



# ASOCIAȚIA ROMÂNĂ A CĂRNII CALITATE TRADIȚIE SIGURANȚĂ

## ANEXA LA REGULAMENTUL INTERN AL ASOCIATIEI ROMANE A CARNII (ARC ) din data de 01.07.2018

### POLITICA INTERNA DE PRELUCRARE SI SECURIZARE A DATELOR CU CARACTER PERSONAL

#### 1. SCOPUL POLITICII

1.1. Scopul acestei politici este de a stabili masurile necesare si responsabilitatile angajatilor **ASOCIATIEI ROMANE A CARNII (in continuare ARC )**, pentru indeplinirea obligatiilor referitoare la garantarea si protejarea drepturilor si libertatilor fundamentale ale persoanelor fizice, in special a dreptului la viata intima, familiala si privata, cu privire la prelucrarea datelor cu caracter personal.

1.2. In vederea prelucrării si securizării datelor cu caracter personal colectate in cadrul activitatii ARC, sa va urmari aplicarea principiilor si a regulilor prevazute de actele internationale - Declaratia Universala a Drepturilor Omului, Conventia pentru Apararea Drepturilor Omului si a Libertatilor Fundamentale; de cele europene - Carta drepturilor fundamentale a Uniunii Europene, Regulamentul general privind protectia datelor nr. 679 din 27 aprilie 2016, precum si de cele nationale.

#### 2. DOMENIUL DE APLICARE

2.1. Prezenta Politica se aplica tuturor angajatilor ARC si/sau dupa caz persoanelor imputernicite, indicand drepturile si obligatiile acestora in ceea ce priveste datele cu caracter personale colectate de catre asociatie.

2.2. Confidentialitatea si securitatea reprezinta o componenta esentiala a derularii optime a activitatii ARC , sens in care prezenta Politica prevede cerinte si reguli imperative pentru protectia tuturor informatiilor, cu precadere a datelor cu caracter personal, impotriva influentelor naturale, erorilor umane si tehnice, precum si impotriva actiunilor deliberate care pot provoca pagube



materiale, respective imateriale, sau care pot duce la incalcari ale legislatiei. Avand in vedere faptul ca siguranta datelor nu poate fi garantata exclusiv cu ajutorul unor sisteme tehnice, prezenta Politica vizeaza, de asemenea, aspecte de ordin organizatorico-juridic si de alta natura.

2.3. Reglementarile prezentei Politici vor proteja datele cu caracter personal ale partenerilor contractuali ai ARC, cat si ale angajatilor sai.

### 3. DEFINITII

- ANSPDCP = Autoritatea Nationala de Supraveghere a Prelucrării Datelor cu Caracter Personal;
- „date cu caracter personal” inseamna orice informatii privind o persoana fizica identificata sau identificabila ("persoana vizata"); o persoana fizica identificabila este o persoana care poate fi identificata, direct sau indirect, in special prin referire la un element de identificare, cum ar fi un nume, un numar de identificare, date de localizare, un identificator online, sau la unul sau mai multe elemente specifice, proprii identitatii sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale;
- „date cu caracter personal sensibile/speciale” inseamna date cu caracter personal care dezvaluie originea rasiala sau etnica, opiniile politice, confesiunea religioasa sau convingerile filozofice sau apartenenta la sindicate si prelucrarea de date genetice, date biometrice pentru identificarea unica a unei persoane fizice, date privind sanatatea sau date privind viata sexuala sau orientarea sexuala ale unei persoane fizice.
- „prelucrare” inseamna orice operatiune sau set de operatiuni efectuate asupra datelor cu caracter personal sau asupra seturilor de date cu caracter personal, cu sau fara utilizarea de mijloace automatizate, cum ar fi colectarea, inregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, divulgarea prin transmitere, diseminarea sau punerea la dispozitie in orice alt mod, alinierea sau combinarea, restrictionarea, stergerea sau distrugerea;
- „restrictionarea prelucrării” inseamna mARC area datelor cu caracter personal stocate cu scopul de a limita prelucrarea viitoare a acestora;



## ASOCIAȚIA ROMÂNĂ A CĂRNII CALITATE TRADIȚIE SIGURANȚĂ

- „operator” înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care, singur sau împreună cu altele, stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal; atunci când scopurile și mijloacele prelucrării sunt stabilite prin dreptul Uniunii sau dreptul intern, operatorul sau criteriile specifice pentru desemnarea acestuia pot fi prevăzute în dreptul Uniunii sau în dreptul intern;
- „persoana împuternicită de operator” înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care prelucrează datele cu caracter personal în numele operatorului;
- „destinatar” înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism careia (caruia) îi sunt divulgate datele cu caracter personal, indiferent dacă este sau nu o parte terță. Cu toate acestea, autoritățile publice cărora li se pot comunica date cu caracter personal în cadrul unei anumite anchete în conformitate cu dreptul Uniunii sau cu dreptul intern nu sunt considerate destinatari; prelucrarea acestor date de către autoritățile publice respective respectă normele aplicabile în materie de protecție a datelor, în conformitate cu scopurile prelucrării;
- „parte terță” înseamnă o persoană fizică sau juridică, autoritate publică, agenție sau organism altul decât persoana vizată, operatorul, persoana împuternicită de operator și persoanele care, sub directă autoritate a operatorului sau a persoanei împuternicite de operator, sunt autorizate să prelucreze date cu caracter personal;
- „utilizator” - orice persoană care acționează sub autoritatea operatorului, a persoanei împuternicite sau a reprezentantului, cu drept recunoscut de acces la bazele de date cu caracter personal;
- „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 printr-o acțiune fără echivoc, ca datele cu caracter personal care o privesc să fie prelucrate.

#### 4. REGULI GENERALE



## ASOCIAȚIA ROMÂNĂ A CĂRNII CALITATE TRADIȚIE SIGURANȚĂ

4.1. ARC a adoptat masuri tehnice si organizatorice adecvate pentru protejarea datelor cu caracter personal impotriva distrugerilor accidentale sau ilegale, pierderii, modificarii, dezvaluirii sau accesului neautorizat, prevazute atat de legislatia interna, cat si de Regulamentul nr. 679/2016.

4.2. Toti salariatii au responsabilitatea respectarii regulilor de prelucrare a datelor cu caracter personal. Niciun salariat, indiferent de nivelul de autoritate/control detinut in cadrul asociatiei, nu va dezvalui sau transmite date cu caracter personal, de care ia cunostina in exercitarea functiei, in afara cadrului organizational intern si nu va utiliza informatii private pe care le detine cu privire la colegii sai in alte scopuri decat cele legale si necesare desfasurarii activitatii sale.

4.3. Raspunderea salariatilor pentru incalcarea prevederilor aplicabile datelor cu caracter personal va putea fi, in functie de particularitatile incalcarii, civila, administrativa sau penala, precum si disciplinara conform prezentelor Proceduri si Regulamentului Intern aplicabil la nivelul unitatii.

### **5. DREPTURILE PERSOANELOR ALE CAROR DATE PERSONALE SUNT COLECTATE SI/ SAU PRELUCRATE**

5.1. Persoanele vizate de colectarea datelor cu caracter personal vor beneficia de urmatoarele drepturi: dreptul la informare; dreptul de acces la date; dreptul de interventie asupra datelor; dreptul de opozitie; dreptul de a nu fi supus unei decizii individuale; dreptul de a fi uitat; dreptul la portabilitatea datelor si dreptul de a se adresa justitiei.

5.2. Exercitarea drepturilor persoanelor vizate se va realiza in conformitate cu prevederile legale, nationale si internationale, aplicabile, precum si in conformitate cu Politica de Confidentialitate a Datelor cu Caracter Personal a ARC .

5.3. Persoanele vizate vor avea acces la toate informatiile privind utilizarea datelor cu caracter personal prin metode corespunzatoare de informare, in special prin publicarea Politicii de Confidentialitate a Datelor cu Caracter Personal pe site-ul oficial al asociatiei:

[www.asociatia-carnii.ro](http://www.asociatia-carnii.ro).

### **6. MASURI TEHNICE SI ORGANIZATORICE DE PROTECTIE A DATELOR CU CARACTER PERSONAL**



## 6.1. Masuri generale de administrare a securitatii datelor cu caracter personal

6.1.1. Procesele activitatii ARC includ masuri organizatorice si tehnice corespunzatoare asigurarii prelucrării conforme a datelor cu caracter personal, dupa cum urmeaza:

- Impiedicarea accesului persoanelor neautorizate la sistemele de prelucrare a datelor in care sunt procesate sau utilizate date cu caracter personal (controlul privind accesul fizic).
- Asigurarea imposibilitatii utilizarii sistemelor de prelucrare a datelor de catre persoane neautorizate (controlul privind refuzul la utilizare).
- Persoanele autorizate sa utilizeze sistemele de prelucrare a datelor pot accesa in mod exclusiv acele date in legatura cu care dispun de acces autorizat, iar datele cu caracter personal nu vor putea fi citite, copiate, modificate sau eliminate in timpul activitatilor de prelucrare sau utilizare sau dupa inregistrarea acestora, de catre persoane neautorizate (controlul privind accesul la date).
- Asigurarea faptului ca, in cursul transmiterii electronice sau al transportului sau al inregistrării datelor cu caracter personal pe suport de date, acestea nu pot fi citite, copiate, modificate sau eliminate de catre persoane neautorizate, si ca se poate verifica si stabili unde urmeaza a fi transmise datele cu caracter personal prin intermediul echipamentelor de transmisiuni de date (controlul privind transmisiunea datelor).
- Asigurarea faptului ca este posibila examinarea retrospectiva si stabilirea daca si de catre cine au fost introduse, modificate sau eliminate datele cu caracter personal in cadrul sistemelor de procesare a datelor (controlul introducerii datelor).
- Asigurarea faptului ca datele cu caracter personal care sunt procesate de subcontractori pot fi prelucrate numai in conformitate cu instructiunile partii care solicita acest lucru (controlul privind sub-contractorii).
- Asigurarea faptului ca datele cu caracter personal sunt protejate impotriva distrugerilor sau pierderilor accidentale (controlul privind disponibilitatea datelor).

6.1.2. Salariatii ARC au obligatia de confidentialitate si vor respecta regulile si procesele interne implementate la nivelul asociatiei pentru protectia datelor cu caracter personal, atat ale clientilor, cat si ale salariatilor, asociatilor sau ale colaboratorilor persoane fizice.



6.1.3. Salariații nu vor utiliza echipamentele de lucru ale angajatorului pentru comunicări în scop personal, înțelegând că se expun riscului ca datele cu caracter personal din respectivele comunicări să fie accesate de angajator în exercitarea dreptului său de a verifica respectarea obligațiilor de serviciu ale angajaților.

### 6.2. **Măsuri de protecție a datelor cu caracter personal la momentul colectării**

6.2.1. Colectarea datelor cu caracter personal se va realiza exclusiv pentru scopurile și durata prevăzută în cadrul Politicii de Confidentialitate a Datelor cu Caracter Personal, precum și conform prevederilor legale aplicabile, cu informarea prealabilă a persoanei vizate.

6.2.2. Atunci când datele personale nu sunt colectate direct de la persoanele vizate se va asigura că persoanele de la care sunt primite respectivele date transmit persoanelor vizate informațiile pe care le-ar fi aflat în cazul unui contact direct cu operatorul.

6.2.3. Colectarea datelor cu caracter personal se va realiza exclusiv de către persoanele din cadrul ARC cu atribuții specifice în acest sens. Orice operațiune de colectare și/sau modificare a datelor cu caracter personal este înregistrată prin mijloace tehnice electronice sau pe suport hârtie, după caz, fiind de asemenea înregistrate și toate logările și delogările tuturor utilizatorilor la baza de date.

### 6.3. **Securitatea mediului fizic folosit în procesul prelucrării datelor cu caracter personal**

a) Accesul în birourile ori spațiile unde sunt amplasate sistemele informaționale de date cu caracter personal este restricționat, fiind permis doar persoanelor care au autorizația necesară, conform organigramei.

b) Se asigură administrarea și monitorizarea accesului fizic în toate punctele de acces la sistemele informaționale de date cu caracter personal, inclusiv se reacționează la încălcarea regimului de acces.

c) Perimetrul de securitate al ARC reprezintă perimetrul spațiilor în care se prelucrează/stochează date cu caracter personal de către persoanele autorizate și al spațiilor la care au acces beneficiarii serviciilor puse la dispoziție de asociație.



- d) Perimetrul cladirii sau incaperilor in care sunt amplasate mijloacele de prelucrare a datelor cu caracter personal este integru din punct de vedere fizic, peretii exteriori ai incaperilor sunt rezistenti, intrarile sunt echipate cu incuietoare si semnalizare.
- e) Amplasarea mijloacelor de prelucrare a datelor cu caracter personal corespunde necesitatii asigurarii securitatii acestora contra accesului nepermis, furturilor, incendiilor, inundatiilor si altor posibile riscuri.
- f) Usile si ferestrele se incuie in cazul in care din incapere lipsesc persoanele autorizate.
- g) Computerele, serverele, alte terminale de acces sunt amplasate in locuri cu acces limitat pentru persoane straine.
- h) Pentru protejarea statiilor de lucru vor fi utilizate parole de acces.
- i) In momentul parasirii locului de munca sau pe durata calatoriilor in interes de serviciu statiile de lucru vor fi blocate.
- j) Utilizarea dispozitivelor mobile de stocare a datelor este conditionata, fiind permisa doar pe anumite statii de lucru, dupa informarea si aprobarea in scris de catre coordonator (superior);

#### 6.4. Controlul accesului la datele cu caracter personal

##### 6.4.1. Autentificarea utilizatorilor:

- a) Este efectuata identificarea si autentificarea utilizatorilor sistemelor informationale de date cu caracter personal si a proceselor executate in numele acestor utilizatori.
- b) In cazul accesarii datelor cu caracter personal in baza unei parole, vor fi respectate urmatoarele criterii:
- parola nu trebuie sa fie predictibila, sa contina cuvinte din dictionar;
  - parola trebuie sa aiba o lungime de minim 8 caractere, pentru laptopuri, calculatoare, notebook-uri;
  - parola trebuie sa contina un mix de caractere alfabetice, atat litere mari cat si litere mici (exemplu: a; C; d; e etc.) si non-alfabetice (!, #, \$, %, 6, 8, etc.);
  - parola trebuie sa contina un mix de cel putin doua tipuri de caractere non-alfabetice;
  - parola nu trebuie sa contina parti din nume, prenume, adrese de e-mail, numar de utilizator;
  - parola trebuie sa fie schimbata la intervale regulate de timp, respectiv la cel mult fiecare 90 de zile calendaristice;





## ASOCIAȚIA ROMÂNĂ A CĂRNII CALITATE TRADIȚIE SIGURANȚĂ

- o parola nu trebuie sa fie una utilizata in mediul privat, respectiv in afara mediului de lucru din cadrul asociatiei ARC .

Exemplu de parola corespunzatoare din punct de vedere al complexitatii: AS178dr! sau 17#\*AMsl

Comunicare catre terte persoane a parolelor utilizate in vederea asigurarii statiilor de lucru este strict interzisa.

- c) Orice utilizator care primeste un cod de identificare si un mijloc de autentificare este obligat prin fisa postului si Regulamentul Intern sa pastreze confidentialitatea acestora si sa raspunda in acest sens in fata operatorului.
- d) In cazul in care contractul de munca al utilizatorului a fost incetat, suspendat sau modificat si noile sarcini nu necesita accesul la date cu caracter personal ori drepturile de acces ale utilizatorului au fost modificate, ori utilizatorul a abuzat de codurile primite in scopul comiterii unei fapte prejudiciabile, a absentat o perioada indelungata, codurile de identificare si autentificare se revoca sau se suspenda de administratorul I.T. sau, dupa caz, de conducerea asociatiei.

### 6.4.2. Tipul de acces

- a) Utilizatorii trebuie sa acceseze numai datele cu caracter personal necesare pentru indeplinirea atributiilor lor de serviciu. Pentru aceasta trebuie sa fie stabilite tipurile de acces dupa functionalitate (administrare, introducere, prelucrare, salvare etc.) si dupa actiuni aplicate asupra datelor cu caracter personal (scriere, citire, stergere), precum si procedurile privind aceste tipuri de acces.
- b) Compartimentul care asigura suportul tehnic poate avea acces la datele cu caracter personal pentru rezolvarea incidentelor si a problemelor aparute in utilizarea sistemelor informatice.

### 6.4.3. Accesul la distanta

- a) Securitatea statiei de lucru, in eventualitatea desfasurarii unor calatorii in interes de serviciu sau a scoaterii statiei de lucru din incinta locului de munca, este responsabilitatea angajatului sau a





colaboratorului. Stațiile de lucru nu se vor lăsa nesupravegheate și se vor asigura, din punct de vedere fizic, corespunzător. Pe durata călătoriilor aeriene, stațiile de lucru nu se vor depozita în bagajele de cală, de asemenea stațiile de lucru nu se vor lăsa nesupravegheate într-un autovehicul neocupat.

#### 6.5. **Securitatea mijloacelor fixe/materiale**

a) Stocarea datelor cu caracter personal pe suport magnetic, optic, de hartie sau alt suport fix al informației, pe care se creează, se fixează, se transmite, se recepționează, se păstrează sau, în alt mod, se utilizează documentul și care permite reproducerea acestuia, este asigurată prin plasarea acestora în dulapuri care se încuie sau prezintă un alt mecanism de securizare. Scoaterea, fără autorizare, a purtătorilor de date cu caracter personal din perimetrul de securitate al operatorului este interzisă.

b) Scoaterea la imprimantă a datelor cu caracter personal se va realiza numai de utilizatori autorizați de către conducerea asociației pentru această operațiune.

#### 6.6. **Securitatea mijloacelor electronice**

a) Echipamentul electric utilizat pentru menținerea funcționalității sistemelor informaționale de date cu caracter personal, a cablurilor electrice este asigurată contra deteriorărilor și conexiunilor nesancționate, prin montarea lor în nișe speciale.

b) Serverele care găzduiesc date cu caracter personal pot fi accesate doar în mod controlat, pe baza de drepturi de acces.

c) Ca regulă generală, este interzisă stocarea de date cu caracter personal și scoaterea din incinta asociației, prin intermediul mediilor mobile de stocare, precum CD/DVD, stick-uri USB, hard disk-uri externe. Excepție de la această regulă pot face echipamentele de back-up, a căror utilizare este aprobată în prealabil de conducerea asociației.

d) Dezactivarea programelor anti-malware preinstalate pe stațiile de lucru este strict interzisă. În plus, fiecare colaborator sau angajat are obligația de a nu modifica setările respectivului program anti-malware, în special setările care vizează următoarele funcționalități, sub sancțiunea atragerii răspunderii: de blocare și detectare a programelor de tip malware; de efectuare a unor scanări



periodice in vederea identificarii eventualelor programe malware; de actualizare a semnatuurilor utilizate la identificarea programelor malware; de actualizare a produsului antimalware.

e) Stațiile de lucru utilizate au activate firewall-uri personale, respectiv activate la nivelul fiecărei stații de lucru, fiind strict interzisă efectuarea unor setări asupra acestei funcționalități a sistemului de operare, care să vizeze, nelimitativ, următoarele: detectarea rețelelor care ar trebui să fie tratate ca și necunoscute; alertarea user-ilor cu privire la programele care solicită acces la rețeaua de internet; blocarea accesului neautorizat.

f) Ca regula principală, instalarea de programe software neautorizate, pe stațiile de lucru care sunt în proprietatea ARC, este strict interzisă. În cazul în care este necesară, în vederea desfășurării unor procese de business, instalarea unor programe tip software, angajatul sau colaboratorul va solicita suport.

g) În cazul apariției situațiilor excepționale, de avarie sau de forță majoră, este asigurată posibilitatea deconectării electricității la sistemele informaționale de date cu caracter personal, inclusiv posibilitatea deconectării oricărui component IT.

#### 6.7. **Măsuri de tehnica informațională pentru securizarea datelor cu caracter personal**

a) Toți salariații ARC au obligația respectării confidențialității, integrității și disponibilității informațiilor asociației și ale clienților, în condiții de conformitate cu cerințele legale, reglementate și cu alte cerințe asumate de securitate a informației, precum și în condiții de asigurare a funcționalității și disponibilității activelor informatice, inclusiv hardware și software.

b) Toate datele cu caracter personal colectate de la membri, furnizori și alți parteneri contractuali ai ARC se vor păstra în baze de date supuse măsurilor de protecție adecvate.

c) Ca regula, este interzisă utilizarea stațiilor de lucru din proprietatea asociației în vederea conectării la internet prin rețele de internet neautorizate, respectiv rețele care nu sunt administrate de către ARC. În cazul în care stațiile de lucru se vor utiliza în regim de teleducă, iar desfășurarea activității presupune conectarea la internet prin intermediul unei rețele personale, care dispune de mijloace de protecție corespunzătoare (exemplu: rețea parolată, user admin cu parola personalizată,



## ASOCIAȚIA ROMÂNĂ A CĂRNII CALITATE TRADIȚIE SIGURANȚĂ

utilizarea unui algoritm de criptare altul decat WEP, dezactivarea functiei WPS), se va solicita acordul conducerii asociatiei.

d) Pentru programele software utilizate in vederea desfasurarii activitatii si in special in vederea procesarii de date cu caracter personal, este interzisa salvarea numelui de utilizator si a parolei prin intermediul browser-ului de internet. In plus, in cazul utilizarii unor aplicatii web, respectiv care necesita conexiune de internet, in cazul incetarii utilizarii respectivei aplicatii se va utiliza mereu functia de log off, respectiv delogare.

e) Comunicarea parolei de acces la infrastructura de internet din cadrul asociatiei (exemplu: routere wireless care ofera conectivitate la internet), este strict interzisa.

f) Utilizarea adresei de e-mail pusa la dispozitie de ARC este permisa doar in vederea exercitarii atributiilor de serviciu. Adresele de e-mail puse la dispozitie de asociatie nu se vor utiliza in vederea crearii de conturi pe pagini de internet sau aplicatii web, care nu au legatura cu desfasurarea activitatii ARC .

g) Personalul cu atributii speciale in domeniu informational va audita periodic masurile de securizare informationala si va raporta conducerii asociatiei, orice suspiciune ce ar putea conduce la un incident de securitate/bresa de securitate:

h) Toti angajatii ARC au obligatia de a informa neintarziat (cel mult 24 de ore) conducerea despre incidentele care incalca securitatea sistemelor informationale de date cu caracter personal.

### 6.8. Instruirea personalului

6.8.1. Personalul ARC este informat cu privire la prevederile normelor nationale, europene si internationale cu privire la colectarea si prelucrarea datelor cu caracter personal, la cerintele minime de securitate a prelucrarilor de date cu caracter personal, precum si cu privire la riscurile pe care le comporta prelucrarea datelor cu caracter personal.

6.8.2. Utilizatorii care au acces la date cu caracter personal vor fi instruiti periodic asupra confidentialitatii si securitatii acestora.

## 7. TRANSFERUL DATELOR CU CARACTER PERSONAL



## ASOCIAȚIA ROMÂNĂ A CĂRNII CALITATE TRADIȚIE SIGURANȚĂ

7.1. Datele cu caracter personal se pot comunica între ARC și imputerniciții acestora sau între ARC sau imputerniciții acestora și alte instituții ori organisme publice sau entități de drept public sau privat în una dintre următoarele situații:

- a) dacă persoana vizată și-a dat consimțământul expres și neechivoc pentru comunicarea datelor sale;
- b) atunci când există un interes legitim sau o obligație legală;
- c) în alte cazuri prevăzute de lege.

7.2. Comunicarea datelor cu caracter personal în situațiile prevăzute la art. 7.1. lit. b) și c) se poate face dacă este îndeplinită una dintre următoarele condiții:

- a) comunicarea se efectuează pe baza apartenenței unui membru la Asociație, a unui contract sau, după caz, a unui document de cooperare care trebuie să cuprindă cel puțin: temeiul legal al prelucrării și scopul acesteia, termenul maxim de prelucrare, drepturile și obligațiile părților, modalitățile de asigurare a securității prelucrărilor și de respectare a drepturilor persoanei vizate, precum și mențiunea că datele pot fi utilizate doar de structura beneficiară și numai în scopul pentru care au fost solicitate;
- b) comunicarea se efectuează în baza unei solicitări scrise, care trebuie să cuprindă temeiul legal, scopul prelucrării și datele solicitate.

7.3. Comunicarea datelor cu caracter personal se poate face și on-line, cu respectarea dispozițiilor art. 7.1. și 7.2. și asigurarea securității sistemelor de comunicații a datelor cu caracter personal.

7.4. Datele cu caracter personal asupra cărora persoanele vizate au exercitat și li s-a recunoscut dreptul de opoziție nu pot face obiectul prelucrării.

7.5. Cererile pentru comunicarea datelor cu caracter personal adresate ARC trebuie să conțină datele de identificare a solicitantului, precum și motivarea și scopul cererii, conform prevederilor legale.

7.6. Cererile care nu conțin aceste elemente se restituie pentru completare, iar cele care nu se încadrează în condițiile prevăzute de lege se resping, menționându-se motivele pentru care comunicarea datelor cu caracter personal nu este posibilă.



## ASOCIAȚIA ROMÂNĂ A CĂRNII CALITATE TRADIȚIE SIGURANȚĂ

7.7. Înainte de comunicarea datelor cu caracter personal, ARC verifica daca acestea sunt exacte si, daca este cazul, actualizate.

7.8. În situația în care se constată că au fost transmise date incorecte sau neactualizate, ARC are obligația de a informa destinatarul respectivelor date asupra neconformității acestora, cu menționarea datelor care au fost modificate.

7.9. La comunicarea datelor cu caracter personal ARC atenționează destinatarul asupra interdicției de a prelucra datele pentru alte scopuri decât cele specificate în cererea de comunicare.

7.10. Dezvăluirea prin transmitere a datelor cu caracter personal prin rețele comunicative ce nu corespund cerințelor de securitate, (*spre exemplu: expedierea informației prin intermediul e-mail-urilor personale de tipul @gmail.com, @mail.ru, @yahoo.com, etc.*) sunt interzise, cu excepția unor situații justificate în care există acordul superiorului.

7.11. Sunt interzise operațiunile de dezvăluire a datelor cu caracter personal între ARC și alte entități care sunt amplasate geografic în țări referitor la care Comisia Europeană a decis că nu asigură un nivel de protecție adecvat referitor la siguranța datelor cu caracter personal.

7.12. Atunci când asociația apelează la serviciile unui sub-contractor, persoana responsabilă cu negocierea și semnarea contractului din cadrul ARC va asigura faptul că în contractul relevant redactat în scris se vor face referiri la obligațiile sub-contractantului ca parte implicată în prelucrarea datelor. Aceste prevederi vor menționa instrucțiunile asociației (partea care controlează datele) cu privire la tipul și maniera prelucrării datelor cu caracter personal, scopul prelucrării, precum și măsurile tehnice și organizatorice necesare pentru protecția datelor. Criteriile privind securitatea datelor cu caracter personal și manipularea legală a acestora vor fi luate în considerare la selectarea sub-contractantului.

## **8. RASPUNDEREA PRIVIND SIGURANTA PRELUCRARIII DATELOR CU CARACTER PERSONAL**

### **8.1. Responsabilitatea angajatilor privind manipularea datelor cu caracter personal**



## ASOCIAȚIA ROMÂNĂ A CĂRNII CALITATE TRADIȚIE SIGURANȚĂ

8.1.1. ARC se angajează față de persoanele vizate de prelucrarea datelor cu caracter personal să respecte legislația aplicabilă, obligându-se în consecință și fiecărui salariat din cadrul asociației.

8.1.2. Personalul care asigură exploatarea datelor cu caracter personal va urmări incidentele de securitate, incluzând aici depistarea, analiza, preîntâmpinarea dezvoltării, înlăturarea incidentelor și restabilirea securității. Se vor monitoriza și documenta, în mod permanent, incidentele de securitate.

8.1.3. Persoanele care se fac vinovate de încălcarea normelor legale, precum și a politicilor proprii ARC privind obținerea, păstrarea, prelucrarea și protecția datelor cu caracter personal vor răspunde civil, contravențional sau penal, după caz.

8.1.4. Salariații ARC care încalcă normele legale, precum și politicile interne de protecție a datelor cu caracter personal vor săvârși o abatere disciplinară gravă, urmând să fie sancționați disciplinar în consecință.

### **9. DISPOZITII FINALE**

9.1. Prezenta Politică Internă este revizuită periodic și ulterior aprobată de către conducerea ARC, în conformitate cu necesitățile legale și practice aferente operațiunilor de colectare și prelucrare a datelor cu caracter personal.

9.2. Prezenta Politică Internă se completează cu prevederile legislației naționale, europene și internaționale în vigoare precum și cu procedurile interne anexate.

9.3. Politică Internă va putea fi comunicată angajaților prin e-mail, acolo unde comunicarea cu aceștia se face în mod frecvent în această manieră, urmând ca aceștia să semneze în vederea luării la cunostință.

**ASOCIATIA ROMANA A CARNII**

**Prin Presedinte, dl. Radu Timiș**