologice.
(2) Revizuirea este coordonată de DPO și aprobată de conducerea centrală.

Art. 84 – Planul anual de conformitate

(1) DPO întocmește un plan anual de conformitate GDPR, care include:
a) obiective, riscuri prioritare și măsuri planificate;
b) calendarul instruirilor;
c) simulările de incidente și testările tehnice;
d) acțiunile de audit intern.
(2) Planul se aprobă de către BP/CNC și se publică într-un rezumat accesibil pentru structurile teritoriale.

TITLUL III – Instruire și conștientizare

Art. 85 – Instruire inițială și periodică

(1) Toți angajații, voluntarii și colaboratorii care au acces la date cu caracter personal participă la instruire inițială privind protecția datelor, înainte de începerea activității.
(2) Instruirile periodice se desfășoară cel puțin o dată pe an și includ studii de caz, incidente anterioare și bune practici.
(3) Evidența instruirilor se păstrează în registrul de conformitate.

Art. 86 – Conștientizare și informare continuă

(1) Operatorul utilizează afișe, ghiduri interne, newslettere electronice sau sesiuni de Q&A pentru a menține gradul de conștientizare al personalului.
(2) DPO publică periodic recomandări și răspunsuri la întrebările frecvente (FAQ).

TITLUL IV – Raportare și responsabilitate

Art. 87 – Raportarea către conducere

(1) DPO prezintă C.E.N.-ului un raport anual privind:
a) incidentele gestionate și măsurile corective;
b) nivelul de implementare a planului anual de conformitate;
c) rezultatele auditurilor interne și recomandările.
(2) Raportul este discutat în ședință și integrat în planul strategic al organizației.

Art. 88 – Îmbunătățire continuă
(1) Pe baza rapoartelor, conducerea adoptă măsuri de îmbunătățire a politicilor, securității și instruirii.
(2) U.B.C.A.R. urmărește să mențină un standard ridicat de conformitate și să prevină aplicarea sancțiunilor printr-o abordare proactivă.

Art. 88¹ – Audit extern obligatoriu
(1) U.B.C.A.R. supune sistemul de protecție a datelor unui audit extern independent cel puțin o dată la 3 ani.
(2) Raportul extern este analizat de conducere și măsurile recomandate devin obligatorii.

Art. 88² – Exerciții practice de conformitate
(1) Se organizează cel puțin o dată pe an simulări practice privind gestionarea cererilor persoanelor vizate și a incidentelor de securitate.
(2) Rezultatele sunt evaluate de DPO și integrate în instruirile viitoare.

Art. 89 – Accesibilitatea rezultatelor auditurilor
(1) Concluziile auditurilor GDPR și ale rapoartelor de conformitate sunt comunicate într-o sinteză accesibilă structurilor teritoriale și departamentelor vizate.
(2) Sinteza este distribuită prin canale interne oficiale (e-mail, intranet, circulare) pentru a asigura transparența și aplicarea uniformă.

Art. 90 – Responsabilitatea implementării recomandărilor
(1) Fiecare departament sau filială este responsabil de aplicarea recomandărilor care îl privesc, în termenul stabilit de conducerea centrală.
(2) DPO monitorizează stadiul implementării și raportează trimestrial conducerii eventualele întârzieri.

Art. 91 – Verificarea nivelului de cunoștințe
(1) La finalul instruirilor periodice, participanții susțin teste de evaluare sau completează chestionare pentru a verifica nivelul de înțelegere.
(2) Rezultatele testării se consemnează în registrul instruirilor și sunt analizate pentru identificarea nevoilor suplimentare de formare.

Art. 92 – Lecții învățate și prevenirea recurenței
(1) Rapoartele de audit și de instruire includ o secțiune dedicată incidentelor anterioare și măsurilor luate pentru prevenirea repetării acestora.
(2) DPO are obligația să integreze aceste lecții în planul anual de conformitate și în materialele de instruire.

Art. 93 – Audit extern și cultură organizațională
(1) O dată la 2–3 ani, U.B.C.A.R. poate solicita realizarea unui audit extern independent privind conformitatea GDPR, pentru obiectivitate și bune practici.
(2) Conducerea centrală are obligația de a susține public cultura de conformitate GDPR, prin exemplu personal și prin includerea obiectivelor de protecție a datelor în strategia organizațională.

CAPITOLUL VIII – DISPOZIȚII FINALE ȘI SANCȚIUNI INTERNE

TITLUL I – Dispoziții generale

Art. 94 – Intrarea în vigoare

(1) Prezentul Regulament intră în vigoare la data aprobării de către conducerea centrală și devine obligatoriu pentru toate structurile U.B.C.A.R.

(2) Regulamentul este comunicat prin canale oficiale și publicat pe site-ul organizației.

Art. 95 – Revizuirea și actualizarea

(1) Regulamentul se revizuiește cel puțin o dată la doi ani sau ori de câte ori apar modificări legislative sau tehnologice relevante.

(2) Revizuirea este coordonată de DPO și aprobată de conducerea centrală.

TITLUL II – Forță juridică și corelări

Art. 96 – Raportul cu alte acte interne

(1) Regulamentul completează Statutul și ROF și prevalează în materie de protecție a datelor cu caracter personal.

(2) În caz de conflict între prezentul Regulament și alte reglementări interne, dispozițiile GDPR și legislația națională aplicabilă au caracter prioritar.

Art. 97 – Obligația de conformare

(1) Toți membrii, angajații, voluntarii și colaboratorii sunt obligați să respecte prezentul Regulament.

(2) Nerespectarea acestuia atrage sancțiuni interne și, după caz, răspundere civilă, contravențională sau penală.

TITLUL III – Sancțiuni interne

Art. 98 – Regimul sancțiunilor

(1) Încălcarea prevederilor Regulamentului atrage aplicarea sancțiunilor interne, proporțional cu gravitatea faptei.

(2) Sancțiunile pot fi:

a) avertisment scris;
b) retragerea temporară a accesului la date;
c) diminuarea atribuțiilor privind prelucrarea datelor;
d) încetarea raportului de muncă sau a colaborării;
e) sesizarea autorităților competente (ANSPDCP, organe judiciare).

Art. 99 – Criterii de individualizare a sancțiunii

La stabilirea sancțiunii se ține cont de:

a) natura și gravitatea încălcării;
b) durata încălcării și consecințele produse;
c) intenția sau culpa persoanei;
d) măsurile luate de persoană pentru a limita prejudiciile.

TITLUL IV – Dispoziții tranzitorii și finale

Art. 100 – Informarea și instruirea
(1) Prezentul Regulament se aduce la cunoștința tuturor persoanelor vizate prin instruiri și materiale de informare.
(2) Semnătura de luare la cunoștință face parte din dosarul de personal sau din contractele de colaborare.

Art. 101 – Dispoziții tranzitorii
(1) Procedurile și registrele existente se aliniază prevederilor prezentului Regulament în termen de 60 de zile de la intrarea sa în vigoare.
(2) Până la finalizarea alinierii, se aplică măsurile provizorii stabilite de conducerea centrală, sub supravegherea DPO.

Art. 102 – Clauză de conformitate
Prezentul Regulament este elaborat în conformitate cu Regulamentul (UE) 2016/679 (GDPR), Legea nr. 190/2018 și legislația națională relevantă și se aplică în mod obligatoriu tuturor structurilor și activităților U.B.C.A.R.

Art. 102[1] – Supraviețuirea obligațiilor de confidențialitate
(1) Obligațiile de confidențialitate și securitate persistă și după încetarea contractului de muncă, a mandatului sau a colaborării.

Art. 102[2] – Arhivare și distrugere finală
(1) Datele cu caracter personal sunt arhivate și ulterior distruse conform termenelor legale și procedurilor interne.
(2) Distrugerea este documentată și certificată de responsabilul desemnat.

Art. 102[3] – Informarea autorităților.
În cazul în care sancțiunile interne indică o problemă sistemică de conformitate, DPO informează conducerea despre necesitatea notificării ANSPDCP.

Art. 103 – Evidențe și dovada conformității
(1) Toate activitățile și măsurile privind aplicarea prezentului Regulament se documentează și se păstrează în registre speciale (registre de prelucrare, instruiri, incidente, sancțiuni).
(2) Aceste evidențe sunt puse la dispoziția ANSPDCP la solicitare.

Art. 104 – Nulitatea parțială Dacă una dintre dispozițiile prezentului Regulament devine nulă sau inaplicabilă, celelalte dispoziții rămân valabile și produc efecte.

Art. 106 – Cooperarea cu autoritățile
(1) U.B.C.A.R. cooperează în mod activ cu ANSPDCP și pune la dispoziția acesteia documentele și informațiile solicitate.
(2) Litigiile privind protecția datelor se soluționează de către instanțele competente din România, conform legislației aplicabile.

Art. 107 – Răspunderea personală. Persoanele care, prin acțiuni sau omisiuni intenționate, cauzează încălcarea prezentului Regulament și prejudicii U.B.C.A.R. sau persoanelor vizate, răspund personal și pot fi obligate la repararea prejudiciului.