Nr. procedură:
C.A.R.S. Bucovina IFN

PROCEDURĂ DE LUCRU PRIVIND UTILIZAREA DATELOR CU CARACTER PERSONAL, SECURIZAREA, ATÂT LA NIVEL INFORMATIC, CÂT ŞI PE SUPORT SCRIS

Aprobată de Consiliul Director al C.A.R.S. Bucovina IFN la data de 24.05.2018.
Aplicabilă de la data de 25.05.2018.

Adusă la cunoştinţa:

a) membrilor prin informarea afișată la sediul C.A.R. și pe site-ul www.carbucovina.ro și care cuprinde mențiunile legale informării acestora;
b) Consiliului director, cenzorilor;
c) salariaților C.A.R. (tuturor), incluzând și pe cei din agențiile de lucru;
d) colaboratorilor (după caz);
e) deținătorilor de programe informatice utilizate de C.A.R.

Definiţii utile:

1. Date cu caracter personal – înseamnă orice informații privind o persoană fizică identificată sau identificabilă (persoană vizată) o persoană identificabilă este o persoană care poate fi identificată, direct sau indirect, în special prin referire la un element de idetificare (cum ar fi: nume, un număr de identificare, date de localizare, un identificator on-line sau la unul sau mai multe elemente specifice, proprii identității sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale).

2. Prelucrare date cu caracter personal – prin prelucrarea datelor cu caracter personal este definită orice operațiune sau set de operațiuni care se efectuează asupra datelor cu caracter personal, prin mijloace automate sau neautomate, cum ar fi colectarea, registrarea, organizarea, stocarea, adaptarea ori modificarea, extragerea, consultarea, utilizarea, dezvăluirea către terți prin transmitere, diseminare sau orice alt mod, alăturarea ori combinarea, blocarea, ștergerea sau distrugerea.

3. Sistem de evidență a datelor – înseamnă orice set structurat de date cu caracter personal accesibile conforme unor criterii specifice, fie ele centralizate, descentralizate sau repartizate după criterii funcționale sau geografice.

4. Operator – încazul nostru este C.A.R. – înseamnă persoană fizică sau juridică, autoritate publică, agenție sau alt organism care, singur sau împreună cu altele, stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal.

5. Parte terță – înseamnă o persoană fizică sau juridică, autoritate publică, organism altul decât persoana vizată, operatorul, persoana împuternicită de operator și persoanele care sub directa autoritate a operatorului sau a persoanei împuternicite de operator, sunt autorizate să prelucreze date cu caracter personal.

6. Persoană împuternicită de operator – înseamnă persoana fizică sau juridică, autoritate publică, agenție sau un alt organism care prelucrează date cu caracter personal.

7. Consimțământ al persoanei vizate înseamnă orice manifestare de voință liberă, specifică, informată și lipsită de ambiguitate a persoanei vizate prin care aceasta acceptă, printr-o declarație sau pintr-o acțiune fără echivoc, ca datele cu caracter personal care o privesc să fie prelucrate.

8. Încălcarea securității datelor cu caracter personal – înseamnă o încălcare a securității care duce, în mod accidental sau ilegal, la distrugerea, pierderea, modificarea sau divulgarea neautorizată a datelor cu caracter personal transmise, stocate sau prelucrate într-un alt mod, sau la accesul neautorizat la acestea.

Legislația aplicabilă:

- Regulamentul General privind protecția datelor;
- Carta Drepturilor Fundamentale a Uniunii Europene;

- Legea nr.677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date;
- Ordinele Avocatului poporului nr.52/2002 și 75/2002;
- Codul Civil;
- Decizii ale Autorității Naționale pentru Protecția Datelor cu Caracter Personal.

1. Scopul.

Scopul acestei Proceduri este de a garanta și proteja drepturile și libertățile fundamentale ale membrilor, potențialilor membri, giranților, debitorilor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date, administrarea în condiții de siguranță, îndeplinirea obligațiilor referitoare la securitatea și controlul sistemelor informatice, în vederea asigurării acurateții datelor și informațiilor, păstrării confidențialității și siguranței acestora pe parcursul desfășurării activității curente de către salariații și alte persoane împuternicite ale C.A.R.S. Bucovina IFN.

2. Reguli generale.

Art.1. Prezenta procedură stabilește măsuri tehnice și organizatorice pentru îndeplinirea obligațiilor referitoare la securitatea și controlul sistemelor informatice, în vederea asigurării confidențialității datelor și informațiilor precum și pentru păstrarea în siguranță a acestora, în cadrul activității curente executate de angajații C.A.R., incluzând și pe cei ai agențiilor de lucru, după caz.

Prin cerințe minime de securitate este avut în vedere un complex de măsuri tehnice, informatice, organizatorice, logistice prin care să se asigure nivelul minim de securitate prevăzut în dispozițiile Legii nr.677/2001, în conformitate cu cerințele minime de securitate a prelucrării datelor cu caracter personal aprobate prin Ordinele Avocatului poporului.

Art.2. C.A.R.S. Bucovina IFN a adoptat măsuri tehnice și organizatorice adecvate pentru protejarea datelor cu caracter personal împotriva distrugeri accidentale sau ilegale, pierderilor, modificărilor, dezvăluirilor sau accesul neautorizat. În acest sens C.A.R.S. Bucovina IFN a împuternicit persoana responsabilă cu respectarea dispozițiilor legale.

Art.3. C.A.R.S. Bucovina IFN a luat măsuri de stocare în siguranță a informațiilor, astfel încât să fie asigurat un nivel adecvat de protecție și securitate, în sensul Legii nr. 677/2001.

Art.4. Pentru îndeplinirea dispozițiilor legale aferente și în vederea satisfacerii cerințelor păstrării în siguranță a datelor și informațiilor, C.A.R. a implementat următoarele măsuri:
- identificarea și autentificarea utilizatorului;
- tipul de acces;
- colectarea datelor;
- execuția copiilor de siguranță;
- computerele și terminalele de acces;
- fișierele de acces;
- instruirea personalului.

3. Proceduri specifice.

Art.5. Identificarea și autentificarea utilizatorului. Prin utilizator se înțelege orice persoană care acționează sub autoritatea operatorului (C.A.R.) cu drept recunoscut de acces la bazele de date cu caracter personal. Fiecare utilizator va avea o parolă de acces unică (cod) niciodată nu este alocată aceeași parolă (cod) mai multor utilizatori. Parolele (codurile) de acces nefolosite o perioadă mai îndelungată sunt dezactivate şi distruse de C.A.R.

Orice utilizator care primeşte o parolă (cod) de identificare şi un mijloc de autentificare răspunde în faţa operatorului C.A.R., iar fişa postului persoanei respective este completată cu obligaţiile privind confidenţialitatea şi răspunderea.

Accesul utilizatorilor la bazelede date cu caracter personal efectuate manual se face numai pe baza unei liste aprobate de conducerea C.A.R.

Art.6. Tipul de acces. Utilizatorii, pentru îndeplinirea atribuțiunilor specifice, pot accesa numai datele cu caracter personal necesare.Programatorii sistemelor de prelucrare a datelor cu caracter personal nu trebuie să aibă acces la aceste date. Fiecare operator are grijă să limiteze accesul utilizatorilor numai privind realizarea atribuțiilor specifice.

Art.7. Colectarea datelor. Operatorul (C.A.R.) desemnează utilizatorii autorizați pentru operațiile de colectare și introducere de date cu caracter personal în sistemul informatic, de regulă, după înscrierea membrilor C.A.R. Orice modificarea datelor cu caracter personal se realizează numai de către utilizatorii desemnați.

Operatorul (C.A.R.) va solicita programatorului sistemului informațional ca acesta să înregistreze cine a făcut modificarea, data și ora modificării și să fie menținute datele șterse sau modificate.

Art.8. Execuția copiilor de siguranță. Operatorul (C.A.R.) stabilește intervalul de timp la care se vor executa copiile de siguranță ale bazelor de date cu caracter personal, precum și ale programelor folosite pentru prelucrările automatizate.Operatorul (C.A.R.) a luat măsuri ca utilizatorii care execută copii de siguranță să fie în număr redus, copiile să fie stocate în condiții de siguranță, iar accesul la copiile de siguranță să fie monitorizat.

Art.9. Securitatea datelor cu caracter personal. Operatorul C.A.R., având în vedere stadiul actual al dezvoltării, costurile implementării și natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și riscul cu diferite grade de probabilitate și gravitate pentru drepturile și libertățile persoanelor fizice operatorul C.A.R. implementează măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător acestui risc, incluzând printre altele, după caz:

- criptarea datelor cu caracter personal;
- capacitatea de a asigura confidențialitatea, integritatea, disponibilitatea și rezistența continuă ale sistemelor și serviciilor de prelucrare;
- capacitatea de a restabili disponibilitatea datelor cu caracter personal și accesul la acestea în timp util în cazul în care are loc un incident de natură fizică sau tehnică;
- un proces pentru testarea, evaluarea și aprecierea periodică a eficacității măsurilor tehnice și organizatorice pentru a garanta securitatea prelucrării.

Operatorul (C.A.R.) și persoana împuternicită de acesta iau măsuri pentru a asigura faptul că orice salariat sau altă persoană fizică care acționează sub autoritatea C.A.R. și are acces la date cu caracter personal nu le prelucrează decât la cererea C.A.R.

Art.10. Computerele și terminalele de acces. Computerele și alte terminale de acces sunt instalate în încăperi cu acces restricționat. Unde nu pot fi asigurate aceste condiții, încăperile unde se află computerele trebuie să poată fi încuiate. Dacă pe ecran apar date cucaracter personal asupra cărora nu se acționează o perioadă dată, stabilită de operator (C.A.R.), sesiunea de lucru se închide automat. Mărimea acestei perioade se determină în funcție de operațiile care trebuie executate.

Terminalele de acces folosite în relațiile cu membri C.A.R., alte persoane fizice, pe care apar date cu caracter personal, vor fi poziționate astfel încât să nu poată fi văzute de public și după o perioadă scurtă, stabilită de operator (C.A.R.) în care nu se acționează asupra lor acestea trebuie ascunse.

Serverele care găzduiesc baza de date pot fi accesate doar în mod controlat pe bază de drepturi de acces. Nu este permisă scoaterea din sediul operatorului a mediilor de stocare mobilă (CD/DVD, USB-Stick etc.) decât cu aprobarea prealabilă a conducerii C.A.R.

Art.11. Fișierele de acces. Operatorul (C.A.R.) împreună cu programatorul iau măsuri ca orice accesare a bazei de date cu caracter personal să fie înregistrată într-un fișier de acces (numit log la prelucrările automate sau într-un registru pentru prelucrările manuale de date cu caracter personal), stabilit de conducerea C.A.R.

Informațiile înregistrate în fișier sau în registru vor fi:

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

Pentru prelucrările automate informațiile vor fi stocate într-un fișier de acces general sau în fișiere separate pentru fiecare utilizator.

Fișierele de acces se păstrează cel puțin 2 ani, pentru a fi folosite ca probe în cazul unor investigații.

Art.12. Instruirea personalului.

Operatorul (C.A.R.) realizează informarea personalului cu privire la prevederile legale referitoare la protecția datelor cu caracter personal precum și la riscurile la care expun C.A.R. în situația nerespectării prevederilor legale.

Utilizatorii care au acces la datele cu caracter personal și care operează cu acestea sunt instruiți separat și le sunt prevăzute separat obligații privind confidențialitatea în fișa postului.

Art.13. Folosirea computerelor.

Pentru menținerea securității prelucrării datelor cu caracter personal (în special împotriva virușilor informatici) C.A.R. va lua măsuri astfel:

- interzicerea folosirii de către cei desemnați (utilizatori) a unor programe software care provin din surse externe sau dubioase;
- informarea utilizatorilor desemnați în privința pericolului privind virușii informatici;
- implementarea unor sisteme automate antivirus și de securitate a sistemelor informatice;
- interzicerea folosirii computerelor în scopuri personale altele decât cele specifice C.A.R.;
- dezactivarea, pe cât posibil, a tastei „Print Screen” atunci când sunt afișate pe monitor date cu caracter personal, interzicându-se astfel scoaterea la imprimantă a acestora;
- salvarea regulată a fișierelor importante.

Art.14. Imprimarea datelor.

Scoaterea la imprimantă a datelor cu caracter personal se va realiza numai de utilizatorii desemnați de C.A.R.

Art.15. Reguli speciale privind prelucrarea datelor cu caracter personal.

În scopul protejării datelor cu caracter personal se iau următoarele măsuri:

1. Prelucrări automate de date cu caracter personal. Accesul utilizatorilor desemnați la bazele de date cu caracter personal se va efectua prin parole de autentificare (coduri) individuale și care se vor dezactiva după un număr de 3 până la 5 încercări de logare nereușite.

Programatorii care dezvoltă aplicațiile care prelucrează datele cu caracter personal nu au acces la datele cu caracter personal. Accesul programatorilor este permis numai dacă datele au fost transformate în date anonime.

2. Prelucrări manuale de date cu caracter personal. Documentele care conțin date cu caracter personal sunt ținute în fișete sau dulapuri sub cheie sau cu un alt mecanism de securizare.

3. Folosirea poștei electronice și a internetului în relațiile de muncă. Pentru utilizarea corectă a rețelei de internet și serviciilor de e-mail se stabilește:

- sistemele informaționale și programele calculatorului trebuie să fie configurate prin reducerea la minimum a utilizării datelor cu caracter personal și de identificare în raport cu scopurile urmărite;
- prelucrarea datelor se face în scopuri determinate, explicite în strictă conformitate cu atribuțiile specificate în fișa postului și așa cum sunt prevăzute în reglementările legale;

- responsabilizarea salariaților care prelucrează date cu caracter personal prin implementarea unor instrucțiuni clare vor permite angajaților de a-și exercita corect obligațiile de serviciu.

Art.16. Prelucrarea datelor cu caracter personal în raportul C.A.R./membru.

a. C.A.R. colectează date cu caracter personal de la membri/potențiali membri, giranți, debitori în scopul realizării obiectului de activitate, respectiv de oferirea de servicii specifice C.A.R., în acest sens are afișată o *Notă de informare* la sediul său, de asemenea dată publicității în alte forme.

Drepturile membrilor:

♦ **dreptul de acces la date**: dreptul membrului de a obține de la C.A.R., la cerere și în mod gratuit pentru o solicitare pe an, confirmarea faptului că datele care îl privesc sunt sau nu prelucrate de C.A.R.;

♦ **dreptul de intervenție**: dreptul de a obține la cererea sa și în mod gratuit, după caz, rectificarea, actualizarea, blocarea, ștergerea datelor a căror prelucrare nu este conformă Legii nr.677/2001, în special a datelor incomplete, inexacte;

♦ **dreptul de opoziție**: membrul C.A.R. are dreptul de a se opune în orice moment, din motive întemeiate și legitime legate de situația sa particulară, ce date care îl vizează să facă obiectul unei prelucrări în scop de marketing direct în numele C.A.R., sau să fie dezvăluite unor terți în acest scop;

♦ **dreptul de a nu fi supus unei decizii individuale**: orice membru are dreptul de a cere și de a obține retragerea sau anularea unei decizii care produce efecte juridice în privința sa care îl afectează în mod semnificativ, adoptată exclusiv pe baza unei prelucrări de date cu caracter personal, efectuată prin mijloace automate destinată să evalueze unele aspecte ale personalității, precum credibilitatea sau alte aspecte;

♦ **dreptul de a se adresa justiției**: este dreptul fiecărui membru pentru apărarea oricăror drepturi garantate de Legea nr.677/2001 și care au fost încălcate. Instanța competentă este cea în a cărei rază teritorială domiciliează reclamantul, iar cererea este scutită de taxă de timbru.

Începând cu data intrării în vigoare a **Regulamentului U.E. nr. 2016/679 (Regulamentul General privind protecția datelor)**, respectiv 25 mai 2018, membri beneficiază si pot exercita suplimentar următoarele drepturi:

♦ **dreptul la ștergerea datelor („dreptul de a fi uitat”)**: dreptul membrului de a solicita ștergerea datelor cu caracter personal care îl privesc, fără întârzieri nejustificate, în oricare dintre următoarele situații: nu mai sunt necesare pentru îndeplinirea scopurilor pentru care au fost colectate; membrul și-a retras consimțământul și nu există alt temei juridic pentru prelucrare; membrul se opune prelucrării; datele au fost colectate ilegal; datele trebuie șterse pentru respectarea unei obligații legale, colectarea s-a făcut cu oferirea de servicii ale societății informaționale;

♦ **dreptul la portabilitatea datelor**, în sensul că membrul poate primi datele personale într-un format structurat, care poate fi citit automat și la dreptul că acestea pot fi transmise direct altui operator;

♦ **dreptul la restricționarea prelucrării**, care poate fi exercitat în următoarele cazuri: este contestată exactitatea datelor pe o perioadă care permite operatorului verificarea corectitudinii acestora; prelucrarea este ilegală, dar nu se dorește ștergerea datelor, ci doar restricționarea acestora; în cazul în care C.A.R.S. Bucovina IFN nu mai are nevoie de datele cu caracter personal în scopul prelucrării, dar membrul le solicită pentru apărarea unui drept în instanță; dacă membrul s-a opus prelucrării pentru intervalul de timp cât se verifică dacă drepturile legitime ale C.A.R.S. Bucovina IFN prevalează asupra drepturilor sale.

b. Dezvăluirea datelor cu caracter personal terților. Fiecare caz de solicitare a accesului la datele cu caracter personal ale membrilor indiferent de statutul solicitantului (autorități, alte instituții, persoane fizice etc.) trebuie analizat în detaliu de reprezentanții C.A.R. pentru identificarea:

- solicitarea are legătură cu scopurile pentru care au fost colectate datele cu caracter personal;
- volumului și categoriilor datelor cu caracter personal la care se solicită accesul
- condițiilor în care vor fi păstrate datele cu caracter personal și termenului pentru care sunt necesare aceste date;
- cadrului normativ care întemeiază cererea de acces al solicitantului la aceste date;

Art.17. Prevenirea pierderii datelor și capabilitatea de recuperare. C.A.R. are în vedere securitatea și protecția datelor prelucrate. Pentru a nu se afla în situația critică se va elabora un plan de salvare a aplicațiilor informatice astfel încât într-un timp foarte scurt să se permită restaurarea acestora și cu pierderi minime.

Ce trebuie să cuprindă planul:

- identificarea datelor și aplicațiilor care trebuie salvate;
- regularitatea cu care se vor face salvările;
- unde vor fi păstrate salvările;
- cine are acces la salvările efectuate;
- perioada de timp necesară pentu a fi păstrate datele până vor fi distruse.

Art.18. Desemnarea unui responsabil cu protecția datelor. C.A.R. desemnează responsabilul cu protecția datelor.

Rolul responsabilului cu protecția datelor:

- să informeze și să consilieze C.A.R. precum și angajații acestuia (împuterniciții) cu privire la obligațiile existente în domeniul protecției datelor cu caracter personal;
- să monitorizeze respectarea Regulamentului General privind Datele cu Caracter Personal și a legislației naționale în domeniul protecției datelor;
- să coopereze cu autoritatea pentru protecția datelor și să reprezinte punctul de contact în relația cu aceasta.

Art.19. Cartografierea prelucrărilor de date cu caracter personal.

Pentru a avea o evidență conformă cu cerințele R.G.P.D. C.A.R. identifică prelucrarea datelor cu caracter personal efectuate și păstrarea evidenței activităților de prelucrare.

În acest sens evidența cuprinde:

- denumirea și datele de contact ale C.A.R., ale reprezentantului C.A.R. și ale responsabilului/ împuternicitului cu protecția datelor;
- scopurile prelucrării;
- categoriile de persoane și categoriile de date cu caracter personal (lista membrilor);
- termenul limită de ștergere (se au în vedere mai cu seamă perioadele de după retragerea membrilor).

Art.20. C.A.R. stabilește o procedură proprie de soluționare a cererilor și a plângerilor adresate de persoanele vizate (membri/giranți/potențiali membri/debitori etc.), exercitarea drepturilor, în condițiile în care au fost colectate prin mijloace electronice datele cu caracter personal, se pot realiza în același mod pe cale electronică.

Consiliul director al C.A.R.S. Bucovina IFN