

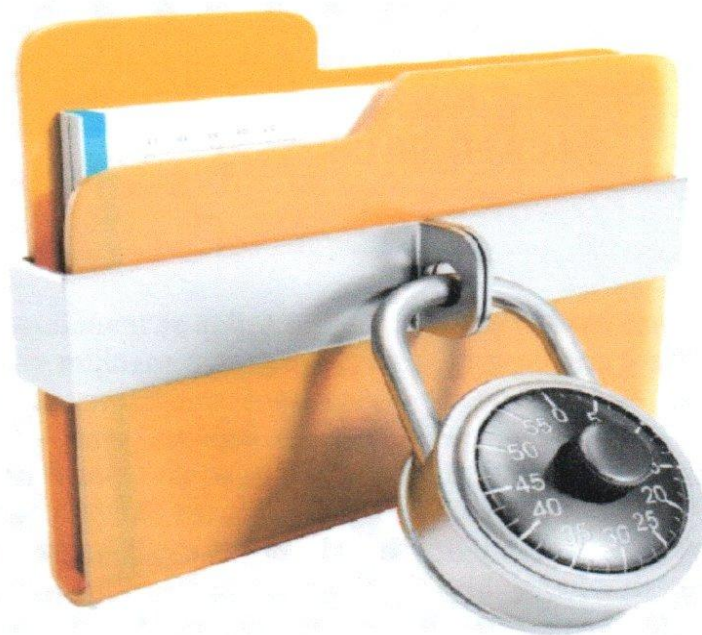


GRĂDINIȚA CU PROGRAM PRELUNGIT „MIHAI EMINESCU”  
STR. OLARI, NR. 3, COD 210258, TG-JIU, GORJ  
COD FISCAL: 29448992  
TEL./FAX: 0353 801417  
E-mail: gr\_eminescu\_gj@yahoo.com

GRĂDINIȚA CU PROGRAM PRELUNGIT  
„MIHAI EMINESCU”  
INTRARE Nr. 692  
IEȘIRE  
Ziua 17 Luna 05 Anul 2018

## REGULAMENT

# privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date



**Avizat:**  
**Aprobat:**  
**Ediția 1**

**Intrat în vigoare**

Consiliul de Administrație al GPPME  
Director, Prof. Ana-Maria Bîzdoacă

Hotărâre nr. 6/15.05.2018



25 Mai 2018

# CAPITOLUL I DISPOZIȚII GENERALE

## SCOPUL ȘI SFERA DE APLICARE

### Art. 1

- (1) Prezentul regulament are ca scop garantarea și protejarea drepturilor și libertăților fundamentale ale persoanelor fizice, în special a dreptului la viața intimă, familială și privată, cu privire la prelucrarea datelor cu caracter personal prelucrate de Grădinița cu Program Prolungit „Mihai Eminescu” Tg-Jiu, denumită în continuare GPPME, operator.
- (2) Exerțarea drepturilor prevăzute în prezentul regulament nu poate fi restrânsă decât în cazuri expres și limitativ prevăzute de lege.
- (3) Prezentul regulament stabilește normele referitoare la protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal, precum și normele referitoare la libera circulație a datelor cu caracter personal.
- (4) Prezentul regulament asigură protecția drepturilor și libertăților fundamentale ale persoanelor fizice și în special a dreptului acestora la protecția datelor cu caracter personal.
- (5) Libera circulație a datelor cu caracter personal în interiorul Uniunii nu poate fi restricționată sau interzisă din motive legate de protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal.

## CAPITOLUL II DOMENIU DE APLICARE

### Art. 2

- (1) Prezentul regulament se aplică prelucrărilor de date cu caracter personal, efectuate, în tot sau în parte, prin mijloace automate, precum și prelucrării prin alte mijloace decât cele automate a datelor cu caracter personal care fac parte dintr-un sistem de evidență sau care sunt destinate să fie incluse într-un asemenea sistem.
- (2) Prezentul regulament nu se aplică prelucrării datelor cu caracter personal:
  - a) în cadrul unei activități care nu intră sub incidența dreptului Uniunii;
  - b) de către o persoană fizică în cadrul unei activități exclusiv personale sau domestice;
  - c) de către autoritățile competente în scopul prevenirii, investigării, depistării sau urmăririi penale a infracțiunilor, sau al executării sancțiunilor penale, inclusiv al protejării împotriva amenințărilor la adresa siguranței publice și al prevenirii acestora.

### Art. 3

- (1) Prezentul regulament are ca scop stabilirea unor norme de conduită pentru asigurarea unui nivel satisfăcător de protecție a datelor cu caracter personal prelucrate de către Grădinița cu Program Prolungit „Mihai Eminescu” Tg-Jiu, denumită în continuare GPPME, operator.
- (2) Normele de conduită stabilesc exercitarea drepturilor și obligațiilor pe care GPPME le are în domeniul protecției persoanelor în privința datelor cu caracter personal, în relațiile instituției cu persoanele vizate, cu alte instituții de învățământ, precum și cu alte persoane fizice sau juridice.

(3) Normele cuprinse în prezentul regulament nu aduc atingere altor obligații legale imperative sau deontologice ce revin GPPME.

### **CAPITOLUL III DEFINIREA TERMENILOR**

**Art. 4** În sensul prezentului regulament:

1. "date cu caracter personal" înseamnă orice informații privind o persoană fizică identificată sau identificabilă ("persoana vizată"); o persoană fizică identificabilă este o persoană care poate fi identificată, direct sau indirect, în special prin referire la un element de identificare, cum ar fi un nume, un număr de identificare, date de localizare, un identificator online, sau la unul sau mai multe elemente specifice, proprii identității sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale;
2. "prelucrare" înseamnă orice operațiune sau set de operațiuni efectuate asupra datelor cu caracter personal sau asupra seturilor de date cu caracter personal, cu sau fără utilizarea de mijloace automatizate, cum ar fi colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, divulgarea prin transmitere, diseminarea sau punerea la dispoziție în orice alt mod, alinierea sau combinarea, restricționarea, ștergerea sau distrugerea;
3. "restricționarea prelucrării" înseamnă marcarea datelor cu caracter personal stocate cu scopul de a limita prelucrarea viitoare a acestora;
4. "creare de profiluri" înseamnă orice formă de prelucrare automată a datelor cu caracter personal care constă în utilizarea datelor cu caracter personal pentru a evalua anumite aspecte personale referitoare la o persoană fizică, în special pentru a analiza sau prevedea aspecte privind performanța la locul de muncă, situația economică, sănătatea, preferințele personale, interesele, fiabilitatea, comportamentul, locul în care se află persoana fizică respectivă sau deplasările acesteia;
5. "pseudonimizare" înseamnă prelucrarea datelor cu caracter personal într-un asemenea mod încât acestea să nu mai poată fi atribuite unei anume persoane vizate fără a se utiliza informații suplimentare, cu condiția ca aceste informații suplimentare să fie stocate separat și să facă obiectul unor măsuri de natură tehnică și organizatorică care să asigure neatribuirea respectivelor date cu caracter personal unei persoane fizice identificate sau identificabile;
6. "sistem de evidență a datelor" înseamnă orice set structurat de date cu caracter personal accesibile conform unor criterii specifice, fie ele centralizate, descentralizate sau repartizate după criterii funcționale sau geografice;
7. "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;
8. "persoană împuternicită de operator" înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care prelucrează datele cu caracter personal în numele operatorului;
9. "destinatar" înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism căreia (cărui) 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;

10. "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 directa autoritate a operatorului sau a persoanei împuternicite de operator, sunt autorizate să prelucreze date cu caracter personal;

11. "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;

12. "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;

13. "date genetice" înseamnă datele cu caracter personal referitoare la caracteristicile genetice moștenite sau dobândite ale unei persoane fizice, care oferă informații unice privind fiziologia sau sănătatea persoanei respective și care rezultă în special în urma unei analize a unei mostre de material biologic recoltate de la persoana în cauză;

14. "date biometrice" înseamnă o date cu caracter personal care rezultă în urma unor tehnici de prelucrare specifice referitoare la caracteristicile fizice, fiziologice sau comportamentale ale unei persoane fizice care permit sau confirmă identificarea unică a respectivei persoane, cum ar fi imaginile faciale sau datele dactiloscopice;

15. "date privind sănătatea" înseamnă date cu caracter personal legate de sănătatea fizică sau mentală a unei persoane fizice, inclusiv prestarea de servicii de asistență medicală, care dezvăluie informații despre starea de sănătate a acesteia;

17. "reprezentant" înseamnă o persoană fizică sau juridică stabilită în Uniune, desemnată în scris de către operator sau persoana împuternicită de operator, care reprezintă operatorul sau persoana împuternicită în ceea ce privește obligațiile lor respective care le revin în temeiul prezentului regulament;

18. "autoritate de supraveghere" înseamnă o autoritate publică independentă instituită de un stat membru;

19. "autoritate de supraveghere vizată" înseamnă o autoritate de supraveghere care este vizată de procesul de prelucrare a datelor cu caracter personal deoarece:

(a) operatorul sau persoana împuternicită de operator este stabilită pe teritoriul statului membru al autorității de supraveghere respective;

(b) persoanele vizate care își au reședința în statul membru în care se află autoritatea de supraveghere respectivă sunt afectate în mod semnificativ sau sunt susceptibile de a fi afectate în mod semnificativ de prelucrare; sau

(c) la autoritatea de supraveghere respectivă a fost depusă o plângere;

20. "obiecție relevantă și motivată" înseamnă o obiecție la un proiect de decizie în scopul de a stabili dacă există o încălcare a prezentului regulament sau dacă măsurile preconizate în ceea ce privește operatorul sau persoana împuternicită de operator respectă prezentul regulament, care demonstrează în mod clar importanța riscurilor pe care le prezintă proiectul de decizie în ceea ce privește drepturile și libertățile fundamentale ale persoanelor vizate și, după caz, libera circulație a datelor cu caracter personal în cadrul Uniunii.

**Art. 5** Principii legate de prelucrarea datelor cu caracter personal

(1) Datele cu caracter personal sunt:

a) prelucrate în mod legal, echitabil și transparent față de persoana vizată ("legalitate, echitate și transparență");

b) colectate în scopuri determinate, explicite și legitime și nu sunt prelucrate ulterior într-un mod incompatibil cu aceste scopuri; prelucrarea ulterioară în scopuri de arhivare în interes

public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice nu este considerată incompatibilă cu scopurile inițiale ("limitări legate de scop");

c) adecvate, relevante și limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate ("reducerea la minimum a datelor");

d) exacte și, în cazul în care este necesar, să fie actualizate; trebuie să se ia toate măsurile necesare pentru a se asigura că datele cu caracter personal care sunt inexacte, având în vedere scopurile pentru care sunt prelucrate, sunt șterse sau rectificate fără întârziere ("exactitate");

e) păstrate într-o formă care permite identificarea persoanelor vizate pe o perioadă care nu depășește perioada necesară îndeplinirii scopurilor în care sunt prelucrate datele; datele cu caracter personal pot fi stocate pe perioade mai lungi în măsura în care acestea vor fi prelucrate exclusiv în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice, sub rezerva punerii în aplicare a măsurilor de ordin tehnic și organizatoric adecvate prevăzute în prezentul regulament în vederea garantării drepturilor și libertăților persoanei vizate ("limitări legate de stocare");

f) prelucrate într-un mod care asigură securitatea adecvată a datelor cu caracter personal, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luarea de măsuri tehnice sau organizatorice corespunzătoare ("integritate și confidențialitate").

(2) Operatorul este responsabil de respectarea alineatului (1) și poate demonstra această respectare ("responsabilitate").

## CAPITOLUL IV

### REGULI GENERALE PRIVIND PRELUCRAREA DATELOR CU CARACTER PERSONAL

#### A. Caracteristicile datelor cu caracter personal în cadrul prelucrării

##### Art. 6

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

a) **prelucrate cu bună-credință** și în conformitate cu dispozițiile legale în vigoare;

b) **colectate** în scopuri determinate, explicite și legitime; prelucrarea ulterioară a datelor cu caracter personal în scopuri statistice, de cercetare istorică sau științifică nu va fi considerată incompatibilă cu scopul colectării dacă se efectuează cu respectarea dispozițiilor legii, inclusiv a celor care privesc efectuarea notificării către autoritatea de supraveghere, precum și cu respectarea garanțiilor privind prelucrarea datelor cu caracter personal, prevăzute de normele care reglementează activitatea statistică ori cercetarea istorică sau științifică;

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

d) **exacte și, dacă este cazul, actualizate**, în acest scop se vor lua măsurile necesare pentru ca datele inexacte sau incomplete din punct de vedere al scopului pentru care sunt colectate și pentru care vor fi ulterior prelucrate, să fie șterse sau rectificate;

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

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

##### Art. 7 Legalitatea prelucrării

(1) Prelucrarea este legală numai dacă și în măsura în care se aplică cel puțin una dintre următoarele condiții:

- a) persoana vizată și-a dat consimțământul pentru prelucrarea datelor sale cu caracter personal pentru unul sau mai multe scopuri specifice;
- b) prelucrarea este necesară pentru executarea unui contract la care persoana vizată este parte sau pentru a face demersuri la cererea persoanei vizate înainte de încheierea unui contract;
- c) prelucrarea este necesară în vederea îndeplinirii unei obligații legale care îi revine operatorului;
- d) prelucrarea este necesară pentru a proteja interesele vitale ale persoanei vizate sau ale altei persoane fizice;
- e) prelucrarea este necesară pentru îndeplinirea unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice cu care este învestit operatorul;
- f) prelucrarea este necesară în scopul intereselor legitime urmărite de operator sau de o parte terță, cu excepția cazului în care prevalează interesele sau drepturile și libertățile fundamentale ale persoanei vizate, care necesită protejarea datelor cu caracter personal, în special atunci când persoana vizată este un copil. Litera (f) nu se aplică în cazul prelucrării efectuate de autorități publice în îndeplinirea atribuțiilor lor.

(2) În cazul în care prelucrarea în alt scop decât cel pentru care datele cu caracter personal au fost colectate nu se bazează pe consimțământul persoanei vizate sau pe dreptul Uniunii sau dreptul intern, care constituie o măsură necesară și proporțională într-o societate democratică, operatorul, pentru a stabili dacă prelucrarea în alt scop este compatibilă cu scopul pentru care datele cu caracter personal au fost colectate inițial, ia în considerare, printre altele:

- a) orice legătură dintre scopurile în care datele cu caracter personal au fost colectate și scopurile prelucrării ulterioare preconizate;
- b) contextul în care datele cu caracter personal au fost colectate, în special în ceea ce privește relația dintre persoanele vizate și operator;
- c) natura datelor cu caracter personal, în special în cazul prelucrării unor categorii speciale de date cu caracter personal, sau în cazul în care sunt prelucrate date cu caracter personal referitoare la condamnări penale și infracțiuni;
- d) posibilele consecințe asupra persoanelor vizate ale prelucrării ulterioare preconizate;
- e) existența unor garanții adecvate, care pot include criptarea sau pseudonimizarea.

(3) GPPME recunoaște și respectă dreptul la viața intimă, familială și privată, prelucrarea datelor cu caracter personal desfășurându-se în conformitate cu prevederile legale în vigoare.

(4) GPPME utilizează datele cu caracter personal ale persoanelor vizate prin intermediul unei baze de date alcătuite din informații obținute direct de la persoanele vizate prin consimțământul acestora și informații obținute de orice sursă externă autorizată de lege.

(5) GPPME este responsabilă pentru datele cu caracter personal aflate sub controlul său, precum și pentru datele transferate către terți.

(6) Persoanele care vor răspunde pentru respectarea dispozițiilor legale din domeniul protecției persoanelor și a datelor cu caracter personal, precum și a principiilor prevăzute de prezentul regulament sunt numai persoanele angajate în cadrul GPPME și care au ca atribuții colectarea, utilizarea, prelucrarea datelor cu caracter personal.

## **B. Condiții de legitimitate privind prelucrarea datelor**

### **Art. 8**

(1) În GPPME colectarea de date cu caracter personal prin mijloc frauduloase, neloiale sau ilegale este interzisă.

(2) Persoanele vizate vor fi informate asupra categoriilor de date care sunt prelucrate (nume, prenume, adresă, cod numeric personal, data și locul nașterii, serie și număr act de identitate, telefon, e-mail, venit, imagine, semnătură, adresa e-mail, date medicale, date privind cazierul judiciar, cetățenia, starea civilă), scopul prelucrării (angajării și derulării raporturilor de muncă, securității și sănătății în muncă, situațiilor de urgență, transport, medicina muncii, contabilitate - salarizare, publicare pe site-ul grădiniței, mass-media, în temeiul art. 6 alin. (1) lit. b, c din Regulamentul (UE) 2016/676 respectiv, prelucrarea este necesară pentru executarea unui contract la care persoana vizată este parte sau pentru a face demersuri la cererea unei persoane vizate înainte de încheierea unui contract; prelucrarea este necesară în vederea îndeplinirii unei obligații legale ce revine operatorului), precum și consecințele refuzului acestora de a furniza GPPME datele solicitate.

(3) Scopurile pentru care se colectează date se precizează în scris, într-un limbaj ușor accesibil pentru persoanele vizate.

#### **Art. 9**

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

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

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

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

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

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

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

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

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

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

(3) Consimțământul se exprimă prin completarea de formulare însoțite de note de informare a persoanelor vizate în legătură cu prelucrarea datelor cu caracter personal. După caz, GPPME va utiliza și alte variante de declarații concepute în aceeași manieră.

(4) Persoana vizată își poate retrage consimțământul în orice moment, sub condiția avizării prealabile a operatorului. Acesta va informa persoana vizată în legătură cu procedura și efectele retragerii consimțământului.

#### **Art. 10** Condiții privind consimțământul

(1) În cazul în care prelucrarea se bazează pe consimțământ, operatorul trebuie să fie în măsură să demonstreze că persoana vizată și-a dat consimțământul pentru prelucrarea datelor sale cu caracter personal.

(2) În cazul în care consimțământul persoanei vizate este dat în contextul unei declarații scrise care se referă și la alte aspecte, cererea privind consimțământul trebuie să fie prezentată într-o formă care o diferențiază în mod clar de celelalte aspecte, într-o formă inteligibilă și ușor accesibilă, utilizând un limbaj clar și simplu. Nicio parte a respectivei declarații care constituie o încălcare a prezentului regulament nu este obligatorie.

(3) Persoana vizată are dreptul să își retragă în orice moment consimțământul. Retragerea consimțământului nu afectează legalitatea prelucrării efectuate pe baza consimțământului înainte de retragerea acestuia. Înainte de acordarea consimțământului, persoana vizată este informată cu privire la acest lucru. Retragerea consimțământului se face la fel de simplu ca acordarea acestuia.

(4) Atunci când se evaluează dacă consimțământul este dat în mod liber, se ține seama cât mai mult de faptul că, printre altele, executarea unui contract, inclusiv prestarea unui serviciu, este condiționată sau nu de consimțământul cu privire la prelucrarea datelor cu caracter personal care nu este necesară pentru executarea acestui contract.

**Art. 11** Condiții aplicabile în ceea ce privește consimțământul copiilor în legătură cu serviciile societății informaționale

(1) În cazul în care se aplică articolul 6 alineatul (1) litera (a), în ceea ce privește oferirea de servicii ale societății informaționale în mod direct unui copil, prelucrarea datelor cu caracter personal ale unui copil este legală dacă copilul are cel puțin vârsta de 16 ani. Dacă copilul are sub vârsta de 16 ani, respectiva prelucrare este legală numai dacă și în măsura în care consimțământul respectiv este acordat sau autorizat de titularul răspunderii părintești asupra copilului.

(2) Operatorul depune toate eforturile rezonabile pentru a verifica în astfel de cazuri că titularul răspunderii părintești a acordat sau a autorizat consimțământul, ținând seama de tehnologiile disponibile.

(3) Alineatul (1) nu afectează dreptul general al contractelor aplicabil în statele membre, cum ar fi normele privind valabilitatea, încheierea sau efectele unui contract în legătură cu un copil.

### C. Încheierea operațiunilor de prelucrare

#### **Art. 12**

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

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

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

#### **Art. 13**

(1) GPPME va prelucra datele cu caracter personal numai pentru scopurile pentru care au fost colectate, cu excepția cazului în care persoana vizată își dă anterior consimțământul și pentru prelucrarea în alte scopuri sau în alte cazuri premise de lege.

(2) Accesul la datele prelucrate va fi permis numai angajaților GPPME, în îndeplinirea obligațiilor de serviciu.

#### **Art. 14**

GPPME se obligă să ia toate măsurile necesare pentru păstrarea datelor cu caracter personal de o manieră exactă, completată și actualizată, pentru a îndeplini scopurile pentru care acestea au fost colectate.

(2) Datele inexacte sau incomplete vor fi rectificate sau eliminate în evidența curentă.



(3) Datele cu caracter personal vor fi păstrate numai pe perioada necesară îndeplinirii scopurilor stabilite, cu respectarea drepturilor persoanei vizate, în special a dreptului de acces, de intervenție și de opoziție.

(4) În urma verificărilor periodice datele cu caracter personal deținute de operator, care nu mai servesc realizării scopurilor sau îndeplinirii unor obligații legale, vor fi distruse sau transformate în date anonime într-un interval de timp rezonabil, potrivit procedurilor stabilite de lege.

#### **Art. 15**

GPPME are obligația de a lua toate măsurile tehnice și organizatorice necesare pentru asigurarea unui nivel de protecție și de securitate adecvat, în cadrul operațiunilor efectuate asupra datelor cu caracter personal: pseudonimizarea și criptarea datelor cu caracter personal; capacitatea de a asigura confidențialitatea, integritatea, disponibilitatea și rezistența continue 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 periodice ale eficacității măsurilor tehnice și organizatorice pentru a garanta securitatea prelucrării. În acest scop la bazele de date vor avea acces numai persoanele autorizate, iar copierea datelor se va putea face numai la locul în care sunt gestionate.

## **CAPITOLUL V**

### **REGULI SPECIALE PRIVIND PRELUCRAREA DATELOR CU CARACTER PERSONAL**

#### **A. Prelucrarea unor categorii speciale de date**

#### **Art. 16**

(1) Prelucrarea de date cu caracter personal care dezvăluie originea rasială sau etnică, opiniile politice, confesiunea religioasă sau convingerile filozofice sau apartenența la sindicate și prelucrarea de date genetice, de date biometrice pentru identificarea unică a unei persoane fizice, de date privind sănătatea sau de date privind viața sexuală sau orientarea sexuală ale unei persoane fizice este interzisă.

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

- a) persoana vizată și-a dat consimțământul explicit pentru prelucrarea acestor date cu caracter personal pentru unul sau mai multe scopuri specifice, cu excepția cazului în care dreptul Uniunii sau dreptul intern prevede ca interdicția prevăzută la alineatul (1) să nu poată fi ridicată prin consimțământul persoanei vizate;
- b) prelucrarea este necesară în scopul îndeplinirii obligațiilor și al exercitării unor drepturi specifice ale operatorului sau ale persoanei vizate în domeniul ocupării forței de muncă și al securității sociale și protecției sociale, în măsura în care acest lucru este autorizat de dreptul Uniunii sau de dreptul intern ori de un acord colectiv de muncă încheiat în temeiul dreptului intern care prevede garanții adecvate pentru drepturile fundamentale și interesele persoanei vizate;
- c) prelucrarea este necesară pentru protejarea intereselor vitale ale persoanei vizate sau ale unei alte persoane fizice, atunci când persoana vizată se află în incapacitate fizică sau juridică de a-și da consimțământul;
- d) prelucrarea este efectuată în cadrul activităților lor legitime și cu garanții adecvate de către o fundație, o asociație sau orice alt organism fără scop lucrativ și cu specific politic, filozofic, religios sau sindical, cu condiția ca prelucrarea să se refere numai la membrii sau la foștii membri ai organismului respectiv sau la persoane cu care acesta are contacte permanente în

legătură cu scopurile sale și ca datele cu caracter personal să nu fie comunicate terților fără consimțământul persoanelor vizate;

e) prelucrarea se referă la date cu caracter personal care sunt făcute publice în mod manifest de către persoana vizată;

f) prelucrarea este necesară pentru constatarea, exercitarea sau apărarea unui drept în instanță sau ori de câte ori instanțele acționează în exercițiul funcției lor judiciare;

g) prelucrarea este necesară din motive de interes public major, în baza dreptului Uniunii sau a dreptului intern, care este proporțional cu obiectivul urmărit, respectă esența dreptului la protecția datelor și prevede măsuri corespunzătoare și specifice pentru protejarea drepturilor fundamentale și a intereselor persoanei vizate;

h) prelucrarea este necesară în scopuri legate de medicina preventivă sau a muncii, de evaluarea capacității de muncă a angajatului, de stabilirea unui diagnostic medical, de furnizarea de asistență medicală sau socială sau a unui tratament medical sau de gestionarea sistemelor și serviciilor de sănătate sau de asistență socială, în temeiul dreptului Uniunii sau al dreptului intern sau în temeiul unui contract încheiat cu un cadru medical și sub rezerva respectării condițiilor și garanțiilor prevăzute la alineatul (3);

i) prelucrarea este necesară din motive de interes public în domeniul sănătății publice, cum ar fi protecția împotriva amenințărilor transfrontaliere grave la adresa sănătății sau asigurarea de standarde ridicate de calitate și siguranță a asistenței medicale și a medicamentelor sau a dispozitivelor medicale, în temeiul dreptului Uniunii sau al dreptului intern, care prevede măsuri adecvate și specifice pentru protejarea drepturilor și libertăților persoanei vizate, în special a secretului profesional; sau

j) prelucrarea este necesară în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice, în baza dreptului Uniunii sau a dreptului intern, care este proporțional cu obiectivul urmărit, respectă esența dreptului la protecția datelor și prevede măsuri corespunzătoare și specifice pentru protejarea drepturilor fundamentale și a intereselor persoanei vizate.

(3) Datele cu caracter personal menționate la alineatul (1) pot fi prelucrate în scopurile menționate la alineatul (2) litera (h) în cazul în care datele respective sunt prelucrate de către un profesionist supus obligației de păstrare a secretului profesional sau sub responsabilitatea acestuia, în temeiul dreptului Uniunii sau al dreptului intern sau în temeiul normelor stabilite de organisme naționale competente sau de o altă persoană supusă, de asemenea, unei obligații de confidențialitate în temeiul dreptului Uniunii sau al dreptului intern ori al normelor stabilite de organisme naționale competente.

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

## **B. Prelucrarea datelor cu caracter personal având funcție de identificare**

### **Art. 17**

Prelucrarea codului numeric personal sau a altor date cu caracter personal având o funcție de identificare de aplicabilitate generală poate fi efectuată numai dacă:

- a) persoana vizată și-a dat în mod expres consimțământul;
- b) prelucrarea este prevăzută în mod expres de o dispoziție legală.

## **C. Prelucrarea datelor cu caracter personal privind starea de sănătate**

### **Art. 18**

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

- a) dacă prelucrarea este necesară pentru protecția sănătății publice;

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

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

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

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

##### **Art. 19**

Prelucrarea datelor cu caracter personal referitoare la săvârșirea de infracțiuni de către persoana vizată ori la condamnări penale, măsuri de siguranță sau sancțiuni administrative ori contravenționale, aplicate persoanei vizate, poate fi efectuată numai de către sau sub controlul unei autorități de stat sau atunci când prelucrarea este autorizată de dreptul Uniunii sau de dreptul intern care prevede garanții adecvate pentru drepturile și libertățile persoanelor vizate. Orice registru cuprinzător al condamnărilor penale se ține numai sub controlul unei autorități de stat.

##### **Art. 20**

(1) În cazul în care scopurile pentru care un operator prelucrează date cu caracter personal nu necesită sau nu mai necesită identificarea unei persoane vizate de către operator, operatorul nu are obligația de a păstra, obține sau prelucra informații suplimentare pentru a identifica persoana vizată în scopul unic al respectării prezentului regulament.

(2) Dacă, în cazurile menționate la alineatul (1), operatorul poate demonstra că nu este în măsură să identifice persoana vizată, operatorul informează persoana vizată în mod corespunzător, în cazul în care este posibil.

## **CAPITOLUL VI**

### **DREPTURILE PERSOANEI VIZATE ÎN CONTEXTUL PRELUCRĂRII DATELOR CU CARACTER PERSONAL**

#### **A. Transparență și modalități**

##### **Art. 21**

(1) Operatorul ia măsuri adecvate pentru a furniza persoanei vizate orice informații și orice comunicări referitoare la prelucrare, într-o formă concisă, transparentă, inteligibilă și ușor accesibilă, utilizând un limbaj clar și simplu, în special pentru orice informații adresate în mod specific unui copil. Informațiile se furnizează în scris sau prin alte mijloace, inclusiv, atunci când este oportun, în format electronic. La solicitarea persoanei vizate, informațiile pot fi furnizate verbal, cu condiția ca identitatea persoanei vizate să fie dovedită prin alte mijloace.

(2) Operatorul facilitează exercitarea drepturilor persoanei vizate. În cazurile menționate la articolul 16, operatorul nu refuză să dea curs cererii persoanei vizate de a-și exercita drepturile, cu excepția cazului în care operatorul demonstrează că nu este în măsură să identifice persoana vizată.

(3) Operatorul furnizează persoanei vizate informații privind acțiunile întreprinse în urma unei cereri, fără întârzieri nejustificate și în orice caz în cel mult o lună de la primirea cererii. Această perioadă poate fi prelungită cu două luni atunci când este necesar, ținându-se seama de complexitatea și numărul cererilor. Operatorul informează persoana vizată cu privire la orice astfel de prelungire, în termen de o lună de la primirea cererii, prezentând și motivele întârzierii. În cazul în care persoana vizată introduce o cerere în format electronic, informațiile sunt furnizate în format electronic acolo unde este posibil, cu excepția cazului în care persoana vizată solicită un alt format.

(4) Dacă nu ia măsuri cu privire la cererea persoanei vizate, operatorul informează persoana vizată, fără întârziere și în termen de cel mult o lună de la primirea cererii, cu privire la motivele pentru care nu ia măsuri și la posibilitatea de a depune o plângere în fața unei autorități de supraveghere și de a introduce o cale de atac judiciară.

(5) Informațiile furnizate și orice comunicare și orice măsuri luate sunt oferite gratuit. În cazul în care cererile din partea unei persoane vizate sunt în mod vădit nefondate sau excesive, în special din cauza caracterului lor repetitiv, operatorul poate:

a) fie să perceapă o taxă rezonabilă ținând cont de costurile administrative pentru furnizarea informațiilor sau a comunicării sau pentru luarea măsurilor solicitate;

b) fie să refuze să dea curs cererii. În aceste cazuri, operatorului îi revine sarcina de a demonstra caracterul vădit nefondat sau excesiv al cererii.

(6) În cazul în care are îndoieli întemeiate cu privire la identitatea persoanei fizice care înaintează cererea, operatorul poate solicita furnizarea de informații suplimentare necesare pentru a confirma identitatea persoanei vizate.

## **B. Informarea persoanei vizate**

### **Art. 22**

(1) La cerere, atunci când legea nu interzice, GPPME va comunica informații referitoare la: categoriile de date cu caracter personal pe care le prelucrează, sursele de la care au fost colectate datele cu caracter personal, scopurile prelucrării, precum și respectiv unui terț i-au fost dezvăluite aceste date.

(2) În cazul în care dezvăluirea datelor este impusă de lege (de exemplu, în vederea executării unei hotărâri judecătorești), GPPME se va asigura ca terțul care solicita dezvăluirea acționează în conformitate cu dispozițiile legale incidente, iar cererea privește numai datele cu caracter personal neexcesive prin raportare la scopul prelucrării. Persoana vizată va fi informată în legătură cu dezvăluirea, numai dacă legea permite.

### **Art. 23**

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

a) identitatea și datele de contact ale operatorului și, după caz, ale reprezentantului acestuia;

b) datele de contact ale responsabilului cu protecția datelor, după caz;

c) scopurile în care sunt prelucrate datele cu caracter personal, precum și temeiul juridic al prelucrării;

d) în cazul în care prelucrarea se face în temeiul articolului 6 alineatul (1) litera (f), interesele legitime urmărite de operator sau de o parte terță;

e) destinatarii sau categoriile de destinatari ai datelor cu caracter personal;

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

(2) În plus față de informațiile menționate la alineatul (1), în momentul în care datele cu caracter personal sunt obținute, operatorul furnizează persoanei vizate următoarele informații suplimentare necesare pentru a asigura o prelucrare echitabilă și transparentă:

- a) perioada pentru care vor fi stocate datele cu caracter personal sau, dacă acest lucru nu este posibil, criteriile utilizate pentru a stabili această perioadă;
  - b) existența dreptului de a solicita operatorului, în ceea ce privește datele cu caracter personal referitoare la persoana vizată, accesul la acestea, rectificarea sau ștergerea acestora sau restricționarea prelucrării sau a dreptului de a se opune prelucrării, precum și a dreptului la portabilitatea datelor;
  - c) atunci când prelucrarea se bazează pe articolul 6 alineatul (1) litera (a) sau pe articolul 9 alineatul (2) litera (a), existența dreptului de a retrage consimțământul în orice moment, fără a afecta legalitatea prelucrării efectuate pe baza consimțământului înainte de retragerea acestuia;
  - d) dreptul de a depune o plângere în fața unei autorități de supraveghere;
  - e) dacă furnizarea de date cu caracter personal reprezintă o obligație legală sau contractuală sau o obligație necesară pentru încheierea unui contract, precum și dacă persoana vizată este obligată să furnizeze aceste date cu caracter personal și care sunt eventualele consecințe ale nerespectării acestei obligații;
  - f) existența unui proces decizional automatizat incluzând crearea de profiluri, precum și informații pertinente privind logica utilizată și privind importanța și consecințele preconizate ale unei astfel de prelucrări pentru persoana vizată.
- (3) În cazul în care operatorul intenționează să prelucrez ulterior datele cu caracter personal într-un alt scop decât cel pentru care acestea au fost colectate, operatorul furnizează persoanei vizate, înainte de această prelucrare ulterioară, informații privind scopul secundar respectiv și orice informații suplimentare relevante, în conformitate cu alineatul (2).
- (4) Alineatele (1), (2) și (3) nu se aplică dacă și în măsura în care persoana vizată deține deja informațiile respective.

#### **Art. 24**

(1) În cazul în care datele cu caracter personal nu au fost obținute de la persoana vizată, operatorul furnizează persoanei vizate următoarele informații:

- a) identitatea și datele de contact ale operatorului și, după caz, ale reprezentantului acestuia;
- b) datele de contact ale responsabilului cu protecția datelor, după caz;
- c) scopurile în care sunt prelucrate datele cu caracter personal, precum și temeiul juridic al prelucrării;
- d) categoriile de date cu caracter personal vizate;
- e) destinatarii sau categoriile de destinatari ai datelor cu caracter personal, după caz;

(2) Pe lângă informațiile menționate la alineatul (1), operatorul furnizează persoanei vizate următoarele informații necesare pentru a asigura o prelucrare echitabilă și transparentă în ceea ce privește persoana vizată:

- a) perioada pentru care vor fi stocate datele cu caracter personal sau, dacă acest lucru nu este posibil, criteriile utilizate pentru a stabili această perioadă;
- b) în cazul în care prelucrarea se face în temeiul articolului 6 alineatul (1) litera (f), interesele legitime urmărite de operator sau de o parte terță;
- c) existența dreptului de a solicita operatorului, în ceea ce privește datele cu caracter personal referitoare la persoana vizată, accesul la acestea, rectificarea sau ștergerea acestora sau restricționarea prelucrării și a dreptului de a se opune prelucrării, precum și a dreptului la portabilitatea datelor;
- d) atunci când prelucrarea se bazează pe articolul 6 alineatul (1) litera (a) sau pe articolul 9 alineatul (2) litera (a), existența dreptului de a retrage consimțământul în orice moment, fără a afecta legalitatea prelucrării efectuate pe baza consimțământului înainte de retragerea acestuia;
- e) dreptul de a depune o plângere în fața unei autorități de supraveghere;
- f) sursa din care provin datele cu caracter personal și, dacă este cazul, dacă acestea provin din surse disponibile public.

- (3) Operatorul furnizează informațiile menționate la alineatele (1) și (2):
- a) într-un termen rezonabil după obținerea datelor cu caracter personal, dar nu mai mare de o lună, ținându-se seama de circumstanțele specifice în care sunt prelucrate datele cu caracter personal;
  - b) dacă datele cu caracter personal urmează să fie utilizate pentru comunicarea cu persoana vizată, cel târziu în momentul primei comunicări către persoana vizată respectivă; sau
  - c) dacă se intenționează divulgarea datelor cu caracter personal către un alt destinatar, cel mai târziu la data la care acestea sunt divulgate pentru prima oară.
- (4) În cazul în care operatorul intenționează să prelucrez ulterior datele cu caracter personal într-un alt scop decât cel pentru care acestea au fost obținute, operatorul furnizează persoanei vizate, înainte de această prelucrare ulterioară, informații privind scopul secundar respectiv și orice informații suplimentare relevante, în conformitate cu alineatul (2).
- (5) Alineatele (1)-(4) nu se aplică dacă și în măsura în care:
- a) persoana vizată deține deja informațiile;
  - b) furnizarea acestor informații se dovedește a fi imposibilă sau ar implica eforturi disproporționate, în special în cazul prelucrării în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice, sau în măsura în care obligația menționată la alineatul (1) din prezentul articol este susceptibil să facă imposibilă sau să afecteze în mod grav realizarea obiectivelor prelucrării respective. În astfel de cazuri, operatorul ia măsuri adecvate pentru a proteja drepturile, libertățile și interesele legitime ale persoanei vizate, inclusiv punerea informațiilor la dispoziția publicului;
  - c) obținerea sau divulgarea datelor este prevăzută în mod expres de dreptul Uniunii sau de dreptul intern sub incidența căruia intră operatorul și care prevede măsuri adecvate pentru a proteja interesele legitime ale persoanei vizate; sau
  - d) în cazul în care datele cu caracter personal trebuie să rămână confidențiale în temeiul unei obligații statutare de secret profesional reglementate de dreptul Uniunii sau de dreptul intern, inclusiv al unei obligații legale de a păstra secretul.

### **C. Dreptul de acces la date**

#### **Art.25**

- (1) Persoana vizată are dreptul de a obține din partea operatorului o confirmare că se prelucrez sau nu date cu caracter personal care o privesc și, în caz afirmativ, acces la datele respective și la următoarele informații:
- a) scopurile prelucrării;
  - b) categoriile de date cu caracter personal vizate;
  - c) destinatarii sau categoriile de destinatari cărora datele cu caracter personal le-au fost sau urmează să le fie divulgate, în special destinatari din țări terțe sau organizații internaționale;
  - d) acolo unde este posibil, perioada pentru care se preconizează că vor fi stocate datele cu caracter personal sau, dacă acest lucru nu este posibil, criteriile utilizate pentru a stabili această perioadă;
  - e) existența dreptului de a solicita operatorului rectificarea sau ștergerea datelor cu caracter personal ori restricționarea prelucrării datelor cu caracter personal referitoare la persoana vizată sau a dreptului de a se opune prelucrării;
  - f) dreptul de a depune o plângere în fața unei autorități de supraveghere;
  - g) în cazul în care datele cu caracter personal nu sunt colectate de la persoana vizată, orice informații disponibile privind sursa acestora;
  - h) existența unui proces decizional automatizat incluzând crearea de profiluri, precum și, cel puțin în cazurile respective, informații pertinente privind logica utilizată și privind importanța și consecințele preconizate ale unei astfel de prelucrări pentru persoana vizată.

(2) În cazul în care datele cu caracter personal sunt transferate către o țară terță sau o organizație internațională, persoana vizată are dreptul să fie informată cu privire la garanțiile adecvate referitoare la transfer.

(3) Operatorul furnizează o copie a datelor cu caracter personal care fac obiectul prelucrării. Pentru orice alte copii solicitate de persoana vizată, operatorul poate percepe o taxă rezonabilă, bazată pe costurile administrative. În cazul în care persoana vizată introduce cererea în format electronic și cu excepția cazului în care persoana vizată solicită un alt format, informațiile sunt furnizate într-un format electronic utilizat în mod curent.

(4) Dreptul de a obține o copie menționată la alineatul (3) nu aduce atingere drepturilor și libertăților altora.

(5) Persoana vizată poate solicita de la operator informațiile prevăzute la alin. (1), printr-o cerere întocmită în formă scrisă, datată și semnată. În cerere solicitantul poate arăta dacă dorește ca informațiile să îi fie comunicate la o anumită adresă, care poate fi și de poștă electronică, sau printr-un serviciu de corespondență care să asigure că predarea i se va face numai personal.

(6) Operatorul este obligat să comunice informațiile solicitate, în termen de 15 zile de la data primirii cererii, cu respectarea eventualei opțiuni a solicitantului exprimate potrivit alin (5).

(7) În cazul datelor cu caracter personal legate de starea de sănătate, cererea prevăzută la alin. (5) poate fi introdusă de persoana vizată fie direct, fie prin intermediul unui cadru medical care va indica în cerere persoana în numele căreia este introdusă. La cererea operatorului sau a persoanei vizate comunicarea prevăzută la alin. (6) poate fi făcută prin intermediul unui cadru medical desemnat de persoana vizată.

(8) În cazul în care datele cu caracter personal legate de starea de sănătate sunt prelucrate în scop de cercetare științifică, dacă nu există, cel puțin aparent, riscul de a se aduce atingere drepturilor persoanei vizate și dacă datele nu sunt utilizate pentru a lua decizii sau măsuri față de o anumită persoană, comunicarea prevăzută la alin. (6) se poate face și într-un termen mai mare decât cel prevăzut la acel alineat, în măsura în care aceasta ar putea afecta bunul mers sau rezultatele cercetării dar nu mai târziu de momentul în care cercetarea este încheiată. În acest caz persoana vizată trebuie să își fi dat în mod expres și neechivoc consimțământul ca datele să fie prelucrate în scop de cercetare științifică, precum și asupra posibilei amânări a comunicării prevăzute la alin. (6) din acest motiv.

(9) Prevederile alin. (5) nu se aplică atunci când prelucrarea datelor se efectuează exclusiv în scopuri jurnalistice, literare sau artistice, dacă aplicarea acestora ar da indicii asupra surselor de informare.

#### **Art.26**

(1) Persoanele vizate au dreptul să se informeze cu privire la datele personale proprii deținute de GPPME, utilizând în acest scop diverse căi de comunicare (email, fax, cerere scrisă).

(2) O persoană vizată nu are dreptul de a accesa datele cu caracter personal ale altei persoane vizate.

### **D. Dreptul la rectificare**

#### **Art. 27**

Persoana vizată are dreptul de a obține de la operator, fără întârzieri nejustificate, rectificarea datelor cu caracter personal inexacte care o privesc. Ținându-se seama de scopurile în care au fost prelucrate datele, persoana vizată are dreptul de a obține completarea datelor cu caracter personal care sunt incomplete, inclusiv prin furnizarea unei declarații suplimentare.

#### **Art. 28**

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

(2) GPPME va păstra o evidență a contestațiilor privind caracterul exact sau complet al datelor, precum și o evidență a datelor transferate către alți operatori. Evidențele vor conține datele care au fost rectificate și datele care au fost transferate.

(3) Actualizarea bazelor de date se face prin intermediul informațiilor transmise de persoanele vizate, precum și prin informațiile furnizate de orice sursă externă autorizată de lege.

## **E. Dreptul la ștergerea datelor ("dreptul de a fi uitat")**

### **Art. 28**

(1) Persoana vizată are dreptul de a obține din partea operatorului ștergerea datelor cu caracter personal care o privesc, fără întârzieri nejustificate, iar operatorul are obligația de a șterge datele cu caracter personal fără întârzieri nejustificate în cazul în care se aplică unul dintre următoarele motive:

- a) datele cu caracter personal nu mai sunt necesare pentru îndeplinirea scopurilor pentru care au fost colectate sau prelucrate;
- b) persoana vizată își retrage consimțământul pe baza căruia are loc prelucrarea, în conformitate cu articolul 6 alineatul (1) litera (a) sau cu articolul 9 alineatul (2) litera (a), și nu există niciun alt temei juridic pentru prelucrarea;
- c) persoana vizată se opune prelucrării și nu există motive legitime care să prevaleze în ceea ce privește prelucrarea;
- d) datele cu caracter personal au fost prelucrate ilegal;
- e) datele cu caracter personal trebuie șterse pentru respectarea unei obligații legale care revine operatorului în temeiul dreptului Uniunii sau al dreptului intern sub incidența căruia se află operatorul;

(2) În cazul în care operatorul a făcut publice datele cu caracter personal și este obligat, în temeiul alineatului (1), să le șteargă, operatorul, ținând seama de tehnologia disponibilă și de costul implementării, ia măsuri rezonabile, inclusiv măsuri tehnice, pentru a informa operatorii care prelucrează datele cu caracter personal că persoana vizată a solicitat ștergerea de către acești operatori a oricăror linkuri către datele respective sau a oricăror copii sau reproduceri ale acestor date cu caracter personal.

(3) Alineatele (1) și (2) nu se aplică în măsura în care prelucrarea este necesară:

- a) pentru exercitarea dreptului la liberă exprimare și la informare;
- b) pentru respectarea unei obligații legale care prevede prelucrarea în temeiul dreptului Uniunii sau al dreptului intern care se aplică operatorului sau pentru îndeplinirea unei sarcini executate în interes public sau în cadrul exercitării unei autorități oficiale cu care este investit operatorul;
- c) din motive de interes public în domeniul sănătății publice;
- d) în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice, în măsura în care dreptul menționat la alineatul (1) este susceptibil să facă imposibilă sau să afecteze în mod grav realizarea obiectivelor prelucrării respective; sau
- e) pentru constatarea, exercitarea sau apărarea unui drept în instanță.

(4) Pentru exercitarea dreptului prevăzut la alin. (1) persoana vizată va înainta operatorului o cerere întocmită în formă scrisă, datată și semnată. În cerere solicitantul poate arăta dacă dorește ca informațiile să îi fie comunicate la o anumită adresă, care poate fi și de poștă electronică, sau printr-un serviciu de corespondență care să asigure că predarea i se va face numai personal.

(5) Operatorul este obligat să comunice măsurile luate în temeiul alin. (1), precum și, dacă este cazul, numele terțului căruia i-au fost dezvăluite datele cu caracter personal referitoare la persoana vizată, în termen de 15 zile de la data primirii cererii, cu respectarea eventualei opțiuni a solicitantului exprimate potrivit alin. (4).



## F. Dreptul la restricționarea prelucrării

### Art. 29

(1) Persoana vizată are dreptul de a obține din partea operatorului restricționarea prelucrării în cazul în care se aplică unul din următoarele cazuri:

- a) persoana vizată contestă exactitatea datelor, pentru o perioadă care îi permite operatorului să verifice exactitatea datelor;
- b) prelucrarea este ilegală, iar persoana vizată se opune ștergerii datelor cu caracter personal, solicitând în schimb restricționarea utilizării lor;
- c) operatorul nu mai are nevoie de datele cu caracter personal în scopul prelucrării, dar persoana vizată i le solicită pentru constatarea, exercitarea sau apărarea unui drept în instanță; sau
- d) persoana vizată s-a opus prelucrării, pentru intervalul de timp în care se verifică dacă drepturile legitime ale operatorului prevalează asupra celor ale persoanei vizate.

(2) În cazul în care prelucrarea a fost restricționată în temeiul alineatului (1), astfel de date cu caracter personal pot, cu excepția stocării, să fie prelucrate numai cu consimțământul persoanei vizate sau pentru constatarea, exercitarea sau apărarea unui drept în instanță sau pentru protecția drepturilor unei alte persoane fizice sau juridice sau din motive de interes public important al Uniunii sau al unui stat membru.

(3) O persoană vizată care a obținut restricționarea prelucrării în temeiul alineatului (1) este informată de către operator înainte de ridicarea restricției de prelucrare.

### Art. 30

Operatorul comunică fiecărui destinatar căruia i-au fost divulgate datele cu caracter personal orice rectificare sau ștergere a datelor cu caracter personal sau restricționare a prelucrării efectuate, cu excepția cazului în care acest lucru se dovedește imposibil sau presupune eforturi disproporționate. Operatorul informează persoana vizată cu privire la destinatarii respectivi dacă persoana vizată solicită acest lucru.

## G. Dreptul la portabilitatea datelor

### Art. 31

(1) Persoana vizată are dreptul de a primi datele cu caracter personal care o privesc și pe care le-a furnizat operatorului într-un format structurat, utilizat în mod curent și care poate fi citit automat și are dreptul de a transmite aceste date altui operator, fără obstacole din partea operatorului căruia i-au fost furnizate datele cu caracter personal, în cazul în care:

- a) prelucrarea se bazează pe consimțământ în temeiul articolului 6 alineatul (1) litera (a) sau al articolului 9 alineatul (2) litera (a) sau pe un contract în temeiul articolului 6 alineatul (1) litera (b); și
- b) prelucrarea este efectuată prin mijloace automate.

(2) În exercitarea dreptului său la portabilitatea datelor în temeiul alineatului (1), persoana vizată are dreptul ca datele cu caracter personal să fie transmise direct de la un operator la altul acolo unde acest lucru este fezabil din punct de vedere tehnic.

(3) Exercitarea dreptului menționat la alineatul (1) nu aduce atingere articolului 20. Respectivul drept nu se aplică prelucrării necesare pentru îndeplinirea unei sarcini executate în interes public sau în cadrul exercitării unei autorități oficiale cu care este investit operatorul.

(4) Dreptul menționat la alineatul (1) nu aduce atingere drepturilor și libertăților altora.

## H. Dreptul de opoziție

### Art. 32

(1) În orice moment, persoana vizată are dreptul să se opună, din motive legate de situația particulară în care se află, prelucrării în temeiul articolului 6 alineatul (1) litera (e) sau (f), a datelor cu caracter personal care o privesc, inclusiv creării de profiluri pe baza respectivelor dispoziții. Operatorul nu mai prelucrează datele cu caracter personal, cu excepția cazului în care operatorul demonstrează că are motive legitime și imperioase care justifică prelucrarea și care prevalează asupra intereselor, drepturilor și libertăților persoanei vizate sau că scopul este constatarea, exercitarea sau apărarea unui drept în instanță.

(2) Atunci când prelucrarea datelor cu caracter personal are drept scop marketingul direct, persoana vizată are dreptul de a se opune în orice moment prelucrării în acest scop a datelor cu caracter personal care o privesc, inclusiv creării de profiluri, în măsura în care este legată de marketingul direct respectiv.

(3) În cazul în care persoana vizată se opune prelucrării în scopul marketingului direct, datele cu caracter personal nu mai sunt prelucrate în acest scop.

(4) Cel târziu în momentul primei comunicări cu persoana vizată, dreptul menționat la alineatele (1) și (2) este adus în mod explicit în atenția persoanei vizate și este prezentat în mod clar și separat de orice alte informații.

(5) În contextual utilizării serviciilor societății informaționale și în pofida Directivei 2002/58/CE, persoana vizată își poate exercita dreptul de a se opune prin mijloace automate care utilizează specificații tehnice.

(6) În cazul în care datele cu caracter personal sunt prelucrate în scopuri de cercetare științifică sau istorică sau în scopuri statistice, persoana vizată, din motive legate de situația sa particulară, are dreptul de a se opune prelucrării datelor cu caracter personal care o privesc, cu excepția cazului în care prelucrarea este necesară pentru îndeplinirea unei sarcini din motive de interes public.

(7) Persoana vizată va înainta operatorului o cerere întocmită în formă scrisă, datată și semnată. În cerere solicitantul poate arăta dacă dorește ca informațiile să îi fie comunicate la o anumită adresă, care poate fi și de poștă electronică, sau printr-un serviciu de corespondență care să asigure că predarea i se va face numai personal.

(8) Operatorul este obligat să comunice persoanei vizate măsurile luate, precum și, dacă este cazul, numele terțului căruia i-au fost dezvăluite datele cu caracter personal referitoare la persoana vizată, în termen de 15 zile de la data primirii cererii, cu respectarea eventualei opțiuni a solicitantului exprimate potrivit alin. (7).

## I. Procesul decizional individual automatizat, inclusiv crearea de profiluri

### Art. 33

(1) Persoana vizată are dreptul de a nu face obiectul unei decizii bazate exclusiv pe prelucrarea automată, inclusiv crearea de profiluri, care produce efecte juridice care privesc persoana vizată sau o afectează în mod similar într-o măsură semnificativă.

(2) Alineatul (1) nu se aplică în cazul în care decizia:

a) este necesară pentru încheierea sau executarea unui contract între persoana vizată și un operator de date;

b) este autorizată prin dreptul Uniunii sau dreptul intern care se aplică operatorului și care prevede, de asemenea, măsuri corespunzătoare pentru protejarea drepturilor, libertăților și intereselor legitime ale persoanei vizate; sau

c) are la bază consimțământul explicit al persoanei vizate.

(3) În cazurile menționate la alineatul (2) literele (a) și (c), operatorul de date pune în aplicare măsuri corespunzătoare pentru protejarea drepturilor, libertăților și intereselor

legitime ale persoanei vizate, cel puțin dreptul acesteia de a obține intervenție umană din partea operatorului, de a-și exprima punctul de vedere și de a contesta decizia.

(4) Deciziile menționate la alineatul (2) nu au la bază categoriile speciale de date cu caracter personal menționate la articolul 9 alineatul (1), cu excepția cazului în care se aplică articolul 9 alineatul (2) litera (a) sau (g) și în care au fost instituite măsuri corespunzătoare pentru protejarea drepturilor, libertăților și intereselor legitime ale persoanei vizate

## **J. Dreptul de a nu fi supus unei decizii individuale**

### **Art. 34**

(1) Orice persoană are dreptul de a cere și de a obține:

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

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

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

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

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

## **K. Restricții**

### **Art. 35**

(1) Dreptul Uniunii sau dreptul intern care se aplică operatorului de date poate restricționa printr-o măsură legislativă domeniul de aplicare al obligațiilor și al drepturilor prevăzute atunci când o astfel de restricție respectă esența drepturilor și libertăților fundamentale și constituie o măsură necesară și proporțională într-o societate democratică, pentru a asigura:

a) securitatea națională;

b) apărarea;

c) securitatea publică;

d) prevenirea, investigarea, depistarea sau urmărirea penală a infracțiunilor sau executarea sancțiunilor penale, inclusiv protejarea împotriva amenințărilor la adresa securității publice și prevenirea acestora;

e) alte obiective importante de interes public general ale Uniunii sau ale unui stat membru, în special un interes economic sau financiar important al Uniunii sau al unui stat membru, inclusiv în domeniile monetar, bugetar și fiscal și în domeniul sănătății publice și al securității sociale;

f) protejarea independenței judiciare și a procedurilor judiciare;

g) prevenirea, investigarea, depistarea și urmărirea penală a încălcării eticii în cazul profesiilor reglementate;

h) funcția de monitorizare, inspectare sau reglementare legată, chiar și ocazional, de exercitarea autorității oficiale în cazurile menționate la literele (a)-(e) și (g);

i) protecția persoanei vizate sau a drepturilor și libertăților altora;

j) punerea în aplicare a pretențiilor de drept civil.

(2) În special, orice măsură legislativă menționată la alineatul (1) conține dispoziții specifice cel puțin, dacă este cazul, în ceea ce privește:

- a) scopurile prelucrării sau ale categoriilor de prelucrare;
- b) categoriile de date cu caracter personal;
- c) domeniul de aplicare al restricțiilor introduse;
- d) garanțiile pentru a preveni abuzurile sau accesul sau transferul ilegal;
- e) menționarea operatorului sau a categoriilor de operatori;
- f) perioadele de stocare și garanțiile aplicabile având în vedere natura, domeniul de aplicare și scopurile prelucrării sau ale categoriilor de prelucrare;
- g) riscurile pentru drepturile și libertăților persoanelor vizate; și
- h) dreptul persoanelor vizate de a fi informate cu privire la restricție, cu excepția cazului în care acest lucru poate aduce atingere scopului restricției.

## **CAPITOLUL VII**

### **CONFIDENȚIALITATEA ȘI SECURITATEA PRELUCRĂRILOR**

#### **A. Confidențialitatea prelucrărilor**

##### **Art. 36**

Orice persoană care acționează sub autoritatea operatorului, care are acces la date cu caracter personal, nu poate să le prelucreze decât pe baza instrucțiunilor operatorului, cu excepția cazului în care acționează în temeiul unei obligații legale.

##### **Art. 37**

(1) Ținând seama de natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și de riscurile cu grade diferite de probabilitate și gravitate pentru drepturile și libertățile persoanelor fizice, operatorul pune în aplicare măsuri tehnice și organizatorice adecvate pentru a garanta și a fi în măsură să demonstreze că prelucrarea se efectuează în conformitate cu prezentul regulament. Respectivul măsuri se revizuiesc și se actualizează dacă este necesar.

(2) Atunci când sunt proporționale în raport cu operațiunile de prelucrare, măsurile menționate la alineatul (1) includ punerea în aplicare de către operator a unor politici adecvate de protecție a datelor.

(3) Aderarea la un cod de conduită aprobat sau la un mecanism de certificare aprobat poate fi utilizată ca element care să demonstreze respectarea obligațiilor de către operator.

##### **Art. 38**

(1) Având în vedere stadiul actual al tehnologiei, costurile implementării, și natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și riscurile cu grade diferite de probabilitate și gravitate pentru drepturile și libertățile persoanelor fizice pe care le prezintă prelucrarea, operatorul, atât în momentul stabilirii mijloacelor de prelucrare, cât și în cel al prelucrării în sine, pune în aplicare măsuri tehnice și organizatorice adecvate, cum ar fi pseudonimizarea, care sunt destinate să pună în aplicare în mod eficient principiile de protecție a datelor, precum reducerea la minimum a datelor, și să integreze garanțiile necesare în cadrul prelucrării, pentru a îndeplini cerințele prezentului regulament și a proteja drepturile persoanelor vizate.

(2) Operatorul pune în aplicare măsuri tehnice și organizatorice adecvate pentru a asigura că, în mod implicit, sunt prelucrate numai date cu caracter personal care sunt necesare pentru fiecare scop specific al prelucrării. Respectiva obligație se aplică volumului de date colectate, gradului de prelucrare a acestora, perioadei lor de stocare și accesibilității lor. În special, astfel de măsuri asigură că, în mod implicit, datele cu caracter personal nu pot fi accesate, fără intervenția persoanei, de un număr nelimitat de persoane.

### **Art. 39**

(1) GPPME păstrează o evidență a activităților de prelucrare desfășurate sub responsabilitatea sa. Respectiva evidență cuprinde toate următoarele informații:

- a) numele și datele de contact ale operatorului și, după caz, ale responsabilului cu protecția datelor;
- b) scopurile prelucrării;
- c) o descriere a categoriilor de persoane vizate și a categoriilor de date cu caracter personal;
- d) categoriile de destinatari cărora le-au fost sau le vor fi divulgate datele cu caracter personal, inclusiv destinatarii din țări terțe sau organizații internaționale;
- e) acolo unde este posibil, termenele-limită preconizate pentru ștergerea diferitelor categorii de date;
- f) acolo unde este posibil, o descriere generală a măsurilor tehnice și organizatorice de securitate.

(2) Evidența menționată la alineatul (1) se formulează în scris, inclusiv în format electronic.

(4) Operatorul pune evidența la dispoziția autorității de supraveghere, la cererea acesteia.

(5) Obligația menționată la alineatul 1 nu se aplică unei întreprinderi sau organizații cu mai puțin de 250 de angajați, cu excepția cazului în care prelucrarea pe care o efectuează este susceptibilă să genereze un risc pentru drepturile și libertățile persoanelor vizate, prelucrarea nu este ocazională sau prelucrarea include categorii speciale de date, astfel cum se prevede la articolul 9 alineatul (1), sau date cu caracter personal referitoare la condamnări penale și infracțiuni.

### **Art. 40**

Operatorul cooperează, la cerere, cu autoritatea de supraveghere în îndeplinirea sarcinilor acesteia.

## **C. Securitatea prelucrărilor**

### **Art. 41**

(1) 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 și persoana împuternicită de acesta implementează măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător acestui risc, incluzând printre altele, după caz:

- a) pseudonimizarea și criptarea datelor cu caracter personal;
- b) capacitatea de a asigura confidențialitatea, integritatea, disponibilitatea și rezistența continue ale sistemelor și serviciilor de prelucrare;
- c) 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;
- d) un proces pentru testarea, evaluarea și aprecierea periodice ale eficacității măsurilor tehnice și organizatorice pentru a garanta securitatea prelucrării.

(2) La evaluarea nivelului adecvat de securitate, se ține seama în special de riscurile prezentate de prelucrare, generate în special, în mod accidental sau ilegal, de distrugerea, pierderea, modificarea, divulgarea neautorizată sau accesul neautorizat la datele cu caracter personal transmise, stocate sau prelucrate într-un alt mod.

(3) Aderarea la un cod de conduită aprobat sau la un mecanism de certificare aprobat poate fi utilizată ca element prin care să se demonstreze îndeplinirea cerințelor prevăzute la alineatul (1) din prezentul articol.

(4) Operatorul ia măsuri pentru a asigura faptul că orice persoană fizică care acționează sub autoritatea operatorului și care are acces la date cu caracter personal nu le prelucrează decât

la cererea operatorului, cu excepția cazului în care această obligație îi revine în temeiul dreptului Uniunii sau al dreptului intern.

## **CAPITOLUL VIII**

### **NOTIFICAREA CĂTRE AUTORITATEA DE SUPRAVEGHERE**

#### **A. Notificarea autorității de supraveghere în cazul încălcării securității datelor cu caracter personal**

##### **Art. 42**

(1) În cazul în care are loc o încălcare a securității datelor cu caracter personal, operatorul notifică acest lucru autorității de supraveghere competente, fără întârzieri nejustificate și, dacă este posibil, în termen de cel mult 72 de ore de la data la care a luat cunoștință de aceasta, cu excepția cazului în care este puțin probabil să genereze un risc pentru drepturile și libertățile persoanelor fizice. În cazul în care notificarea către autoritatea de supraveghere nu are loc în termen de 72 de ore, aceasta este însoțită de o explicație motivată pentru întârziere.

(2) Notificarea menționată la alineatul (1) cel puțin:

- a) descrie caracterul încălcării securității datelor cu caracter personal, inclusiv, acolo unde este posibil, categoriile și numărul aproximativ al persoanelor vizate în cauză, precum și categoriile și numărul aproximativ al înregistrărilor de date cu caracter personal în cauză;
- b) comunică numele și datele de contact ale responsabilului cu protecția datelor sau un alt punct de contact de unde se pot obține mai multe informații;
- c) descrie consecințele probabile ale încălcării securității datelor cu caracter personal;
- d) descrie măsurile luate sau propuse spre a fi luate de operator pentru a remedia problema încălcării securității datelor cu caracter personal, inclusiv, după caz, măsurile pentru atenuarea eventualelor sale efecte negative.

(3) Atunci când și în măsura în care nu este posibil să se furnizeze informațiile în același timp, acestea pot fi furnizate în mai multe etape, fără întârzieri nejustificate.

(4) Operatorul păstrează documente referitoare la toate cazurile de încălcare a securității datelor cu caracter personal, care cuprind o descriere a situației de fapt în care a avut loc încălcarea securității datelor cu caracter personal, a efectelor acesteia și a măsurilor de remediere întreprinse. Această documentație permite autorității de supraveghere să verifice conformitatea cu prezentul articol.

#### **B. Informarea persoanei vizate cu privire la încălcarea securității datelor cu caracter personal**

##### **Art. 43**

(1) În cazul în care încălcarea securității datelor cu caracter personal este susceptibilă să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice, operatorul informează persoana vizată fără întârzieri nejustificate cu privire la această încălcare.

(2) În informarea transmisă persoanei vizate prevăzută la alineatul (1) din prezentul articol se include o descriere într-un limbaj clar și simplu a caracterului încălcării securității datelor cu caracter personal, precum și cel puțin informațiile și măsurile menționate la articolul 42 alineatul (2) literele (b), (c) și (d).

(3) Informarea persoanei vizate menționată la alineatul (1) nu este necesară în cazul în care oricare dintre următoarele condiții este îndeplinită:

- a) operatorul a implementat măsuri de protecție tehnice și organizatorice adecvate, iar aceste măsuri au fost aplicate în cazul datelor cu caracter personal afectate de încălcarea securității datelor cu caracter personal, în special măsuri prin care se asigură că datele cu caracter personal devin neinteligibile oricărei persoane care nu este autorizată să le acceseze, cum ar fi criptarea;

b) operatorul a luat măsuri ulterioare prin care se asigură că riscul ridicat pentru drepturile și libertățile persoanelor vizate menționat la alineatul (1) nu mai este susceptibil să se materializeze;

c) ar necesita un efort disproporționat. În această situație, se efectuează în loc o informare publică sau se ia o măsură similară prin care persoanele vizate sunt informate într-un mod la fel de eficace.

(4) În cazul în care operatorul nu a comunicat deja încălcarea securității datelor cu caracter personal către persoana vizată, autoritatea de supraveghere, după ce a luat în considerare probabilitatea ca încălcarea securității datelor cu caracter personal să genereze un risc ridicat, poate să îi solicite acestuia să facă acest lucru sau poate decide că oricare dintre condițiile menționate la alineatul (3) sunt îndeplinite.

### C. Evaluarea impactului asupra protecției datelor

#### Art. 44

(1) Având în vedere natura, domeniul de aplicare, contextul și scopurile prelucrării, în cazul în care un tip de prelucrare, în special cel bazat pe utilizarea noilor tehnologii, este susceptibil să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice, operatorul efectuează, înaintea prelucrării, o evaluare a impactului operațiunilor de prelucrare prevăzute asupra protecției datelor cu caracter personal. O evaluare unică poate aborda un set de operațiuni de prelucrare similare care prezintă riscuri ridicate similare.

(2) La realizarea unei evaluări a impactului asupra protecției datelor, operatorul solicită avizul responsabilului cu protecția datelor, dacă acesta a fost desemnat.

(3) Evaluarea impactului asupra protecției datelor menționată la alineatul (1) se impune mai ales în cazul:

a) unei evaluări sistematice și cuprinzătoare a aspectelor personale referitoare la persoane fizice, care se bazează pe prelucrarea automată, inclusiv crearea de profiluri, și care stă la baza unor decizii care produc efecte juridice privind persoana fizică sau care o afectează în mod similar într-o măsură semnificativă;

b) prelucrării pe scară largă a unor categorii speciale de date, sau a unor date cu caracter personal privind condamnări penale și infracțiuni; sau

c) unei monitorizări sistematice pe scară largă a unei zone accesibile publicului.

(4) Evaluarea conține cel puțin:

a) o descriere sistematică a operațiunilor de prelucrare preconizate și a scopurilor prelucrării, inclusiv, după caz, interesul legitim urmărit de operator;

b) o evaluare a necesității și proporționalității operațiunilor de prelucrare în legătură cu aceste scopuri;

c) o evaluare a riscurilor pentru drepturile și libertățile persoanelor vizate menționate la alineatul (1); și

d) măsurile preconizate în vederea abordării riscurilor, inclusiv garanțiile, măsurile de securitate și mecanismele menite să asigure protecția datelor cu caracter personal și să demonstreze conformitatea cu dispozițiile prezentului regulament, luând în considerare drepturile și interesele legitime ale persoanelor vizate și ale altor persoane interesate.

(5) La evaluarea impactului operațiunilor de prelucrare efectuate de operator se are în vedere în mod corespunzător respectarea de către operator a codului de conduită aprobat, în special în vederea unei evaluări a impactului asupra protecției datelor.

(6) Operatorul solicită, acolo unde este cazul, avizul persoanelor vizate sau al reprezentanților acestora privind prelucrarea prevăzută, fără a aduce atingere protecției intereselor comerciale sau publice ori securității operațiunilor de prelucrare.

(7) Atunci când prelucrarea în temeiul articolului 6 alineatul (1) litera (c) sau (e) are un temei juridic în dreptul Uniunii sau al unui stat membru sub incidența căruia intră operatorul, iar

dreptul respectiv reglementează operațiunea de prelucrare specifică sau setul de operațiuni specifice în cauză și deja s-a efectuat o evaluare a impactului asupra protecției datelor ca parte a unei evaluări a impactului general în contextul adoptării respectivului temei juridic, alineatele (1)-(6) nu se aplică, cu excepția cazului în care statele membre consideră că este necesară efectuarea unei astfel de evaluări înaintea desfășurării activităților de prelucrare.

(8) Acolo unde este necesar, operatorul efectuează o analiză pentru a evalua dacă prelucrarea are loc în conformitate cu evaluarea impactului asupra protecției datelor, cel puțin atunci când are loc o modificare a riscului reprezentat de operațiunile de prelucrare.

#### **D. Consultarea prealabilă**

##### **Art. 45**

(1) Operatorul consultă autoritatea de supraveghere înainte de prelucrare atunci când evaluarea impactului asupra protecției datelor indică faptul că prelucrarea ar genera un risc ridicat în absența unor măsuri luate de operator pentru atenuarea riscului.

(2) Atunci când consideră că prelucrarea ar încălca prezentul regulament, în special atunci când riscul nu a fost identificat sau atenuat într-o măsură suficientă de către operator, autoritatea de supraveghere oferă consiliere în scris operatorului, în cel mult opt săptămâni de la primirea cererii de consultare. Această perioadă poate fi prelungită cu șase săptămâni, ținându-se seama de complexitatea prelucrării prevăzute. Autoritatea de supraveghere informează operatorul, în termen de o lună de la primirea cererii, cu privire la orice astfel de prelungire, prezentând motivele întârzierii. Aceste perioade pot fi suspendate până când autoritatea de supraveghere a obținut informațiile pe care le-a solicitat în scopul consultării.

(3) Atunci când consultă autoritatea de supraveghere, operatorul îi furnizează acesteia:

- a) dacă este cazul, responsabilitățile respective ale operatorului în activitățile de prelucrare;
- b) scopurile și mijloacele prelucrării preconizate;
- c) măsurile și garanțiile prevăzute pentru protecția drepturilor și libertăților persoanelor vizate, în conformitate cu prezentul regulament;
- d) dacă este cazul, datele de contact ale responsabilului cu protecția datelor;
- e) evaluarea impactului asupra protecției datelor; și
- f) orice alte informații solicitate de autoritatea de supraveghere.

##### **Art. 46**

(1) Operatorul este obligat să notifice autorității de supraveghere înainte de efectuarea oricărei prelucrări ori a oricărui ansamblu de prelucrări având același scop sau scopuri corelate. Notificarea nu este necesară în cazul în care prelucrarea are ca unic scop ținerea unui registru destinat prin lege informării publicului și deschis spre consultare publicului în general sau oricărei persoane care probează un interes legitim, cu condiția ca prelucrarea să se limiteze la datele strict necesare ținerii registrului menționat.

(2) Notificarea va cuprinde cel puțin următoarele informații:

- a) numele sau denumirea și domiciliul ori sediul operatorului;
- b) scopul sau scopurile prelucrării;
- c) o descriere a categoriei sau a categoriilor de persoane vizate și a datelor ori a categoriilor de date ce vor fi prelucrate;
- d) destinatarii sau categoriile de destinatari cărora se intenționează să li se dezvăluie datele;
- e) garanțiile care însoțesc dezvăluirea datelor către terți;
- f) modul în care persoanele vizate sunt informate asupra drepturilor lor; data estimată pentru încheierea operațiunilor de prelucrare, precum și destinația ulterioară a datelor;
- g) transferuri de date care se intenționează să fie făcute către alte state;
- h) o descriere generală care să permită aprecierea preliminară a măsurilor luate pentru asigurarea securității prelucrării;



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

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

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

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

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

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

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

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

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

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

## **CAPITOLUL IX**

### **SUPRAVEGHEREA ȘI CONTROLUL PRELUCRĂRILOR DE DATE CU CARACTER PERSONAL**

#### **A. Responsabilul cu protecția datelor**

##### **Art. 47**

(1) Responsabilul cu protecția datelor este desemnat pe baza calităților profesionale și, în special, a cunoștințelor de specialitate în dreptul și practicile din domeniul protecției datelor, precum și pe baza capacității de a îndeplini sarcinile.

(2) Responsabilul cu protecția datelor este un membru al personalului operatorului.

(3) Operatorul publică datele de contact ale responsabilului cu protecția datelor și le comunică autorității de supraveghere.

#### **Art. 48**

(1) Operatorul se asigură că responsabilul cu protecția datelor este implicat în mod corespunzător și în timp util în toate aspectele legate de protecția datelor cu caracter personal.

(2) Operatorul sprijină responsabilul cu protecția datelor în îndeplinirea sarcinilor, asigurându-i resursele necesare pentru executarea acestor sarcini, precum și accesarea datelor cu caracter personal și a operațiunilor de prelucrare, și pentru menținerea cunoștințelor sale de specialitate.

(3) Operatorul se asigură că responsabilul cu protecția datelor nu primește niciun fel de instrucțiuni în ceea ce privește îndeplinirea acestor sarcini. Acesta nu este demis sau sancționat de către operator pentru îndeplinirea sarcinilor sale. Responsabilul cu protecția datelor răspunde direct în fața celui mai înalt nivel al conducerii operatorului.

(4) Persoanele vizate pot contacta responsabilul cu protecția datelor cu privire la toate chestiunile legate de prelucrarea datelor lor și la exercitarea drepturilor lor în temeiul prezentului regulament.

(5) Responsabilul cu protecția datelor are obligația de a respecta secretul sau confidențialitatea în ceea ce privește îndeplinirea sarcinilor sale, în conformitate cu dreptul Uniunii sau cu dreptul intern.

(6) Responsabilul cu protecția datelor poate îndeplini și alte sarcini și atribuții. Operatorul se asigură că niciuna dintre aceste sarcini și atribuții nu generează un conflict de interese.

#### **Art. 49**

(1) Responsabilul cu protecția datelor are cel puțin următoarele sarcini:

a) informarea și consilierea operatorului, precum și a angajaților care se ocupă de prelucrare cu privire la obligațiile care le revin în temeiul prezentului regulament și al altor dispoziții de drept al Uniunii sau drept intern referitoare la protecția datelor;

b) monitorizarea respectării prezentului regulament, a altor dispoziții de drept al Uniunii sau de drept intern referitoare la protecția datelor și a politicilor operatorului în ceea ce privește protecția datelor cu caracter personal, inclusiv alocarea responsabilităților și acțiunile de sensibilizare și de formare a personalului implicat în operațiunile de prelucrare, precum și auditurile aferente;

c) furnizarea de consiliere la cerere în ceea ce privește evaluarea impactului asupra protecției datelor și monitorizarea funcționării acesteia;

d) cooperarea cu autoritatea de supraveghere;

e) asumarea rolului de punct de contact pentru autoritatea de supraveghere privind aspectele legate de prelucrare, inclusiv consultarea prealabilă menționată, precum și, dacă este cazul, consultarea cu privire la orice altă chestiune.

(2) În îndeplinirea sarcinilor sale, responsabilul cu protecția datelor ține seama în mod corespunzător de riscul asociat operațiunilor de prelucrare, luând în considerare natura, domeniul de aplicare, contextul și scopurile prelucrării.

### **B. Autoritatea de supraveghere**

#### **Art. 50**

(1) Autoritatea de supraveghere este Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal.

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

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

## CAPITOLUL X

### TRANSFERUL ÎN STRĂINĂTATE AL DATELOR CU CARACTER PERSONAL

#### A. Condițiile transferului în străinătate al datelor cu caracter personal

##### Art. 51

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

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

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

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

## CAPITOLUL XI

### SOLUȚIONAREA PLÂNGERILOR

#### A. Dreptul de a depune o plângere la o autoritate de supraveghere

##### Art. 52

GPPME este obligată să rezolve plângerile și orice alte cereri legate de prelucrarea datelor cu caracter personal, în termenele și condițiile prevăzute de lege.

##### Art. 53

(1) Fără a aduce atingere oricăror alte căi de atac administrative sau judiciare, orice persoană vizată are dreptul de a depune o plângere la o autoritate de supraveghere, în special în statul membru în care își are reședința obișnuită, în care se află locul său de muncă sau în care a avut loc presupusa încălcare, în cazul în care consideră că prelucrarea datelor cu caracter personal care o vizează încalcă prezentul regulament.

(2) Autoritatea de supraveghere la care s-a depus plângerea informează reclamantul cu privire la evoluția și rezultatul plângerii, inclusiv posibilitatea de a exercita o cale de atac judiciară.

##### Art. 54

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

- (2) Plângerea către autoritatea de supraveghere nu poate fi înaintată dacă o cerere în justiție, având același obiect și aceleași părți, a fost introdusă anterior.
- (3) În afara cazurilor în care o întârziere ar cauza un prejudiciu iminent și ireparabil, plângerea către autoritatea de supraveghere nu poate fi înaintată mai devreme de 15 zile de la înaintarea unei plângeri cu același conținut către operator.
- (4) În vederea soluționării plângerii, dacă apreciază că este necesar, autoritatea de supraveghere poate audia persoana vizată, operatorul sau asociația ori fundația care reprezintă interesele persoanei vizate. Aceste persoane au dreptul de a înainta cereri, documente și memorii. Autoritatea de supraveghere poate dispune efectuarea de expertize.
- (5) Dacă plângerea este găsită întemeiată, autoritatea de supraveghere poate decide suspendarea provizorie sau încetarea prelucrării datelor, ștergerea parțială ori integrală a datelor prelucrate și poate să sesizeze organele de urmărire penală sau să intenteze acțiuni în justiție. Interdicția temporară a prelucrării poate fi instituită numai până la încetarea motivelor care au determinat luarea acestei măsuri.
- (6) Decizia trebuie motivată și se comunică părților interesate în termen de 30 de zile de la data primirii plângerii.
- (7) Autoritatea de supraveghere poate ordona, dacă apreciază necesar, suspendarea unora sau tuturor operațiunilor de prelucrare până la soluționarea plângerii în condițiile alin. (5).
- (8) Autoritatea de supraveghere se poate adresa justiției pentru apărarea oricăror drepturi garantate de prezenta lege persoanelor vizate. Instanța competentă este Tribunalul Municipiului București. Cererea de chemare în judecată este scutită de taxa de timbru.
- (9) La cererea persoanelor vizate, pentru motive întemeiate, instanța poate dispune suspendarea prelucrării până la soluționarea plângerii de către autoritatea de supraveghere.
- (10) Prevederile alin. (4)-(9) se aplică în mod corespunzător și în situația în care autoritatea de supraveghere află pe orice altă cale despre săvârșirea unei încălcări a drepturilor recunoscute de prezenta lege persoanelor vizate.

## **B. Dreptul la o cale de atac judiciară eficientă împotriva unei autorități de supraveghere**

### **Art. 55**

- (1) Fără a aduce atingere oricăror alte căi de atac administrative sau nejudiciare, fiecare persoană fizică sau juridică are dreptul de a exercita o cale de atac judiciară eficientă împotriva unei decizii obligatorii din punct de vedere juridic a unei autorități de supraveghere care o vizează.
- (2) Fără a aduce atingere oricăror alte căi de atac administrative sau nejudiciare, fiecare persoană vizată are dreptul de a exercita o cale de atac judiciară eficientă în cazul în care autoritatea de supraveghere care este competentă nu tratează o plângere sau nu informează persoana vizată în termen de trei luni cu privire la progresele sau la soluționarea plângerii depuse.
- (3) Acțiunile introduse împotriva unei autorități de supraveghere sunt aduse în fața instanțelor din statul membru în care este stabilită autoritatea de supraveghere.
- (4) În cazul în care acțiunile sunt introduse împotriva unei decizii a unei autorități de supraveghere care a fost precedată de un aviz sau o decizie a comitetului în cadrul mecanismului pentru asigurarea coerenței, autoritatea de supraveghere transmite curții avizul respectiv sau decizia respectivă.

## **C. Dreptul la o cale de atac judiciară eficientă împotriva unui operator**

### **Art. 56**

- (1) Fără a aduce atingere vreunei căi de atac administrative sau nejudiciare disponibile, inclusiv dreptului de a depune o plângere la o autoritate de supraveghere, fiecare persoană vizată are dreptul de a exercita o cale de atac judiciară eficientă în cazul în care consideră că

drepturile de care beneficiază în temeiul prezentului regulament au fost încălcate ca urmare a prelucrării datelor sale cu caracter personal fără a se respecta prezentul regulament.

(2) Acțiunile introduse împotriva unui operator sunt prezentate în fața instanțelor din statul membru unde operatorul își are un sediu. Alternativ, o astfel de acțiune poate fi prezentată în fața instanțelor din statul membru în care persoana vizată își are reședința obișnuită, cu excepția cazului în care operatorul este o autoritate publică a unui stat membru ce acționează în exercitarea competențelor sale publice.

#### **D. Dreptul de a se adresa justiției**

##### **Art. 57**

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

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

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

## **CAPITOLUL XII DISPOZIȚII FINALE**

##### **Art. 58**

(1) Prezentul Regulament a fost adoptat în ședința Consiliului de Administrație din data de .....

(2) Temeiul legal în baza căruia a fost adoptat prezentul regulament este REGULAMENTUL nr. 679 din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date

##### **Art. 59**

Anexele 1,2,3,4 fac parte integrantă din prezentul regulament.

#### **LISTA ANEXELOR**

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

*Anexa 2* – Notă de informare

*Anexa 3* – Formular de consimțământ

*Anexa 4* – Cod de conduită

## ANEXE LA PREZENTUL REGULAMENT

### Anexa 1

#### ***CERINȚELE MINIME DE SECURITATE a prelucrărilor de date cu caracter personal***

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

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

#### ***1. Identificarea și autentificarea utilizatorului***

*Prin utilizator se înțelege orice persoană care acționează sub autoritatea operatorului, a persoanei împuternicite sau a reprezentantului, cu drept recunoscut de acces la bazele de date cu caracter personal.*

*Utilizatorii, pentru a căpăta acces la o bază de date cu caracter personal, trebuie să se identifice. Identificarea se poate face prin mai multe metode, cum ar fi: introducerea codului de identificare de la tastatură (un șir de caractere), folosirea unei cartele cu cod de bare, folosirea unei cartele inteligente (smart card) sau a unei cartele magnetice.*

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

*Codurile de identificare (sau conturi de utilizator) nefolosite o perioadă mai îndelungată trebuie dezactivate și distruse după un control prealabil intern al operatorului. Perioada după care codurile trebuie dezactivate și distruse se stabilește de operator.*

*Orice cont de utilizator este însoțit de o modalitate de autentificare. Autentificarea poate fi făcută prin introducerea unei parole sau prin mijloace biometrice: amprenta dactiloscopică, amprenta vocală, angiografia retiniană etc.*

*Parolele sunt șiruri de caractere. Cu cât șirul de caractere este mai lung, cu atât parola este mai greu de aflat. La introducerea parolelor acestea nu trebuie să fie afișate în clar pe monitor. Parolele trebuie schimbate periodic în funcție de politicile de securitate ale entității (operator sau persoană împuternicită). Schimbarea periodică a parolelor se face numai de către utilizatori autorizați de operator.*

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

*Orice utilizator care primește un cod de identificare și un mijloc de autentificare trebuie să păstreze confidențialitatea acestora și să răspundă în acest sens în fața operatorului.*

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

*Operatorii autorizează anumiți utilizatori pentru a revoca sau a suspenda un cod de identificare și autentificare, dacă utilizatorul acestora și-a dat demisia ori a fost concediat, și-a încheiat contractul, a fost transferat la alt serviciu și noile sarcini nu îi solicită accesul la date cu caracter personal, a abuzat de codurile primite sau dacă va absenta o perioadă îndelungată stabilită de entitate.*

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

## **2. Tipul de acces**

*Utilizatorii trebuie să acceseze numai datele cu caracter personal necesare pentru îndeplinirea atribuțiilor lor de serviciu. Pentru aceasta operatorii trebuie să stabilească tipurile de acces după funcționalitate (cum ar fi: administrare, introducere, prelucrare, salvare etc.) și după acțiuni aplicate asupra datelor cu caracter personal (cum ar fi: scriere, citire, ștergere), precum și procedurile privind aceste tipuri de acces.*

*Programatorii sistemelor de prelucrare a datelor cu caracter personal nu vor avea acces la datele cu caracter personal. Operatorul va permite accesul programatorilor la datele cu caracter personal după ce acestea au fost transformate în date anonime.*

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

*Pentru activitatea de pregătire a utilizatorilor sau pentru realizarea de prezentări se vor folosi date anonime. Angajații care predau cursurile de pregătire vor folosi date cu caracter personal pe parcursul propriei lor pregătiri.*

*Operatorul va stabili modalitățile stricte prin care se vor distruge datele cu caracter personal. Autorizarea pentru această prelucrare de date cu caracter personal trebuie limitată la câțiva utilizatori.*

## **3. Colectarea datelor**

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

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

*Operatorul va lua măsuri pentru ca sistemul informațional să înregistreze cine a făcut modificarea, data și ora modificării. Pentru o mai bună administrare operatorul va lua măsuri ca sistemul informațional să mențină datele șterse sau modificate.*

## **4. Execuția copiilor de siguranță**

*Operatorul va stabili intervalul de timp la care se vor executa copiile de siguranță ale bazelor de date cu caracter personal, precum și ale programelor folosite pentru prelucrările automatizate. Utilizatorii care execută aceste copii de siguranță vor fi numiți de operator, într-un număr restrâns. Copiile de siguranță se vor stoca în alte camere, în fișete metalice cu sigiliu aplicat, și, dacă este posibil, chiar în camere din altă clădire.*

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

## **5. Computerele și terminalele de acces**

*Computerele și alte terminale de acces vor fi instalate în încăperi cu acces restricționat. Dacă nu pot fi asigurate aceste condiții, computerele se vor instala în încăperi care se pot încuia sau se vor lua măsuri ca accesul la computere să se facă cu ajutorul unor chei ori cartele magnetice.*

*Dacă pe ecran apar date cu caracter personal asupra cărora nu se acționează o perioadă dată, stabilită de operator, sesiunea de lucru trebuie închisă automat. Mărimea acestei perioade se determină în funcție de operațiile care trebuie executate.*

*Terminalele de acces folosite în relația cu publicul, pe care apar date cu caracter personal, vor fi poziționate astfel încât să nu poată fi văzute de public și după o perioadă scurtă, stabilită de operator, în care nu se acționează asupra lor, acestea trebuie ascunse.*

## **6. Fișierele de acces**

*Operatorul este obligat să ia măsuri ca orice accesare a bazei de date cu caracter personal să fie înregistrată într-un fișier de acces (numit log la prelucrările automate) sau într-un registru pentru prelucrările manuale de date cu caracter personal, stabilit de operator. Informațiile înregistrate în fișierul de acces sau în registru vor fi:*

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

*Pentru prelucrările automate aceste informații vor fi stocate într-un fișier de acces general sau în fișiere separate pentru fiecare utilizator. Orice încercare de acces neautorizat va fi, de asemenea, înregistrată.*

*Operatorul este obligat să păstreze fișierele de acces cel puțin 2 ani, pentru a fi folosite ca probe în cazul unor investigații. Dacă investigațiile se prelungesc, aceste fișiere se vor păstra atât timp cât se va considera necesar.*

*Fișierele de acces trebuie să facă posibilă identificarea de către operator sau de către persoana împuternicită a persoanelor care au accesat date cu caracter personal fără un motiv anume, în vederea aplicării unor sancțiuni sau a sesizării organelor competente.*

## **7. Sistemele de telecomunicații**

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

*Operatorii sunt obligați să conceapă sistemul de telecomunicații astfel încât datele cu caracter personal să nu poată fi interceptate sau transmise de oriunde. Dacă sistemul de telecomunicații nu poate fi astfel securizat, operatorul este obligat să impună folosirea metodei de criptare pentru transmisia datelor cu caracter personal.*

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

## **8. Instruirea personalului**



*În cadrul cursurilor de pregătire a utilizatorilor operatorul este obligat să facă informarea acestora cu privire la prevederile regulamentului cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date, la cerințele minime de securitate a prelucrărilor de date cu caracter personal, precum și cu privire la riscurile pe care le comportă prelucrarea datelor cu caracter personal, în funcție de specificul activității utilizatorului.*

*Utilizatorii care au acces la date cu caracter personal vor fi instruiți de către operator asupra confidențialității acestora și vor fi avertizați prin mesaje care vor apărea pe monitoare în timpul activității. Utilizatorii sunt obligați să își închidă sesiunea de lucru atunci când părăsesc locul de muncă.*

## **9. Folosirea computerelor**

*Pentru menținerea securității prelucrării datelor cu caracter personal (în special împotriva virușilor informatici) operatorul va lua măsuri care vor consta în:*

- a) interzicerea folosirii de către utilizatori a programelor software care provin din surse externe sau dubioase;*
- b) informarea utilizatorilor în privința pericolului privind virușii informatici;*
- c) implementarea unor sisteme automate de devirusare și de securitate a sistemelor informatice;*
- d) dezactivarea, pe cât posibil, a tastei "Print screen", atunci când sunt afișate pe monitor date cu caracter personal, interzicându-se astfel scoaterea la imprimantă a acestora.*

## **10. Imprimarea datelor**

*Scoaterea la imprimantă a datelor cu caracter personal se va realiza numai de utilizatori autorizați pentru această operațiune de către operator. Operatorii sunt obligați să aprobe proceduri interne specifice privind folosirea și distrugerea acestor materiale.*

*Fiecare entitate își va aproba propriul sistem de securitate, ținând seama de aceste cerințe minime de securitate a prelucrărilor de date cu caracter personal, iar în funcție de importanța datelor cu caracter personal prelucrate, își va impune măsuri de securitate suplimentare.*

## **11. Prelucrări automate de date cu caracter personal**

*Accesul utilizatorilor la bazele de date ce conțin date cu caracter personal se va efectua prin coduri personale de acces (nume de logare, nume de utilizator).*

*Codurile de acces sunt protejate prin metode de autentificare (parole). Codurile de acces (conturi utilizator) sunt alocate individual pentru fiecare utilizator pe baza unei proceduri specifice. Conturile de utilizator nefolosite o perioadă mai îndelungată sunt șterse sau dezactivate permanent după un control prealabil intern al operatorului. Codurile de acces se vor dezactiva automat după un număr rezonabil de încercări nereușite. Perioada și numărul de încercări nereușite după care codurile trebuie dezactivate sau șterse se stabilește de operator.*

*Codurile de acces vor permite doar nivelul minim de acces la datele cu caracter personal ce sunt necesare pentru îndeplinirea atribuțiilor de serviciu.*

*Programatorii care dezvoltă aplicațiile care prelucrează datele cu caracter personal nu au acces la datele cu caracter personal. Operatorul va permite accesul programatorilor la datele cu caracter personal după ce acestea au fost transformate în date anonime.*

*Pentru activitatea de pregătire a utilizatorilor sau pentru realizarea de prezentări se vor folosi date anonime. Angajații care predau cursurile de pregătire nu vor folosi date cu caracter personal pe parcursul propriei lor pregătiri.*

*Computerele vor fi instalate în încăperi cu acces restricționat. Dacă nu pot fi asigurate aceste condiții, computerele se vor instala în încăperi care se pot încuia sau se vor lua măsuri ca accesul la computere să se facă cu ajutorul unor chei.*

*Orice accesare a bazei de date cu caracter personal, inclusiv orice încercare de acces neautorizat, va fi înregistrată într-un fișier de acces. Fișierele de acces trebuie să facă posibilă identificarea de către operator, reprezentant sau de către persoana împuternicită a persoanelor care au accesat date cu caracter personal fără un motiv legitim, în vederea aplicării unor sancțiuni sau a sesizării organelor competente.*

*Operatorul este obligat să păstreze fișierele de acces cel puțin 2 ani, pentru a fi folosite ca probe în cazul unor investigații. Dacă investigațiile se prelungesc, aceste fișiere se vor păstra atât timp cât se va considera necesar.*

*Computerele și alte terminale de acces vor fi instalate în încăperi cu acces restricționat. Dacă nu pot fi asigurate aceste condiții, acestea se vor instala în încăperi care se pot încuia sau se vor lua măsuri ca accesul la computere să se facă cu ajutorul unor chei.*

*Computerele sau terminalele de acces folosite în relația cu publicul, pe care sunt afișate date cu caracter personal, vor fi poziționate astfel încât acestea să nu poată fi dezvăluite publicului. După o perioadă scurtă, stabilită de operator, în care nu se acționează asupra lor, acestea trebuie ascunse.*

*Operatorii sunt obligați să conceapă sistemul de telecomunicații astfel încât datele cu caracter personal să nu poată fi interceptate sau transmise de oriunde. Dacă sistemul de telecomunicații nu poate fi astfel securizat, operatorul este obligat să impună folosirea unor metode de criptare pentru transmisia datelor cu caracter personal. Prin sistemele de telecomunicații se vor transmite numai datele cu caracter personal strict necesare pentru realizarea scopului comunicației respective.*

*Operatorul va stabili intervalul de timp rezonabil la care se vor executa copiile de siguranță ale bazelor de date cu caracter personal, precum și ale programelor folosite pentru prelucrările automatizate. Copiile de siguranță se vor stoca în alte camere decât cele destinate utilizării computerelor, în fișete metalice cu sigiliu aplicat.*

## **12. Prelucrări manuale de date cu caracter personal**

*În cadrul prelucrărilor de date cu caracter personal efectuate manual, accesul utilizatorilor se va realiza pe baza unei liste aprobate de conducerea entității.*

*Modalitatea de acces și datele care pot fi accesate de fiecare utilizator vor fi stabilite de către operator prin proceduri interne.*

*Documentele care conțin date cu caracter personal vor fi ținute în fișete sau dulapuri închise cu cheie sau cu un alt mecanism de securizare.*

*Documentele care conțin date cu caracter personal, folosite pentru realizarea anumitor operațiuni se vor preda persoanelor abilitate sau se vor închide imediat după terminarea acestora.*

## **13. Prelucrări automate de date cu caracter personal care fac parte din categoria datelor cu caracter special**

*Pe lângă prevederile referitoare la prelucrările automate de date cu caracter personal se vor impune suplimentar următoarele măsuri:*

*a. accesul utilizatorilor la computerele sau terminalele de acces va fi posibil prin folosirea unor cartele magnetice sau a unor cartele inteligente („smart carduri”) de preferință sau se va*

*impune schimbarea periodică automată a codului de acces pentru autentificare. Perioada de schimbare automată a codului de acces pentru autentificare va fi stabilită prin procedură internă de către operator dar fără să depășească o lună calendaristică;*

*b. nivelul de autorizare și acces la aceste date pentru fiecare utilizator se va stabili de către persoanele desemnate special pentru aceste sarcini;*

*c. periodic, la intervale care nu vor depăși un an, se vor efectua verificări privind accesul și nivelul de acces ale utilizatorilor la datele cu caracter personal.*

#### **14. Prelucrări manuale de date cu caracter personal care fac parte din categoria datelor cu caracter special**

*Pe lângă prevederile referitoare la prelucrările manuale ale datelor cu caracter personal se vor impune suplimentar următoarele măsuri:*

- a. prelucrarea datelor cu caracter personal se va efectua numai de către utilizatorii desemnați de operator prin proceduri interne;*
- b. accesul utilizatorilor se va face pe baza unor proceduri emise de operator;*
- c. orice accesare a datelor cu caracter personal va fi înregistrată într-un registru de acces.*

#### **15. Documente obligatorii pentru prelucrarea datelor personale care fac parte din categoria datelor cu caracter special**

*Operatorii care prelucrează date cu caracter personal care fac parte din categoria datelor cu caracter special vor întocmi obligatoriu următoarele documente:*

- a. proceduri de control al accesului în aceste zone (măsuri tehnice și organizatorice privind securizarea zonei în care se prelucrează aceste date);*
- b. proceduri de asigurare a integrității și disponibilității datelor;*
- c. proceduri privind securitatea transmisiilor de date și accesul securizat la aceste mijloace de transmitere a datelor.*

#### **16. Securitatea datelor colectate**

*În conformitate cu prevederile legale în vigoare și cu stadiul actual al tehnologiei, GPPME a implementat măsuri tehnice și organizatorice adecvate pentru asigurarea securității datelor cu caracter personal în decursul activității noastre, conform regulilor detaliate mai jos. Am actualizat formularistica utilizată în cadrul GPPME pentru a ne asigura că întotdeauna persoanele vizate sunt permanent informate cu privire la procesările pe care le efectuăm și sunt la curent cu drepturile lor.*

*În activitatea noastră urmărim în primul rând prevenirea oricăror incidente de securitate, precum acces neautorizat la date, scurgeri de informații, ștergere accidentală a datelor și altele asemenea, întreaga structură a prelucrărilor de date fiind construită în jurul principiului prevenției.*

*Totuși, având în vedere că în societatea informațională securitatea prelucrărilor nu poate fi 100% garantată, GPPME a luat, de asemenea, măsuri ca, în cazul improbabil în care apar incidente de securitate, întinderea și gravitatea acestora să fie diminuate.*

#### **A. REGULI GENERALE**

*Pentru a asigura protecția adecvată a datelor cu caracter personal la care GPPME are acces, am implementat măsuri organizatorice și tehnice, precum:*

a) Semnarea unor documente suplimentare cu angajatii, colaboratorii și partenerii noștri pentru asigurarea confidențialității datelor cu caracter personal la care au acces cel puțin la un nivel similar cu cel impus de entitatea noastră.

b) Implementarea unor măsuri de securitate fizice cu privire la documentele care conțin date cu caracter personal, cum ar fi, de exemplu, stocarea documentelor în dulapuri închise cu cheie la care are acces doar personalul autorizat, implementarea unor sisteme de acces restricționat (de exemplu, chei, carduri de acces) exclusiv pentru persoanele care justifică un interes pentru accesul respectivelor date.

c) Implementarea unor măsuri de securitate în ceea ce privește sistemele informatice, cum ar fi, de exemplu, asigurarea ca toate echipamentele noastre dispun de programe de securitate corespunzătoare, asigurarea unor copii de rezervă etc.

d) Implementarea unor programe de instruire a personalului cu privire la cerințele GDPR.

## **B. REGULI SPECIFICE**

GPPME a implementat următoarele reguli specifice pentru protecția datelor cu caracter personal:

### **a) Reguli de securitate tehnică**

i. Interzicerea folosirii de către utilizatorii de sisteme a unor programe software nelicențiate sau care provin din surse nesigure;

ii. Implementarea unui sistem de autentificare bazat pe user și parole securizate, unice pentru fiecare utilizator autorizat; astfel, pe de o parte se împiedică accesul terților la terminale/bazele de date și, pe de altă parte, la introducerea greșită a userului/parolei de un anumit număr de ori, sistemul se blochează automat, conform procedurilor tehnice interne;

iii. Implementarea unor măsuri de securitate adecvate ale echipamentelor IT și software-ului utilizat în activitatea noastră, după cum urmează:

- informarea utilizatorilor în privința pericolului privind virușii informatici;
- implementarea unor software-uri de protecție adecvate pe terminalele utilizate, precum programe antivirus și informarea salariaților asupra obligativității de scanare periodică a sistemelor pentru prevenirea oricăror programe neautorizate (e.g. malware, phishing) sau, după caz, implementarea unor sisteme automate de devirusare și de securitate a sistemelor informatice;
- dezactivarea pe cât posibil tastei "Print screen", atunci când sunt afișate pe monitor date cu caracter personal, limitându-se astfel posibilitatea de scoatere la imprimantă a acestora de către alți utilizatori decât aceia autorizați în acest sens;
- limitarea drepturilor de printare, prin implementarea unor sisteme bazate pe user/parolă;
- monitorizarea accesului la baza de date și logarea accesului și a parcursului utilizatorului;
- schimbarea periodică a parolelor de acces la baza de date și la sistemele informatice;
- obligația angajaților de a securiza accesul în terminalele proprii atunci când nu le utilizează și de a închide terminalele la finalul programului de muncă;
- limitarea drepturilor de acces la bazele de date de la distanță (i.e. din afara instituției)/cu utilizarea altor dispozitive decât cele puse la dispoziție de unitate;
- interzicerea utilizării unor rețele publice (cu acces deschis) de conexiune la internet

## ***b) Reguli de securitate organizatorică***

*i. Limitarea numărului de destinatari/utilizatori care au acces la datele cu caracter personal și corelarea drepturilor de acces cu necesitatea justificată de fiecare utilizator – e.g. prin împărțirea pe arii geografice a informațiilor despre persoanele vizate, prin transmiterea către împuterniciți doar a datelor necesare pentru executarea contractului etc.;*

*ii. Introducerea unor condiții și obligații de confidențialitate și protecție a datelor cu caracter personal suplimentare pentru angajați, colaboratori, furnizori și parteneri;*

*iii. Introducerea unor reguli specifice privind copierea și diseminarea documentelor pentru a preveni răspandirea și accesul unor persoane neautorizate la datele cu caracter personal;*

*iv. Introducerea unor reguli prin care angajații, colaboratorii și partenerii noștri au acces numai la acele date cu caracter personal necesare îndeplinirii fișei postului sau, după caz, a obligațiilor asumate față de GPPME;*

*v. Instalarea unor sisteme de alarmă și monitorizare a accesului în spațiile unde sunt stocate documentele care conțin date cu caracter personal sau echipamentele pe care sunt stocate aceste date;*

*vi. Instalarea unor sisteme de asigurare a securității fizice a documentelor care cuprind date cu caracter personal, precum dulapuri închise sub cheie, asigurarea supravegherii video a clădirii în care ne desfășurăm activitatea (fiind marcate corespunzător zonele supravegheate video);*

*vii. Realizarea unor copii de siguranță a datelor stocate;*

*viii. Restricționarea accesului persoanelor neautorizate în spațiile unde sunt stocate datele cu caracter personal sau echipamentele pe care acestea sunt stocate, decât cu asigurarea unor condiții de confidențialitate corespunzătoare;*

*ix. Interzicerea copierii datelor cu caracter personal pe medii de stocare mobile, fără acordul prealabil al conducerii unității, cu excepția situației când aceasta este necesară pentru îndeplinirea unor obligații asumate contractual;*

*x. Asigurarea instruirii periodice a personalului cu privire la cerințele GDPR, precum și cele de securitate și riscurile privind datele cu caracter personal.*

ANEXA 1 LA CONTRACTUL DE MUNCĂ NR. \_\_\_\_/\_\_\_\_\_  
AL SALARIATULUI \_\_\_\_\_

### NOTĂ DE INFORMARE

În condițiile art. 13 al Regulamentului (UE) 2016/679 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul General privind protecția datelor)

Grădinița cu Program Prolungit „Mihai Eminescu”, având sediul în Tg-Jiu, str. Olari, Nr.3, având CUI 29448992, nr. tel./fax 0353 801417, e-mail [gr\\_eminescu\\_gj@yahoo.com](mailto:gr_eminescu_gj@yahoo.com), în calitate de operator de date cu caracter personal, reprezentată legal de dna. Bîzdoacă Ana-Maria, nr. tel. 0774608439, e-mail [ana\\_maria883@yahoo.com](mailto:ana_maria883@yahoo.com), în conformitate cu art. 13 al Regulamentului (UE) 2016/676, vă aducem la cunoștință următoarele:

A. Datele dumneavoastră personale sunt prelucrate în scopul/scopurile: angajării și derulării raporturilor de muncă, securității și sănătății în muncă, situațiilor de urgență, transport, medicina muncii, contabilitate - salarizare, în temeiul art. 6 alin. (1) lit. b, c din Regulamentul (UE) 2016/676 (respectiv, **prelucrarea este necesară pentru executarea unui contract la care persoana vizată este parte sau pentru a face demersuri la cererea unei persoane vizate înainte de încheierea unui contract; prelucrarea este necesară în vederea îndeplinirii unei obligații legale ce revine operatorului**).

Furnizarea datelor personale precum nume, prenume, adresă, cod numeric personal, data și locul nașterii, serie și număr act de identitate, telefon, e-mail, venit, imagine, semnătură, adresa e-mail, date medicale, date privind cazierul judiciar, cetățenia, starea civilă reprezintă o obligație legală/contractuală sau o obligație necesară pentru încheierea unui contract, astfel că furnizarea acestor informații este obligatorie, iar nerespectarea ei atrage imposibilitatea încheierii unui contract individual de muncă.

B. Datele dumneavoastră cu caracter personal pot fi transmise următorilor destinatari:

- Societăți comerciale autorizate a presta activități în domeniul SSM, S.U., MEDICINA MUNCII, RESURSE UMANE, SALARIZARE-CONTABILITATE, TRANSPORT, cu care unitatea noastră are încheiat un contract de prestări servicii;
- REGISTRUL GENERAL DE EVIDENȚĂ AL SALARIAȚILOR, prin aplicația REVISAL;
- EDUSAL;
- FOREXEBUG;
- SIIIR;
- Autorități publice, la solicitarea acestora;
- Organe de control, la solicitarea acestora;
- Organe fiscale/organe judiciare;
- Executori judecătorești, la solicitarea acestora;
- Instituțiilor bancare, la solicitarea acestora.

C. Datele personale ale dumneavoastră vor fi/nu vor fi transmise către o țară terță sau organizație internațională.

D. Perioada pentru care vor fi stocate datele cu caracter personal este: fișele SSM, PSI și fișele de aptitudine eliberate de către serviciile de medicina muncii, pe perioada derulării raporturilor de muncă, evidențele REVISAL și cele financiar-contabile conform dispozițiilor legale în materie.

E. În raport cu operatorul și în ceea ce privește datele personale furnizate, aveți următoarele drepturi:

- Dreptul de a obține din partea operatorului o confirmare că se prelucrează sau nu datele dumneavoastră personale;
- Dreptul de acces la următoarele informații: scopurile prelucrării; categoriile de date cu caracter personal vizate; destinatarii sau categoriile de destinatari cărora datele cu caracter personal le-au fost sau urmează să le fie divulgate; acolo unde este posibil, perioada pentru care se preconizează că vor fi stocate datele cu caracter personal sau dacă acest lucru nu este posibil, criteriile utilizate pentru a stabili această perioadă;
- Dreptul de a solicita operatorului rectificarea sau ștergerea datelor ori restricționarea prelucrării datelor cu caracter personal;
- Dreptul de a se opune prelucrării;
- Dreptul de a depune o plângere în fața autorității de supraveghere; în cazul în care datele cu caracter personal nu sunt colectate de la persoana vizată, orice informații disponibile privind sursa acestora; existența unui proces decizional automatizat incluzând crearea de profiluri, precum și informații pertinente privind logica utilizată și privind importanța și consecințele preconizate ale unei astfel de prelucrări;
- Dreptul la rectificarea datelor inexacte;
- Dreptul la ștergerea datelor sau „dreptul de a fi uitat”;
- Dreptul la restricționarea prelucrării în cazurile următoare: când contestați exactitatea datelor (restricționarea prelucrării va dura o perioadă ce îi permite operatorului să verifice exactitatea datelor); când prelucrarea este ilegală, iar dumneavoastră vă opuneți ștergerii datelor, solicitând în schimb restricționarea utilizării lor; când operatorul nu mai are nevoie de datele cu caracter personal în scopul prelucrării, dar dumneavoastră le solicitați pentru exercitarea unui drept în instanță;
- Dreptul de a primi datele cu caracter personal și de a le transmite unui alt operator sau „dreptul la portabilitatea datelor”;
- Dreptul de a va opune prelucrării necesare pentru îndeplinirea unei sarcini ce servește unui interes public sau care rezultă din exercitarea autorității publice cu care este investit operatorul sau prelucrării necesare în scopul intereselor legitime urmărite de operator sau de o terță parte, precum și creării de profiluri pe baza acestor dispoziții;
- Dreptul de a nu face obiectul unei decizii bazate exclusiv pe prelucrarea automată, inclusiv crearea de profiluri, cu excepția cazurilor în care o astfel de prelucrare este necesară pentru încheierea sau executarea unui contract, când este autorizată de dreptul Uniunii sau de dreptul intern sau când există consimțământul persoanei vizate;
- Dreptul de a va retrage consimțământul în orice moment, pentru situația în care se prelucrează date în temeiul consimțământului expres (conform art. 6 alin. 1 lit. a din Regulamentul UE 2016/679), precum și în situația în care se prelucrează date cu caracter personal care dezvăluie originea rasială sau etnică, opiniile politice, confesiunea religioasă sau convingerile filozofice sau apartenența la sindicate și prelucrarea de date genetice, de date biometrice pentru identificarea unică a unei persoane fizice, de date privind sănătatea sau date privind viața sexuală sau orientarea sexuală, când prelucrarea acestor date se realizează în baza consimțământului explicit;
- Dreptul de a depune o plângere în fața unei autorități de supraveghere.

Prezenta cuprinde 3 (trei) pagini și servește la informarea persoanei/persoanelor vizate, pentru situația în care datele cu caracter personal sunt colectate direct de la persoana vizată.

Am luat la cunoștință,

Data: \_\_\_\_\_

Nume, prenume: \_\_\_\_\_

Semnătura: \_\_\_\_\_



**ANEXA NR. 2 LA CONTRACTUL DE MUNCĂ NR. \_\_\_\_/\_\_\_\_\_  
AL SALARIATULUI \_\_\_\_\_**

**FORMULAR DE CONSIMȚĂMÂNT**

În temeiul art. 6 alin. (1) lit. a) al Regulamentului (UE) 2016/679 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul General privind protecția datelor)

Subsemnatul/subsemnata \_\_\_\_\_, cu următoarele date de identificare, \_\_\_\_\_, am adus la cunoștința Grădiniței cu Program Prelungit „Mihai Eminescu”, având sediul în Tg-Jiu, str. Olari, Nr.3, având CUI 29448992, nr. tel./fax 0353 801417, e-mail [gr\\_eminescu\\_gj@yahoo.com](mailto:gr_eminescu_gj@yahoo.com), reprezentată legal de dna. Bîzdoacă Ana-Maria, nr. tel. 0774608439, e-mail [ana\\_maria883@yahoo.com](mailto:ana_maria883@yahoo.com), în calitate de operator de date cu caracter personal, următoarele date personale: nume, prenume, adresă, cod numeric personal, data și locul nașterii, serie și număr act de identitate, telefon, e-mail, venit, imagine, semnătura, adresa IP, date medicale, date privind cazierul judiciar, cetățenia, starea civilă.

Datele personale antemenționate au fost furnizate operatorului de date cu caracter personal în contextul unui CV, a unui formular de angajare și a unui contract individual de muncă, precum și cu ocazia efectuării controlului medical în vederea angajării.

Cu ocazia furnizării datelor cu caracter personal, mi s-au adus la cunoștință informațiile prevăzute de art. 13 al Regulamentului (UE) 2016/679, precum și drepturile ce îmi revin în temeiul acestui Regulament, prin intermediul unei note de informare ce constituie parte integrantă a prezentului formular.

În egală măsură, mi s-a adus la cunoștință și înțeleg că scopul prelucrării datelor cu caracter personal furnizate este reprezentat de efectuarea controalelor medicale de medicina muncii, angajarea subsemnatului/subsemnatei, efectuarea instructajelor în domeniul SSM, PSI, prelucrarea realizându-se în temeiul art. 6 alin.1, lit. b, c din Regulamentul (UE) 2016/676 (respectiv, prelucrarea este necesară pentru executarea unui contract la care persoana vizată este parte sau pentru a face demersuri la cererea unei persoane vizate înainte de încheierea unui contract; prelucrarea este necesară în vederea îndeplinirii unei obligații legale ce revine operatorului).

Prin semnarea prezentului formular, în mod liber, declar că înțeleg și că sunt de acord ca datele cu caracter personal puse la dispoziția operatorului să fie prelucrate de către acesta, în scopul/scopurile încheierii unui contract individual de muncă și derulării raporturilor de muncă.

Data: \_\_\_\_\_

Nume, prenume: \_\_\_\_\_

Semnătura: \_\_\_\_\_

## **COD DE CONDUITĂ**

### *Preambul*

*Luând în considerare importanța deosebită a garantării dreptului la viață intimă, familială și privată, așa cum este prevăzut la art. 26 din Constituția României, ținând seama de necesitatea protejării acestui drept fundamental în cadrul activităților de prelucrare a datelor cu caracter personal, reglementate prin Regulamentul nr. 679 din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date*

### *CAPITOLUL I Dispoziții generale*

#### *Scopul și sfera de aplicare*

##### *Art. 1*

- (1) Prezentul cod de conduită are ca scop stabilirea unor norme de conduită pentru asigurarea unui nivel satisfăcător de protecție a datelor cu caracter personal prelucrate.*
- (2) Normele de conduită stabilesc exercitarea drepturilor și obligațiilor în domeniul protecției persoanelor în privința datelor cu caracter personal, în relațiile GPPME cu persoanele vizate (în calitate de beneficiari ai serviciilor prestate, de utilizatori etc.).*
- (3) Normele cuprinse în prezentul model de cod de conduită nu aduc atingere altor obligații legale imperative sau deontologice care revin asociațiilor profesionale.*

#### *Definirea termenilor*

##### *Art. 2*

- (1) Termenii folosiți în prezentul cod de conduită au următorul sens:*
- a) persoană vizată - persoana fizică ale cărei date cu caracter personal sunt prelucrate;*
- b) a colecta - a strânge, a aduna, a primi date cu caracter personal prin orice mijloace și din orice sursă;*
- c) a dezvălui - a transmite, a disemina, a face disponibile în orice alt mod date cu caracter personal, în afara operatorului;*
- d) a utiliza - a se folosi datele cu caracter personal de către și în interiorul operatorului;*
- e) consimțământ - acordul neviciat al persoanei vizate de a-i fi prelucrate datele cu caracter personal, care trebuie să fie întotdeauna expres și neechivoc;*
- f) nivel de protecție și de securitate adecvat al prelucrărilor de date cu caracter personal - nivelul de securitate proporțional riscului, pe care îl comportă prelucrarea față de datele cu*

*caracter personal respective și față de drepturile și libertățile persoanelor și conform cerințelor minime de securitate a prelucrărilor de date cu caracter personal, elaborate de autoritatea de supraveghere și actualizate corespunzător stadiului dezvoltării tehnologice și costurilor implementării acestor măsuri;*

*g) marketing direct - promovarea produselor și a serviciilor, adresată direct clienților, persoane fizice, prin mijloace de genul poștei, inclusiv cea electronică, sau alte mijloace de marketing la distanță, altele decât modalitățile promoționale obișnuite (reclame).*

*(2) Termeni precum: date cu caracter personal, prelucrarea datelor cu caracter personal, stocare, operator, terț, destinatar, date anonime, autoritate de supraveghere, dreptul de informare, dreptul de acces, dreptul de intervenție, dreptul de opoziție au sensurile definite de REGULAMENTUL nr. 679 din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date*

### *Cadrul legal al codurilor de conduită*

#### *Art. 3*

*Vor fi respectate dispozițiile legale referitoare la protecția dreptului la viață intimă, familială și privată, în ceea ce privește prelucrarea datelor cu caracter personal. Se vor avea în vedere în mod special dispozițiile REGULAMENTULUI nr. 679 din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date.*

## *CAPITOLUL II*

### *Principiile prelucrărilor de date cu caracter personal efectuate de GPPME*

#### *Legalitatea și transparența*

#### *Art. 4*

*(1) GPPME recunoaște și respectă dreptul la viață intimă, familială și privată.*

*(2) Prelucrarea datelor cu caracter personal de către GPPME se desfășoară în conformitate cu prevederile legale în vigoare.*

*(3) GPPME este obligată să asigure transparența prelucrărilor de date cu caracter personal.*

#### *Responsabilitatea*

#### *Art. 5*

*(1) GPPME este responsabilă pentru datele cu caracter personal aflate sub controlul său, precum și pentru datele transferate către terți.*

*(2) GPPME va desemna persoanele care vor răspunde pentru respectarea dispozițiilor legale din domeniul protecției persoanelor și a datelor cu caracter personal, precum și a principiilor prevăzute în prezentul cod de conduită.*

## *Legitimitatea scopului colectării*

### *Art. 6*

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

*(2) GPPME va comunica scopurile pentru care sunt colectate datele cu caracter personal fie înainte, fie cel mai târziu la momentul colectării.*

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

## *Consimțământul*

### *Art. 7*

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

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

*(3) Persoana vizată își poate retrage consimțământul în orice moment, sub condiția avizării prealabile a operatorului. Acesta va informa persoana vizată în legătură cu procedura și efectele retragerii consimțământului.*

## *Legitimitatea dezvoltării*

### *Art. 8*

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

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

## *Legitimitatea stocării*

### *Art. 9*

*(1) GPPME este obligată să păstreze datele cu caracter personal exacte, complete și actualizate, pentru realizarea scopurilor pentru care sunt utilizate.*

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

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

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

*(5) În urma verificărilor periodice datele cu caracter personal deținute de operator, care nu mai servesc realizării scopurilor sau îndeplinirii unor obligații legale, vor fi distruse sau transformate în date anonime într-un interval de timp rezonabil, potrivit procedurilor stabilite de lege.*

### *Securitatea prelucrărilor*

#### *Art. 10*

*GPPME va lua toate măsurile tehnice și organizatorice necesare pentru asigurarea unui nivel de protecție și de securitate adecvat, în cadrul operațiunilor efectuate asupra datelor cu caracter personal, în următoarele scopuri: pentru a limita accesul la bazele de date, care este permis numai persoanelor autorizate; pentru a interzice copierea datelor în afara locurilor în care sunt gestionate; în general, pentru a împiedica orice circulație necontrolată a datelor.*

### *Dreptul de informare*

#### *Art. 11*

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

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

*(3) În cazul în care dezvăluirea datelor este impusă de lege (de exemplu, în vederea executării unei hotărâri judecătorești), GPPME se va asigura că terțul care solicită dezvăluirea acționează în conformitate cu dispozițiile legale incidente, iar cererea privește numai datele cu caracter personal neexcesive prin raportare la scopul prelucrării. Persoana vizată va fi informată în legătură cu dezvăluirea, numai dacă legea permite.*

### *Dreptul de acces*

#### *Art. 12*

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

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

*(3) GPPME este obligată să motiveze refuzul de a permite accesul la anumite date cu caracter personal.*

## *Dreptul de intervenție*

### *Art. 13*

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

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

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

*(4) Actualizarea bazelor de date se face prin intermediul informațiilor transmise de persoanele vizate, precum și prin informațiile furnizate de orice sursă externă autorizată de lege.*

## *Dreptul de opoziție*

### *Art. 14*

*(1) Exercițarea de către persoana vizată a dreptului de opoziție împotriva prelucrării datelor cu caracter personal, în efectuarea operațiunilor de marketing direct, este asigurată prin intermediul formulării unor cereri în acest sens și prin includerea în listele de opoziție a persoanelor vizate. Persoana vizată va fi încunoștințată de existența listelor de opoziție, precum și de modalitatea de a solicita includerea în acestea.*

*(2) Persoanele vizate își pot exercita dreptul de opoziție în orice moment, de preferință într-un termen rezonabil acordat de operator, fără a se aduce atingere posibilității ca dreptul să fie exercitat și în afara acestui termen.*

*(3) Listele de opoziție sunt gestionate de GPPME.*

*(4) În cazul prelucrărilor ulterioare, precum și al transferului către alți operatori al datelor cu caracter personal, GPPME se va asigura că acestea nu privesc date pentru care persoanele vizate au exercitat anterior dreptul de a le fi șterse datele sau dreptul de opoziție la transferul acestora.*

## *Legitimitatea transferului*

### *Art. 15*

*(1) În cazul transferului de date cu caracter personal către alți operatori, în special în operațiunile de marketing direct, persoanele vizate vor fi informate cu privire la transfer prin înscrierea unor mențiuni pe ofertele de produse sau servicii.*

*(2) Mențiunile prevăzute la alin. (1) vor cuprinde și specificarea dreptului de opoziție la transferul datelor, precum și metoda prin care persoanele vizate își pot exercita acest drept.*

*(3) Garanțiile pentru asigurarea protecției datelor cu caracter personal în cadrul transferului de date către alți operatori vor fi prevăzute prin clauze contractuale privind utilizarea acestor date, acolo unde este cazul. Aceste clauze vor menționa, printre altele, drepturile recunoscute persoanelor vizate, precum și faptul că aceste drepturi pot fi exercitate doar cu respectarea confidențialității anumitor clauze comerciale.*

## *Soluționarea plângerilor*

### *Art. 16*

*(1) GPPME este obligată să rezolve plângerile și orice alte cereri legate de prelucrarea datelor cu caracter personal, în termenele și condițiile prevăzute de lege.*

*(2) Procedura de primire, investigare și de soluționare a plângerilor și a celorlalte cereri ale persoanelor vizate va fi stabilită de către GPPME și va fi adusă la cunoștință persoanelor vizate.*

### *Colaborarea cu autoritatea de supraveghere*

### *Art. 17*

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

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

### *Cheltuielile suportate de către persoanele vizate*

### *Art. 18*

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

## *CAPITOLUL III*

### *Dispoziții finale și tranzitorii*

### *Modul de aplicare*

### *Art. 19*

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

### *Modificarea și completarea modelului de cod de conduită*

### *Art. 20*

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

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