



UNIUNEA EUROPEANĂ



GUVERNUL ROMÂNIEI



Instrumente Structurale  
2014-2020

## FONDUL SOCIAL EUROPEAN

Proiect cofinanțat prin Programul Operational Capital Uman

**Axa Prioritară 4 - Incluziunea socială și combaterea sărăciei**

Componentă 1 - Apel : POCU/449/4/16/Consolidarea capacității întreprinderilor de economie sociala de a funcționa într-o manieră auto-sustenabilă/16/Consolidarea capacității întreprinderilor de economie sociala de a funcționa într-o manieră auto-sustenabilă

Titlul proiectului: „ANTREPRENORIATUL SOCIAL, SOLUȚIA PENTRU O ECONOMIE DURABILĂ”

Nr. Contract de finanțare: **POCU/449/4/16/128609**

Beneficiar: **Fundația CORPUL EXPERȚILOR ÎN ACCESAREA FONDURILOR STRUCTURALE ȘI DE COEZIUNE EUROPENE**

***PROCEDURA OPERAȚIONALĂ  
PRIVIND PROTECȚIA PERSOANELOR FIZICE ÎN CEEA CE PRIVEȘTE PRELUCRAREA  
DATELOR CU CARACTER PERSONAL ȘI LIBERA CIRCULAȚIE A ACESTOR DATE ÎN  
CADRUL PROIECTULUI  
„ANTREPRENORIATUL SOCIAL, SOLUȚIA PENTRU O ECONOMIE DURABILĂ” –  
POCU 449/4/16/128609***



UNIUNEA EUROPEANĂ



Primăria  
Municipiului  
Câmpina



PRIMĂRIA PLOIEȘTI



ASOCIAȚIA PROFESIONALĂ A  
FORMĂRII ÎN ADMINISTRAȚIA PUBLICĂ LOCALĂ



## CUPRINS

Capitolul 1. Ce este GDPR .....	3
1.1. Documente de referinta .....	3
1.2. Terminologie – definiții, detalierea termenilor, conform GDPR .....	4
Capitolul 2. Tipuri de date cu caracter personal pe care le prelucrează ASSED .....	6
Capitolul 3. Principiile prelucrării datelor cu caracter personal .....	8
3.1. Cum se face informarea persoanei vizate .....	9
3.2. Cand se face informarea .....	9
3.3. Excepții de la obligația de informare .....	9
Capitolul 4. Drepturile persoanei vizate .....	10
4.1. Dreptul de acces la date .....	10
4.2. Dreptul la rectificarea datelor .....	11
4.3. Dreptul la ștergerea datelor .....	11
4.4. Dreptul la restricționarea prelucrării .....	12
4.5. Dreptul de opoziție la prelucrarea datelor .....	12
4.6. Dreptul de a nu fi supus unor decizii automatizate, inclusiv profilarea .....	13
Capitolul 5. Când se poate solicita ștergerea datelor .....	13
5.1. Ștergerea datelor nu este obligatorie în cazul în care prelucrarea este necesară .....	14
Capitolul 6. Mecanisme de raspuns la cererile de exercitare a drepturilor persoanelor vizate .....	14
Capitolul 7. Principalele sarcini ale unui Responsabil cu Protecția Datelor .....	16
Capitolul 8. Confidentialitatea si securitatea datelor .....	19
8.1. Sursa datelor cu caracter personal .....	21
8.2. Categoriile de destinatari ai datelor cu caracter personal .....	22
Capitolul 9. Formulare .....	22





UNIUNEA EUROPEANĂ



GUVERNUL ROMÂNIEI



Instrumente Structurale  
2014-2020

## Capitolul 1. Ce este GDPR

Începând cu data de 25 mai 2018, a intrat în vigoare și se aplică direct în toate statele membre ale Uniunii Europene Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 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, cunoscut și ca GDPR (General Data Protection Regulation).

Regulamentul (UE) 679/2016, în conformitate cu dispozițiile art. 2 alin. (1) din acesta, se aplică prelucrării datelor cu caracter personal, efectuată total sau parțial prin mijloace automatizate, precum și prelucrării prin alte mijloace decât cele automatizate a datelor cu caracter personal care fac parte dintr-un sistem de evidență a datelor sau care sunt destinate să facă parte dintr-un sistem de evidență a datelor.

În calitatea sa de operator de date cu caracter personal, Proiectului „ANTREPRENORIATUL SOCIAL, SOLUȚIA PENTRU O ECONOMIE DURABILĂ”respectă dispozițiile legale privitoare la protecția datelor cu caracter personal și pune în aplicare măsuri tehnice și organizatorice de protejare a tuturor operațiunilor care privesc în mod direct sau indirect datele cu caracter personal și care previn prelucrările neautorizate sau ilegale, precum și pierderile sau distrugerile accidentale sau ilegale.

### 1.1. Documente de referință

- Regulamentul (UE) 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 și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor);
- Legea nr. 190 din 18 iulie 2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 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);
- Directiva (UE) 2016/680 a Parlamentului European și a Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor și privind libera circulație a acestor date și de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului;
- Legea nr. 102 din 3 mai 2005 privind înființarea, organizarea și funcționarea Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal, cu modificările și completările ulterioare;
- Legea nr. 129 din 15 iunie 2018 pentru modificarea și completarea Legii nr. 102/2005 privind înființarea, organizarea și funcționarea Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal, precum și pentru abrogarea Legii nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date;
- Regulamentul de Organizare și Funcționare al ANSPDCP din 11 Noiembrie 2005, cu modificările și completările ulterioare;



REGULAMENTUL DE ORGANIZARE ȘI FUNCȚIONARE



Primăria  
Municipiului  
Câmpina



PRIMĂRIA PLOIEȘTI



ASOCIAȚIA PROFESIONALĂ A  
FORMĂRII ÎN ADMINISTRAȚIA PUBLICĂ LOCALĂ



- Decizia nr. 99 din 18 mai 2018 – ANSPDCP – privind încetarea aplicabilității unor acte normative cu caracter administrativ emise în aplicarea Legii nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date;
- Decizia nr. 128 din 22 iunie 2018 – ANSPDCP – privind aprobarea formularului tipizat al notificării de încălcare a securității datelor cu caracter personal în conformitate cu Regulamentul (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);
- Decizia nr. 133 din 3 iulie 2018 – ANSPDCP – privind aprobarea Procedurii de primire și soluționare a plângerilor;
- Decizia nr. 174 din 18 octombrie 2018 – ANSPDCP – privind lista operațiunilor pentru care este obligatorie realizarea evaluării impactului asupra protecției datelor cu caracter personal;
- Orientări privind Consimțământul în temeiul Regulamentului (UE) 679/2016 (17/RO/WP259);
- Ghidul privind Responsabilul cu protecția datelor (DPO) – (16/RO/WP 243 rev.01, revizuit și adoptat în data de 5 aprilie 2017);
- Ghidul privind Evaluarea impactului asupra protecției datelor (DPIA) și stabilirea dacă o lucrare este „susceptibilă să genereze un risc ridicat” în sensul Regulamentului 2016/679 (17/RO WP 248 rev.01) revizuit și adoptat în data de 4 octombrie 2017;
- Avizul nr. 2/2017 privind prelucrarea datelor la locul de muncă (Articolul 29 – Grupul de lucru pentru protecția datelor 17/RO GL 249), adoptat la 8 iunie 2017.

## 1.2. Terminologie – definiții, detalierea termenilor, conform GDPR

- 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;
- Prelucrarea de date cu caracter personal - înseamnă orice operațiune care se efectuează asupra datelor cu caracter personal, prin mijloace automate sau neautomate în cadrul unor operațiuni ori seturi de operațiuni, fără a fi limitate la acestea, 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.
- Colectarea presupune acțiunea de a strânge, a aduna, a primi date cu caracter personal de la persoanele vizate prin intermediul Proiectului „ANTREPRENORIATUL SOCIAL, SOLUȚIA PENTRU O ECONOMIE DURABILĂ”;
- Înregistrare presupune consemnarea datelor cu caracter personal într-un sistem de evidențiere automată ori neautomată, care poate fi registru, fișier automat, bază de date sau orice altă formă de evidență organizată, structurată ori ad-hoc sau într-un text, înșiruire de date ori document, indiferent de modalitatea în care se înscriu datele;





- Organizarea presupune ordonarea, structurarea sau sistematizarea datelor cu caracter personal, conform unor criterii prestabilite, potrivit atribuțiilor legale ale operatorului, în scopul eficientizării/optimizării activităților de prelucrare a acestora;
- Stocarea presupune păstrarea pe orice fel de suport a datelor cu caracter personal culese, inclusiv prin efectuarea unor copii de siguranță;
- Adaptarea presupune transformarea datelor cu caracter personal colectate inițial, conform criteriilor prestabilite și scopurilor pentru care au fost colectate;
- Modificarea presupune actualizarea, completarea, schimbarea, corectarea ori refacerea datelor cu caracter personal, în scopul menținerii caracteristicilor de exactitate, realitate și actualitate;
- Extragerea presupune scoaterea unei părți din categoria specifică de date cu caracter personal, în scopul utilizării acesteia, separat și distinct de prelucrarea inițială;
- Consultarea presupune examinarea, vizualizarea, interogarea ori cercetarea datelor cu caracter personal fără a fi limitate la acestea, în scopul efectuării unei operațiuni sau set de operațiuni de prelucrare ulterioară;
- Utilizarea presupune folosirea datelor cu caracter personal, în totalitate sau în parte, de către și în interiorul operatorului, împuterniciților operatorului sau destinatarului, după caz, inclusiv prin tipărire, copiere, multiplicare, scanare sau alte procedee similare;
- Dezvăluirea presupune acțiunea de a face disponibile datele cu caracter personal către terți prin comunicare, transmitere, diseminare sau în orice alt mod;
- Alăturarea presupune acțiunea de adăugare, alipire sau anexare a unor date cu caracter personal la cele deja existente, pe care nu le modifică;
- Combinarea presupune îmbinarea, unirea sau asamblarea unor date cu caracter personal separate inițial, într-o formă nouă, pe baza unor criterii prestabilite, pentru scopuri anume determinate;
- Restricționarea presupune limitarea accesului la datele cu caracter personal pentru o perioadă determinată, pentru scopuri anume determinate;
- Ștergerea presupune eliminarea sau înlăturarea, în totalitate sau în parte, a datelor cu caracter personal din evidențe sau înregistrări, prin împlinirea termenului de păstrare, la atingerea scopului pentru care au fost introduse, caducitatea, inexistența ori inexactitatea acestora;
- Transformarea presupune operațiunea efectuată asupra datelor cu caracter personal având ca scop anonimizarea ori utilizarea în scopuri exclusiv statistice;
- Distrugerea presupune aducerea la stare de neîntrebuințare, în condițiile legii, definitivă și irecuperabilă, prin mijloace mecanice sau termice, a suportului fizic pe care au fost prelucrate date cu caracter personal.
- Categoriile speciale de date cu caracter personal – date cu caracter personal care dezvăluie originea rasială sau etnică, opinii politice, convingeri religioase sau filosofice sau apartenența sindicală și prelucrarea datelor genetice, date biometrice în scopul identificării unice a unei persoane fizice, date privind sănătatea sau date privind viața sexuală sau orientarea sexuală a unei persoane fizice.
- Operator de date (Controller)- persoană fizică sau juridică, autoritate publică, agenție sau alt organism care, singur sau în comun cu alții, determină scopurile și mijloacele de prelucrare a datelor cu caracter personal;





- Persoana vizată – orice persoană vie care face obiectul datelor cu caracter personal deținute în cadrul Proiectului „ANTREPRENORIATUL SOCIAL, SOLUȚIA PENTRU O ECONOMIE DURABILĂ”.
- Prelucrare – orice operațiune sau set de operațiuni care vizează date personale sau seturi de date cu caracter personal, indiferent dacă sunt sau nu sunt realizate prin mijloace automate, cum ar fi: colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea, modificarea, recuperarea, divulgarea prin transmitere, diseminare sau punerea la dispoziție prin alt mod, alinierea sau combinarea, restricționarea, ștergerea sau distrugerea acestora.
- 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.
- 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.

Fundatia CORPUL EXPERTILOR IN ACCESAREA FONDURILOR STRUCTURALE SI DE COEZIUNE EUROPENE “CEAFSC” este operator de date și/ sau procesator de date conform prevederilor Regulamentului general privind protecția datelor (GDPR).

Activitățile de prelucrare a datelor cu caracter personal sunt desfășurate în scopul implementării/monitorizării programelor/proiectelor, îndeplinirii obiectivelor acestora, precum și în scop statistic, în conformitatea cu regulamentele europene ce guvernează absorbția fondurilor structurale și de investiții.

## Capitolul 2. Tipuri de date cu caracter personal pe care le prelucrează ASSED

Prelucrează numai datele personale necesare în scopurile menționate și solicită persoanelor vizate comunicarea datelor cu caracter personal strict necesare îndeplinirii acestor scopuri.

Categoriile de date personale (clasice sau digitale) supuse prelucrărilor la nivelul serviciilor/ birourilor/ compartimentelor din cadrul ASSED sunt următoarele:

Pentru relații publice/petiționare/formulare de puncte de vedere la solicitările persoanelor fizice:

- nume, prenume
- semnătură
- detalii de contact – număr de telefon personal, adresă de email, adresa de domiciliu/ reședință etc.,

În mod excepțional:

- serie și număr CI/BI
- CNP

Pentru formulare de acțiuni și reprezentare în instanță:







UNIUNEA EUROPEANĂ



- nume, prenume
- semnătură
- detalii de contact – număr de telefon personal, adresă de email, adresa de domiciliu/ reședință etc.
- serie și număr CI/BI
- CNP

Pentru organizare/derulare evenimente:

- nume, prenume
- funcție, profesie
- denumire angajator
- detalii de contact – număr de telefon personal/ de serviciu, adresă de email, adresă poștală

Pentru accesarea site-ului Ministerului fondurilor Europene

- adresa IP
- tipul de browser folosit

Pentru soluționarea notificărilor de încălcare a securității datelor:

- nume, prenume
- funcție
- detalii de contact – număr de telefon personal/ de serviciu, adresă de email, adresă poștală

Pentru soluționarea plângerilor/ sesizărilor:

- nume, prenume
- semnătura
- detalii de contact – număr de telefon personal, adresă de email, adresa de domiciliu/reședință etc.
- serie și număr CI/BI
- CNP

Pentru încheiere contracte de furnizare de bunuri/ servicii:

- nume, prenume
- funcție
- denumire angajator/ furnizor
- detalii de contact – număr de telefon personal/ de serviciu, adresă de email, adresă poștală

ASSED își rezervă dreptul de a solicita alte date necesare pentru îndeplinirea atribuțiilor persoanelor vizate din cadrul Proiectului, strict în conformitate cu prevederile legale.





### Capitolul 3. Principiile prelucrării datelor cu caracter personal

<ul style="list-style-type: none"><li>• Legalitate, echitate și transparență</li></ul>	<ul style="list-style-type: none"><li>• Datele cu caracter personal vor fi prelucrate în mod legal, echitabil și transparent față de persoana vizată</li></ul>
<ul style="list-style-type: none"><li>• Limitări legate de scop</li></ul>	<ul style="list-style-type: none"><li>• Datele cu caracter personal vor fi colectate în scopuri determinate, explicite și legitime și nu sunt prelucrate ulterior într-un mod incompatibil cu aceste scopuri</li></ul>
<ul style="list-style-type: none"><li>• Reducerea la minimum a datelor</li></ul>	<ul style="list-style-type: none"><li>• Datele cu caracter personal vor fi adecvate, relevante și limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate</li></ul>
<ul style="list-style-type: none"><li>• Exactitate</li></ul>	<ul style="list-style-type: none"><li>• Datele cu caracter personal vor fi exacte și, în cazul în care este necesar, actualizate</li></ul>
<ul style="list-style-type: none"><li>• Limitări legate de stocare</li></ul>	<ul style="list-style-type: none"><li>• Datele cu caracter personal vor fi păstrate într-o formă care permite identificarea persoanei vizate pe o perioadă care nu depășește perioada necesară îndeplinirii scopurilor în care sunt prelucrate datele</li></ul>
<ul style="list-style-type: none"><li>• Integritate și confidențialitate</li></ul>	<ul style="list-style-type: none"><li>• Datele cu caracter personal vor fi 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</li></ul>
<ul style="list-style-type: none"><li>• Responsabilitate</li></ul>	<ul style="list-style-type: none"><li>• Operatorul este responsabil și va trebui să demonstreze conformitatea cu reglementările europene privind protecția datelor cu caracter personal</li></ul>

În virtutea respectării principiului legalității, echității și transparenței, operatorul are obligația de a furniza persoanei vizate o serie de informații.







### 3.1. Cum se face informarea persoanei vizate

- (1) Informarea trebuie oferită într-o formă concisă, transparentă, inteligibilă și ușor accesibilă, utilizând un limbaj clar și simplu.
- (2) Documentul de informare este pus la dispoziția persoanei vizate în forme diferite, depinzând de scopurile prelucrării și de sursa datelor (persoană vizată sau altă sursă): de exemplu, politica de confidențialitate a unui website, anexa la contractul încheiat cu persoana fizică, nota de informare inserată într-un formular de aplicație pentru o poziție în cadrul operatorului etc.
- (3) Ca principiu, nota de informare se livrează în scris inclusiv, atunci când este oportun, în format electronic.
- (4) Pot exista și informări verbale, la solicitarea persoanei vizate, cu condiția ca identitatea persoanei vizate să fie dovedită prin alte mijloace.

### 3.2. Când se face informarea

- (1) În cazul datelor cu caracter personal colectate direct de la persoana vizată, informarea se face în momentul obținerii datelor.
- (2) În cazul datelor cu caracter personal colectate din alte surse, informarea se face:
  - 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 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.

### 3.3. Excepții de la obligația de informare

- Indiferent dacă datele cu caracter personal sunt obținute de la persoana vizată sau din alte surse, informarea nu este necesară dacă și în măsura în care persoana vizată deține deja informațiile respective.
- În plus, pentru cazul particular al prelucrărilor de date cu caracter personal obținute din alte surse, alte excepții de la obligația de informare pot deveni incidente:
- Furnizarea acestor informații se dovedește a fi imposibilă sau ar implica eforturi disproporționate;
- Obținerea sau divulgarea datelor este prevăzută în mod expres de dreptul Uniunii sau de dreptul intern și care prevede măsuri adecvate pentru a proteja interesele legitime ale persoanei vizate;
- 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.

## Capitolul 4. Drepturile persoanei vizate

Regulamentul prevede 8 drepturi specifice în materie de prelucrare a datelor cu caracter personal:

- a) Dreptul de acces la date;
- b) Dreptul la rectificarea datelor;
- c) Dreptul la ștergerea datelor;
- d) Dreptul la restricționarea prelucrării;
- e) Dreptul la portabilitatea datelor;
- f) Dreptul de opoziție la prelucrarea datelor;
- g) Dreptul de a nu fi supus unor decizi automatizate, inclusiv profilarea;
- h) Dreptul la notificarea destinatarilor privind rectificarea, ștergerea ori restricționarea datelor cu caracter personal.

### 4.1. Dreptul de acces la date

Atunci când acționează în calitate de operator, Responsabilul cu protecția datelor din cadrul Proiectului „ANTREPRENORIATUL SOCIAL, SOLUȚIA PENTRU O ECONOMIE DURABILĂ” are obligația, la cererea transmisă pe orice canal de către persoana vizată, de a confirma acesteia ce date prelucrează și în ce condiții.

În cazul în care se solicită accesul la datele cu caracter personal, soluționarea unei astfel de solicitări presupune.

Confirmarea cu privire la operațiunea prelucrării de date (dacă se prelucrează sau nu);

Informații cu privire la:

- Scopurile prelucrării;
- Categoriile de date personale vizate;
- Destinatarii cărora datele personale au fost sau vor fi divulgate (în special destinatari din țări terțe sau organizații internaționale);
- Perioada de stocare a datelor personale (dacă este posibil);
- Existența dreptului la ștergere, rectificare sau restricționare, precum și dreptul de a se opune prelucrării;
- Dreptul de a depune plângere în fața unei autorități de supraveghere;
- Existența unui proces decizional automatizat, inclusiv crearea de profiluri și informații privind logica utilizată și consecințele prelucrării;

Informații cu privire la garanțiile adecvate (când datele sunt transferate către o țară terță sau o organizație internațională);





Copie a datelor care fac obiectul prelucrării. Pentru orice alte copii solicitate de persoana vizată, se poate percepe o taxa rezonabilă, bazată pe costurile administrative, dacă este cazul. 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.

#### 4.2. Dreptul la rectificarea datelor

Când acționează ca operator, Responsabilul cu Protecția Datelor din cadrul Proiectului „ANTREPRENORIATUL SOCIAL, SOLUȚIA PENTRU O ECONOMIE DURABILĂ” are obligația de a asigura respectarea drepturilor persoanei vizate de a obține fără întârziere rectificarea oricăror date inexacte (eronate sau incomplete) care le privesc.

#### 4.3. Dreptul la ștergerea datelor

În cazul în care persoana vizată solicită ștergerea datelor cu caracter personal care o privesc, se va transmite acesteia o declarație în care să se menționeze că toate datele au fost șterse (inclusiv copii sau reproduceri).

În cazul în care Responsabilul cu Protecția Datelor din cadrul Proiectului „ANTREPRENORIATUL SOCIAL, SOLUȚIA PENTRU O ECONOMIE DURABILĂ” a făcut publice datele cu caracter personal și este obligat să le șteargă, ținând seama de tehnologia disponibilă și de costul implementării, Responsabilul cu Protecția Datelor din cadrul Proiectului „ANTREPRENORIATUL SOCIAL, SOLUȚIA PENTRU O ECONOMIE DURABILĂ” 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 link-uri către datele respective sau a oricăror copii sau reproduceri ale acestor date cu caracter personal.





#### 4.4. Dreptul la restricționarea prelucrării

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

#### 4.5. Dreptul de opoziție la prelucrarea datelor

Persoana vizată se poate opune oricând la prelucrarea datelor sale cu caracter personal:

- a) din motive legate de situația particulară în care se află, operațiunilor de prelucrare desfășurate în temeiul necesității prelucrării pentru îndeplinirea unei sarcini care servește unui interes public cu care este investit Responsabilul cu protecția datelor din cadrul Proiectului „ANTREPRENORIATUL SOCIAL, SOLUȚIA PENTRU O ECONOMIE DURABILĂ”; și/ sau prelucrărilor efectuate în temeiul intereselor legitime urmărite de Proiectului „ANTREPRENORIATUL SOCIAL, SOLUȚIA PENTRU O ECONOMIE DURABILĂ” sau de o parte terță a datelor cu caracter personal, inclusiv creării de profiluri.

Responsabilul cu protecția datelor din cadrul Proiectului „ANTREPRENORIATUL SOCIAL, SOLUȚIA PENTRU O ECONOMIE DURABILĂ” nu mai poate prelucra datele cu caracter personal în cazul opunerii, cu excepția cazului în care demonstrează că are motive legitime și imperioase care justifică prelucrarea și care prevalează asupra intereselor, drepturilor și libertăților persoanei vizate sau că scopul prelucrării este constatarea, exercitarea sau apărarea unui





drept în instanță.

#### 4.6. Dreptul de a nu fi supus unor decizii automatizate, inclusiv profilarea

În general, 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.

Prelucrarea datelor pentru luarea de decizii automatizate este permisă când:

- (a) este necesară pentru încheierea sau executarea unui contract între persoana vizată și operatorul de date;
- (b) este autorizată prin dreptul Uniunii sau dreptul intern care prevede, de asemenea, măsuri corespunzătoare pentru protejarea drepturilor, libertăților și intereselor legitime ale persoanei vizate;
- (c) are la bază consimțământul explicit al persoanei vizate.

#### Capitolul 5. Când se poate solicita ștergerea datelor

- a datele cu caracter personal nu mai sunt necesare pentru îndeplinirea pentru care au fost colectate sau
- b persoana vizată își retrage consimțământul pe baza căruia are loc nu există alt temei juridic pentru
- c persoana vizată se opune prelucrării și nu există motive legitime prevaleze în ceea ce privește prelucrarea sau persoana vizată se opune prelucrării, atunci când prelucrarea datelor are drept scop marketingul
- d datele cu caracter personal au fost prelucrate
- e datele cu caracter personal trebuie șterse pentru respectarea unei legale care revine operatorului în temeiul dreptului Uniunii sau al dreptului intern sub incidența căruia se află operatorul;
- f datele cu caracter personal au fost colectate în legătură cu oferirea de societății



### 5.1. Ștergerea datelor nu este obligatorie în cazul în care prelucrarea este necesară

- a) pentru exercitarea dreptului la libera exprimare și la
- b) pentru respectarea unei obligații legale care prevede prelucrarea în dreptul 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, în dispozițiile
- d) în scopuri de arhivare în interes public, în scopuri de cercetare istorică ori în scopuri statistice, în măsura în care dreptul la ștergerea datelor este susceptibil să facă imposibilă sau să afecteze în mod grav realizarea obiectivelor prelucrării respective;
- e) pentru constatarea, exercitarea sau apărarea unui drept în

### Capitolul 6. Mecanisme de raspuns la cererile de exercitare a drepturilor persoanelor vizate

Pentru a asigura tratarea cu celeritate a cererilor persoanei vizate pentru exercitarea drepturilor specifice, respectiv a cererilor altor entități, următoarele mecanisme pot fi avute în vedere:

Alocarea unei / unor persoane care să se ocupe de tratarea în timp util a cererilor persoanelor vizate, care să răspundă în scris la asemenea solicitări;

Redactarea unor formulare de exercitare a drepturilor / răspuns tipizate care să fie utilizate atunci când persoana vizată își exercită drepturile specifice;

Dacă cererile sunt transmise prin mijloace electronice, răspunsul trebuie transmis prin aceleași mijloace, dacă persoanele vizate nu solicită altfel;

Implementarea unor secțiuni specifice pentru exercitarea drepturilor persoanei vizate on-line, în special în cazurile în care colectarea datelor se realizează on-line;

Pentru formele de exercitare cu personal numeros, conceperea unei proceduri specifice cu reguli clare de urmat în cazul primirii unor astfel de cereri, inclusiv cu principiile de avut în vedere în contextul conceperii răspunsurilor la cererile specifice.

În cazul în care există îndoieli întemeiate cu privire la identitatea persoanei fizice care





înaintea cererea pentru exercitarea drepturilor specifice, operatorul poate solicita furnizarea de informații suplimentare necesare pentru a confirma identitatea persoanei vizate.

Soluționarea cererilor se va realiza fără întârzieri nejustificate, în termen de cel mult 1 lună de la data recepționării acestora.

Perioada de soluționare a cererilor poate fi prelungită cu două luni atunci când este necesar, ținându-se seama de complexitatea și numărul cererilor. În acest caz, persoana vizată trebuie să fie informată 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 persoană vizată solicită un alt format.

Dacă nu se iau măsuri cu privire la cererea persoanei vizate, persoana vizată este informată, 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 autorității de supraveghere și de a introduce o cale de atac judiciară.

Informațiile furnizate în temeiul solicitărilor persoanei vizate în exercitarea drepturilor specifice, orice comunicare și orice măsuri luate în temeiul acestora 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:

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

fie să refuze să dea curs cererii.

În aceste cazuri, operatorului îi revine sarcina de a demonstra caracterul vădit nefondat sau excesiv al cererii.

În cadrul Proiectului „ANTREPRENORIATUL SOCIAL, SOLUȚIA PENTRU O ECONOMIE DURABILĂ” se păstrează evidențe clare ale răspunsurilor date în contextul cererilor persoanei vizate de exercitare a drepturilor specifice în materie de prelucrare a datelor cu caracter personal, atât când acționează ca operator, cât și ca persoana împuternicită, astfel:

În cadrul Proiectului „ANTREPRENORIATUL SOCIAL, SOLUȚIA PENTRU O ECONOMIE DURABILĂ” operator trebuie să aibă dovezi clare scrise (conținând inclusiv răspunsurile și data transmiterii acestora) care să ateste îndeplinirea obligațiilor specifice în materie; în atare condiții, păstrarea evidenței se va

realiza pe două paliere: solicitări primite cu toate informațiile aferente cu evidențierea datei primirii acestora și respectiv răspunsuri transmise, cu evidențierea datei transmiterii răspunsurilor, iar unde este cazul de prelungire a termenului de răspuns după o lună, cu indicarea clară a motivului prelungirii;

În cadrul Proiectului „ANTREPRENORIATUL SOCIAL, SOLUȚIA PENTRU O ECONOMIE DURABILĂ” persoană împuternicită trebuie să aibă dovezi scrise care să susțină





transmiterea în termen util a informațiilor solicitate respectiv implementarea în mod rezonabil a măsurilor necesare pentru conformarea cu drepturile specifice ale persoanei vizate a operatorilor care le solicită informații / luarea de măsuri specifice;

De principiu, în cadrul Proiectului „ANTREPRENORIALUL SOCIAL, SOLUȚIA PENTRU O ECONOMIE DURABILĂ” se păstrează dovezile în formă scrisă. Cu toate acestea, dacă persoana vizată solicită anumite informații oral, este admisibilă și păstrarea unor dovezi ale înregistrărilor care să ateste răspunsul acordat unor asemenea solicitări.

## Capitolul 7. Principalele sarcini ale unui Responsabil cu Protecția Datelor (RPD)

### 1. Responsabilul cu protecția datelor are cel puțin următoarele sarcini:

- informarea și consilierea operatorului sau a persoanei împuternicite de operator, 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 ale Uniunii sau drept intern referitoare la protecția datelor;
- monitorizarea respectării prezentului regulament, a altor dispoziții de drept ale Uniunii sau de drept intern referitoare la protecția datelor și a politicilor operatorului sau ale persoanei împuternicite de operator 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;
- furnizarea de consiliere la cerere în ceea ce privește evaluarea impactului asupra protecției datelor și monitorizarea funcționării acesteia;
- cooperarea cu autoritatea de supraveghere;
- asumarea rolului de punct de contact pentru autoritatea de supraveghere privind aspectele legate de prelucrare, inclusiv consultarea prealabilă, precum și, dacă este cazul, consultarea cu privire la orice altă chestiune.

### 2. Regulamentul impune o serie de garanții pe care Fundația CORPUL EXPERTILOR IN ACCESAREA FONDURILOR STRUCTURALE SI DE COEZIUNE EUROPENE “CEAFSCE” trebuie să le ofere RPD în vederea îndeplinirii sarcinilor și rolului acestuia stabilite prin Regulament.

Este implicat în mod corespunzător și în timp util în toate aspectele legate de protecția datelor cu caracter personal	<ul style="list-style-type: none"><li>RPD este invitat să participe în mod regulat la sesiunile conducerii la nivel înalt și la nivel mediu.</li><li>Prezența RPD este recomandată în cazul în care se iau decizii cu</li></ul>
--	---



	<p>implicații asupra protecției datelor. Toate informațiile relevante trebuie să fie transmise RPD în timp util pentru a permite ca acesta să ofere o consiliere corespunzătoare.</p> <ul style="list-style-type: none"><li>• Avizului RPD trebuie să i se acorde întotdeauna o importanță deosebită. În caz de dezacord, ca bună practică, documentarea motivelor pentru care nu a fost urmat avizul RPD.</li><li>• RPD trebuie să fie consultat cu promptitudine imediat ce a avut loc o încălcare a securității datelor sau un alt incident.</li></ul>
<p>I se asigură resursele necesare pentru executarea sarcinilor ce îi revin, precum și accesarea datelor cu caracter personal și a operațiunilor de prelucrare, și pentru menținerea cunoștințelor sale de specialitate</p>	<ul style="list-style-type: none"><li>• Sprijin activ al funcției RPD din partea managementului superior.</li><li>• Timp suficient pentru RPD în vederea îndeplinirii atribuțiilor sale.</li><li>• Sprijin corespunzător în ceea ce privește resursele financiare, infrastructură (sediul, facilitati, echipament) și personal, după caz.</li><li>• Comunicare oficială către toți angajații cu privire la desemnarea RPD astfel încât să se asigure că este cunoscută existența și funcționarea RPD.</li><li>• Accesul necesar la alte servicii precum resurse umane, juridic, IT, securitate etc. astfel încât RPD să beneficieze de un sprijin esențial, reacții și informații din partea altor servicii.</li><li>• Pregătire continuă. RPD trebuie să aibă posibilitatea de a rămâne la curent cu evoluțiile în domeniul</li></ul>

	protecției datelor.
RPD nu primește niciun fel de instrucțiuni în ceea ce privește îndeplinirea sarcinilor sale	<ul style="list-style-type: none"> <li>• În îndeplinirea sarcinilor ce îi revin, RPD nu trebuie să fie instruit cum să se ocupe de o problemă.</li> <li>• Acesta nu trebuie să fie instruit să adopte o anumită perspectivă a problemei legată de legislația privind protecția datelor, de exemplu, o anumită interpretare a legii.</li> <li>• RPD răspunde direct în fața celui mai înalt nivel al conducerii operatorului sau persoanei împuternicite de operator.</li> </ul>
Demiterea sau sancționarea RPD	<ul style="list-style-type: none"> <li>• RPD nu poate să fie demis sau sancționat de operator sau persoana împuternicită de operator pentru îndeplinirea sarcinilor sale.</li> <li>• Sancțiunile sunt interzise potrivit GDPR numai în cazul în care acestea sunt impuse ca urmare a îndeplinirii sarcinilor RPD în calitate de RPD. De exemplu, un RPD nu poate fi demis pentru oferirea unei opinii privind prelucrarea datelor personale.</li> <li>• Un RPD ar putea fi totuși demis, în mod legal, din alte motive decât cele privind îndeplinirea sarcinilor sale în calitate de RPD.</li> </ul>
Poziția de RPD nu trebuie să genereze un conflict de interese	<p>În principiu, RPD nu poate exercita o funcție care îi permite să determine scopurile sau mijloacele unei prelucrări.</p> <p>RPD incompatibil cu o poziție de conducere / de decizie sau în situația în care un RPD extern este rugat să reprezinte operatorul sau persoana împuternicită</p>



	<p>de operator în instanță, în cazurile care implică probleme de protecție a datelor. Bune practici pentru Fundatia CORPUL EXPERTILOR IN ACCESAREA FONDURILOR STRUCTURALE SI DE COEZIUNE EUROPENE “CEAFSCE”:</p> <ul style="list-style-type: none"><li>- să identifice funcțiile ce ar fi incompatibile cu funcția de RPD;</li><li>- să elaboreze norme interne pentru a evita conflictele de interese;</li><li>- să realizeze o declarație în sensul că RPD nu are niciun conflict de interese în ceea ce privește funcția sa;</li><li>- să includă garanții în normele interne ale Fundatia CORPUL EXPERTILOR IN ACCESAREA FONDURILOR STRUCTURALE SI DE COEZIUNE EUROPENE “CEAFSCE” și să se asigure că anunțul de post vacant pentru funcția de RPD sau contractul de prestari servicii este suficient de precis și detaliat pentru a evita conflictul de interese.</li></ul>
--	--

## Capitolul 8. Confidentialitatea și securitatea datelor

1. Operatorul și persoana împuternicită de acesta trebuie să implementeze măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător acestui risc, incluzând printre altele, după caz:

- 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 natura fizică sau tehnică;





- un proces pentru testarea, evaluarea și aprecierea periodice ale eficacității măsurilor tehnice și organizatorice pentru a garanta securitatea prelucrării.

2. Este necesar să se stabilească dacă au fost implementate toate măsurile tehnologice de protecție și organizatorice corespunzătoare în scopul de a se stabili imediat dacă s-a produs o încălcare a securității datelor cu caracter personal și de a se informa cu promptitudine autoritatea de supraveghere și persoana vizată.

Există diferite exemple de încălcări ale securității datelor: atacuri informatice tip ransomware, pierderea cheii de criptare a datelor, nefuncționarea sistemelor informatice, pierderea unor documente, transmiterea unei corespondențe la adresa gresită etc.).

Încălcările de securitate pot avea cauze diferite: de la nefuncționarea sau funcționarea necorespunzătoare a sistemelor informatice până la erori umane.

Este foarte important ca operatorul să se asigure că indiferent de cauza acestuia și forma în care se manifestă, apariția unei breșe de securitate este identificată imediat și adusă în mod corespunzător la cunoștința persoanelor competente să implementeze măsurile care se impun.

Pentru gestionarea incidentelor de securitate, în cadrul proiectului se va desemna una sau mai multe persoane, dacă este cazul, care va acționa pentru gestionarea rapidă și eficientă a incidentelor de securitate a datelor cu caracter personal.

3. În cazul în care are loc o încălcare a securității datelor cu caracter personal, operatorul are obligația de a notifica acest lucru autorității de supraveghere, 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 susceptibilă să genereze un risc pentru drepturile și libertățile persoanelor fizice.

4. Notificarea trimisă autorității de supraveghere conține cel puțin următoarele:

- descrie caracterul încălcării securității datelor cu caracter personal, inclusiv, acolo unde este posibil, categoriile și numărul aproximativ al persoanelor vizate, precum și categoriile și numărul aproximativ al înregistrărilor de date cu caracter personal al persoanelor;
- 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;
- descrie consecințele probabile ale încălcării securității datelor cu caracter personal;







- 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.

5. 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.

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.

Informarea persoanei vizate nu este necesară în cazul în care oricare dintre următoarele condiții este îndeplinită:

- 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;
- Operatorul a luat măsuri ulterioare prin care se asigură ca riscul ridicat pentru drepturile și libertățile persoanei vizate nu mai este susceptibil să se materializeze;
- ar necesita un efort disproporționat; în această situație, se efectuează pe loc o informare publică sau se ia o măsură similară prin care persoana vizată sunt informate într-un mod la fel de eficace.
- Regulamentul nu prescrie un anumit formalism pentru informarea persoanei vizate. Dacă circumstanțele concrete nu reclamă o altă abordare, informarea se va face printr-o comunicare adresată direct persoanei vizate, printr-un mijloc de comunicare corespunzător (poștă electronică).
- 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 acestora și a măsurilor de remediere întreprinse.

### 8.1. Sursa datelor cu caracter personal

ASSED prin serviciile/ birourile/ compartimentele colectează date personale direct de la persoanele vizate sau de la terți (cum ar fi alte instituții ori entități care se adresează ASSED ori alte persoane vizate) sau din documente publice.





## 8.2. Categoriile de destinatari ai datelor cu caracter personal

Datele personale sunt destinate utilizării de către ASSED și sunt comunicate următorilor destinatari, dacă este cazul:

- persoanelor vizate/ reprezentanții legali ai persoanelor vizate;
- angajați;
- împuterniciți ai ASSED (persoane fizice sau juridice);
- parteneri contractuali;
- alte instituții/autorități centrale și locale;
- instanțelor de judecată în vederea formulării de acțiuni și reprezentării în instanță;
- în cadrul activității de organizare/derulare evenimente a ASSED;
- în cadrul activității de investigare/control;
- Auditori interni, externi și internaționali;
- Organe de cercetare penală.

Dezvăluirea datelor către terți se face conform prevederilor legale pentru categoriile de destinatari precizați anterior.

Datele personale sunt stocate pe perioada necesară pentru scopurile menționate mai sus, în vederea efectuării tuturor demersurilor întreprinse pentru susținerea activităților serviciilor/birourilor/compartimentelor din cadrul ASSED, ținând cont de prevederile legislației naționale și europene în domeniu, după care vor fi arhivate potrivit legislației aplicabile.

## Capitolul 9. Formulare

3. Acord GDPR
4. Acord de confinențiate
1. Acord prelucrare date salariat
2. Informare finala persoana vizata

Responsabil protecția datelor cu caracter personal la nivelul Proiectului „ANTREPRENORIATUL SOCIAL, SOLUȚIA PENTRU O ECONOMIE DURABILĂ”

Nume și prenume: Dobre Irina Georgeta

Funcție: Responsabil Protectie Date Si Procesare GT/Ofiter Securitatea Informatiei

