1. ANEXA 1 -

CRITERII DE ANALIZĂ PENTRU DESEMNAREA DPO

Nivelul de expertiză a responsabilului cu protecția datelor nu este în mod expres și strict definit în cadrul RGPD, însă el trebuie să fie proporțional cu sensibilitatea, complexitatea și volumul de date prelucrate de organizație. Astfel, în situația în care o operațiune de prelucrare a datelor este deosebit de complexă sau în cazul în care este implicat un volum mare de date speciale, responsabilul cu protecția datelor poate necesita un nivel mai ridicat de expertiză și suport. Există, de asemenea, diferențe și în funcție de faptul dacă organizația transferă în mod sistematic date cu caracter personal în afara spațiului UE sau dacă, dimpotrivă, astfel de transferuri sunt doar ocazionale. Prin urmare, responsabilul cu protecția datelor trebuie ales cu multă atenție, ținându-se cont de complexitatea aspectelor de protecție a datelor care apar în cadrul organizației.

Calitățile profesionale ce ar trebui luate în considerare la desemnarea unui responsabil cu protecția datelor nu sunt nici ele explicitate în cuprinsul RGPD, însă din interpretarea dispozițiilor sale în spiritul lor se poate deduce că un element relevant ar fi ca persoana respectivă să aibă experiență în legislația și practicile de protecție a datelor la nivel național și european, precum și o înțelegere complexă a RGPD. În același timp, este utilă cunoașterea sectorului de afaceri și a organizării operatorului. Responsabilul cu protecția datelor va trebui, de asemenea, să înțeleagă foarte bine operațiunile de prelucrare efectuate, precum și sistemele de informații și necesitățile de securitate și protecție a datelor operatorului. În cazul unei autorități publice sau a unui organism public, responsabilul cu protecția datelor trebuie să aibă cunoștință și de regulile și procedurile administrative ale organizației respective.

Capacitatea de a îndeplini sarcinile ce revin responsabilului cu protecția datelor trebuie interpretată ca referindu-le atât la calitățile sale personale și la cunoștințe, cât și la poziția lui în cadrul organizației. Calitățile personale trebuie să includă, spre exemplu, integritatea și etica profesională, principala preocupare a responsabilului cu protecția datelor trebuind să fie respectarea RGPD. Responsabilul cu protecția datelor joacă un rol-cheie în promovarea unei adevărate culturi de protecție a datelor în cadrul organizației și ajută la implementarea elementelor esențiale ale RGPD, cum ar fi principiile de prelucrare a datelor, drepturile persoanelor vizate, asigurarea protecției datelor începând cu momentul conceperii și în mod implicit, înregistrarea (cartografierea) activităților de prelucrare, securitatea prelucrării, precum și notificarea încălcărilor de securitate.

Deosebit de importante pentru înțelegerea **poziției responsabilului cu protecția datelor** sunt dispozițiile art. 38 din RGPD, potrivit cărora operatorul sau persoana

împuternicită de operator se asigură **că responsabilul este implicat în mod corespunzător și în timp util în toate aspectele legate de protecția datelor cu caracter personal**.

Este esențial ca responsabilul cu protecția datelor (sau echipa sa) să fie implicat, cât mai devreme posibil, în toate aspectele legate de protecția datelor. Referitor la evaluările impactului asupra protecției datelor, RGPD prevede în mod expres implicarea timpurie a responsabilului și precizează că operatorul îi solicită avizul atunci când efectuează o astfel de evaluare.

Totodată, potrivit art. 38 alin. (3) din RGPD, operatorii/persoanele împuternicite de operatori trebuie să se asigure de faptul **că responsabilul cu protecția datelor nu primește niciun fel de instrucțiuni în ceea ce privește îndeplinirea sarcinilor sale**, garantându-se astfel că responsabilul este în măsură să-și îndeplinească sarcinile cu un **grad suficient de autonomie în cadrul organizației**.

Acest lucru semnifică faptul că, în îndeplinirea sarcinilor specifice care-i revin în temeiul prevederilor RGPD, responsabilul cu protecția datelor nu trebuie să fie instruit asupra modului în care trebuie să se ocupe de o problemă ce-i intră în competență, spre exemplu, ce rezultat ar trebui atins, cum să fie investigată o plângere sau legat de oportunitatea consultării autorității de supraveghere. Mai mult, responsabilul nu trebuie să fie instruit nici sub aspectul adoptării unei anumite perspective a problemei legată de legislația privind protecția datelor (ex. – un anumit mod de interpretare a legislației sectoriale).

În cazul în care operatorul sau persoana împuternicită de operator ia decizii care sunt incompatibile cu RGPD și cu opinia responsabilului cu protecția datelor, acesta din urma ar trebui să aibă posibilitatea de a-și exprima cât se poate de clar punctul de vedere divergent la cel mai înalt nivel de management și persoanelor implicate in luarea deciziilor. Alt fel spus**, responsabilul cu protecția datelor răspunde direct în fața celui mai înalt nivel al conducerii operatorului sau persoanei împuternicite de operator**. O asemenea raportare directă asigură că managementul superior (consiliul de conducere) este conștient de consilierea și recomandările responsabilului cu protecția datelor ca parte a misiunii acestuia de a informa și consilia operatorul sau persoana împuternicită de operator.

Criterii obligatorii pentru un **DPO**	*D/N*	*Comentarii*
Procesarea datelor este făcută de către o autoritate publică (nu judiciară)? *Procesarea datelor este făcută de către un tribunal, judecătorie, etc., dar nu în legătură cu capacitatea sa judiciară ci în legătură cu activitatea sa administrativă (de ex. Tribunale care procesează datele ca și angajator)?*	*DA*	*(dacă răspunsul este DA)* *Este necesar un DPO*
Sunteți o autoritate națională, regională sau locală?		
Îndepliniți sarcini din partea publicului care sunt guvernate de legi private sau publice în sectoare cum ar fi: *– servicii în transportul public* *– apă și energie* *– infrastructură rutieră* *– radiodifuzare servicii publice* *– locuințe sociale* *– comisii disciplinare pentru profesii liberale*		
Activitățile principale ale Organizației ***(controlor sau procesator****) sunt operațiuni de procesare a datelor? Aceste activități necesită monitorizare la scară largă, sistematică și regulară a subiecților vizați?*		*(dacă răspunsul este DA)*
Sunt aceste activități efectuate la intervale aparte pentru o perioadă aparte?		
Se repetă sau sunt repetate la intervale fixe?		
Au loc constant sau periodic?		
Se fac în concordanță cu o strategie sistematică?		
Sunt pre-aranjate, organizate sau metodice?		
Sunt parte a unui plan general de colectare a datelor?		
Fac parte dintr-o strategie?		

Coordonați operațiuni de colectare a datelor de categorii speciale de date sau date referitoare la condamnări penale și delicte sau legate de măsuri de siguranță la scară largă?		*(dacă da, este necesar un DPO)*
Câte persoane vizate sunt implicate?		
Care este volumul de date procesat?		
Cât de variată este informația procesată?		
Cât durează activitatea de procesare?		
Care este permanența activității de procesare?		
Datele procesate conțin categorii speciale cum ar fi: - Origine etnică și rasială - Opinii politice - Convingeri filozofice sau religioase - Apartenența la sindicate - Date genetice - Date Biometrice - Medicale/sănătate - Orientare sexuală - Condamnări penale sau delicte - Măsuri de securitate legate de condamnări penale sau delicte		

***Numirea voluntară a unui* DPO** ** în plus față de cerințele de mai sus*	***D/N***	***Comentarii***
Ați luat în considerare natura si sfera de acțiune a procesării?		
Ați luat în considerare contextul și scopul procesării?		
Ați luat în considerare mărimea, complexitatea și diversitatea procesării față de operațiunile de afaceri?		
Au fost aceste criterii revizuite și luate în considerare în conjuncție cu nivelul de risc acceptabil fața de activitatea organizației în		

legătură cu desemnarea unui DPO *sau ne desemnarea acestuia?*		

Justificare managerială pentru a nu desemna un Responsabil pentru Protecția Datelor (*DPO*):
Articolul 37 GDPR specifică trei cazuri în care organizația trebuie să desemneze on DPO. La acest punct ați putea să specificați printr-o justificare clară, de ce nu este necesar un DPO.

2. ANEXA 2 -

MODEL ORIENTATIV PENTRU DESCRIEREA ATRIBUȚIILOR DE RESPONSABIL CU PROTECȚIA DATELOR CARE URMEAZĂ A FI CUPRINSE ÎN FIȘA POSTULUI

DESCRIEREA SARCINILOR / ATRIBUȚIILOR / ACTIVITĂȚILOR POSTULUI

Responsabilul cu Protecția Datelor are responsabilități privind legislația în vigoare și practicile de protecție a datelor, precum și alte calități profesionale, pentru a se asigura că activitățile Operatorului sau Persoanei Împuternicite de Operator, se derulează în conformitate cu cerințele RGPD-ului UE și a legilor și reglementărilor relevante din România.
Responsabilul cu protecția datelor va raporta, va informa și va consilia cu privire la protecția datelor cu caracter personal în legătură cu legile interne și RGPD direct către directorul general (se va menționa nivelul cel mai înalt).
Responsabilul cu Protecția Datelor se va asigura că este actualizată documentația care demonstrează conformitatea cu RGPD, precum politicile și procedurile. De exemplu, registrul de procesare solicitat în temeiul articolului 30. De asemenea,

Responsabilul cu Protecția Datelor va planifica și programa în mod regulat auditurile de prelucrare a datelor, urmărind activitățile principale pentru a se asigura că acestea respectă RGPD.
Responsabilul cu Protecția Datelor este principalul punct de contact pentru angajați și va lua legătura cu toți membrii personalului în probleme de protecție a datelor.
Sarcinile principale ale responsabilului cu protecția datelor (articolul 39 și considerentul 97):

a) Să informeze și să consilieze toți membrii personalului cu privire la obligația lor de a adera la legislația UE privind RGPD și la legislația națională atunci când se ocupă de datele cu caracter personal.
- ✓ să colecteze informații pentru a identifica operațiunile de prelucrare
- ✓ să analizeze și să verifice conformitatea operațiunilor de prelucrare
- ✓ să informeze, să consilieze și să emită recomandări operatorului sau persoanei împuternicite de operator

b) Să monitorizeze respectarea legislației UE privind RGPD și a legislației naționale.
- ✓ să elaboreze un plan de monitorizare pentru planificarea activităților pentru îndeplinirea conformității cu prevederile legislației pe linia protecției prelucrării datelor cu caracter personal

c) Să consulte și să informeze cu privire la evaluarea impactului privind protecția datelor (DPIA), inclusiv monitorizarea performanței DPIA în raport cu cerințele articolului 35 din RGPD UE.
- ✓ oportunitatea (dacă să se efectueze sau nu evaluarea impactului operațiunilor de prelucrare);
- ✓ ce metodologie să fie uzitată la efectuarea evaluării impactului operațiunilor de prelucrare;
- ✓ dacă efectuarea evaluării impactului operațiunilor de prelucrare să fie în sistem intern sau să fie extern;
- ✓ ce garanții (inclusiv măsuri tehnice și organizatorice) să pună în aplicare pentru reducerea oricăror riscuri la adresa drepturilor, libertăților și intereselor legitime ale persoanelor vizate;
- ✓ dacă evaluarea impactului operațiunilor de prelucrare a fost efectuată în mod corect sau nu și dacă, finalmente, concluziile sale (dacă să continue sau nu prelucrarea și ce garanții să pună în aplicare) respectă RGPD.

d) Să mențină legătura și să coopereze cu Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal.
- ✓ analizează solicitările persoanelor și coordonează elaborarea și transmiterea răspunsului conform prevederilor legale în materie;
- ✓ consultă această Autoritate atunci consideră necesar pentru soluționarea diverselor neconcordanțe existente în prevederile unor legi în raport cu cele ale Regulamentului;

e) Să fie persoana de contact cu Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal cu privire la aspectele legate de prelucrarea datelor cu caracter personal și să consulte autoritatea, dacă este cazul, cu privire la orice alte date cu caracter personal.
- ✓ responsabilul cu protecția datelor este consultat cu promptitudine imediat ce a survenit o încălcare a securității datelor cu caracter personal sau un alt incident

f) Să contribuie la elaborarea și menținerea tuturor politicilor și procedurilor privind protecția datelor în cadrul organizației din care face parte.
- ✓ responsabilul cu protecția datelor este invitat să participe, în mod regulat, la ședințele conducerii la nivel înalt și la nivel mediu;
- ✓ prezența responsabilului cu protecția datelor este efectivă în cazul în care se iau decizii cu implicații asupra protecției datelor. Toate informațiile relevante trebuie să fie transmise responsabilului cu protecția datelor în timp util pentru a permite ca acesta să ofere o consiliere corespunzătoare;
- ✓ avizului responsabilului cu protecția datelor i se acordă întotdeauna o atenție deosebită. În caz de dezacord se recomandă, ca bună practică, documentarea motivelor pentru care nu a fost urmat avizul responsabilului cu protecția datelor;

g) Să consilieze conducerea cu privire la alocarea responsabilităților la nivel intern pentru a sprijini respectarea în permanență a legislației UE și a celei naționale pe linia prelucrării datelor cu caracter personal.
- ✓ coordonează elaborarea și implementarea, la nivelul operatorului, a procedurilor proprii în domeniul măsurilor de protecție a persoanelor cu privire la prelucrarea datelor cu caracter personal conform legislației în domeniu

h) Să se asigure că sunt disponibile și sunt furnizate instruire și conștientizare tuturor membrilor personalului implicat în procesarea operațiunilor referitoare la datele cu caracter personal.
- ✓ instruiește personalul care prelucrează date cu caracter personal referitor la normele și regulile de protecție a persoanelor cu privire la prelucrarea datelor cu caracter personal

i) Să monitorizeze în mod regulat respectarea legislației interne și europene privind protecția datelor prin efectuarea de audituri privind procesele referitoare la datele cu caracter personal și să raporteze directorului general (nivelul cel mai înalt).
- ✓ informează operativ conducerea despre vulnerabilitățile și riscurile semnalate în sistemul de securitate a prelucrării datelor cu caracter personal și propune măsuri pentru înlăturarea acestora;

j) Să fie punctul de contact pentru persoanele vizate în ceea ce privește prelucrarea datelor lor cu caracter personal.

- ✓ verifică și coordonează modul în care se asigură informarea corectă și oportună a tuturor persoanelor vizate care se adresează operatorului cu privire la drepturile și obligațiile ce le revin în domeniul protecției datelor cu caracter personal;
- ✓ coordonează soluționarea și ține evidența cererilor persoanelor vizate;
- ✓ coordonează soluționarea cererilor care implică transferul de date, în condițiile legii;

k) Să monitorizeze respectarea Politicii de protecție a datelor în cadrul organizației și să dezvolte / sfătuiască procedurile de securitate eficientă.

- ✓ verifică modul în care se respectă aplicarea acestei politici în organizație de către toți lucrătorii cu sarcini în domeniu.

l) Să consilieze conducerea cu privire la alocarea responsabilităților în materie de securitate a informațiilor.

- ✓ efectuează prin sondaj, verificări privind modul de aplicare a măsurilor legale de protecție a datelor cu caracter personal, întocmește rapoarte și face propuneri pentru remedierea deficiențelor constatate, pe care le înaintează spre aprobare conducerii operatorului;

m) Să dezvolte / să consilieze cu privire la procedurile formale de raportare a incidentelor (RGPD UE și securitatea informațională) și investigațiilor în temeiul articolelor 33 și 34 din RGPD.

n) Să contribuie la procesul de planificare a continuității afacerii și a procesului de recuperare în caz de dezastru.

- ✓ întocmește împreună cu factorii de decizie Planul de Conformitate cu prevederile RGPD în ce privește prelucrarea datelor cu caracter personal și urmărește îndeplinirea măsurilor planificate

o) Să consilieze și să monitorizeze protejarea managementului înregistrărilor organizaționale.

- ✓ analizează împreună cu Responsabilul pentru securitatea informației măsurile existente pentru protejarea prelucrării datelor cu caracter personal și propun măsuri de îmbunătățire a acestora;

p) Să lucreze cu proprietarii de informații pentru a stabili măsura în care datele cu caracter personal sunt colectate, păstrate și / sau utilizate în organizație și că sunt controlate corespunzător și protejate de pierderea confidențialității, integrității sau disponibilității din orice cauză.

- ✓ efectuează controale periodice planificate și inopinate privind modul de îndeplinire a atribuțiilor personalului care prelucrează date cu caracter personal;

q) Se asigură că înregistrările procesării sunt păstrate în cadrul organizației, așa cum este detaliat în articolul 30 din RGPD.

- ✓ verifică modul de respectare a rubricilor din documentele întocmite;

r) Să informeze operatorul cu privire la obligația de a emite notificări privind confidențialitatea datelor persoanelor vizate în momentul colectării datelor lor cu caracter personal în conformitate cu articolele 13-15.
   - ✓ se asigură de existența informațiilor puse la dispoziția persoanelor vizate cu privire la Politica de Confidențialitate a operatorului și acolo unde este cazul, a Politicii privind utilizarea de Cookies

În funcție de timpul necesar pentru a cerceta domeniul protecției datelor și pentru a lua în considerare zonele potențiale de activitate, următoarele elemente ar putea fi adăugate în mod util în listă.

- să examineze și să evalueze soliditatea, adecvarea și aplicarea securității și altor controale pentru protecția datelor.
- să identifice și să testeze controalele și, dacă este cazul, să propună controale suplimentare care pot fi stabilite pentru a menține confidențialitatea, integritatea și disponibilitatea datelor cu caracter personal.
- să aducă în atenția conducerii superioare a oricăror aspecte care ar putea constitui factori de risc potențiali pentru protejarea adecvată a datelor cu caracter personal în cadrul organizației.

Responsabilul cu Protecția Datelor este autorizat să aibă acces la toate sistemele organizației referitoare la colectarea, prelucrarea și stocarea datelor cu caracter personal în scopul evaluării utilizării și securității datelor cu caracter personal. Responsabilul cu Protecția Datelor poate cere colaborarea întregului personal în îndeplinirea acestor sarcini, inclusiv accesul la sisteme și înregistrări. În cazul în care nu există o cooperare, Responsabilul cu Protecția Datelor va raporta în mod corespunzător conducerii superioare a organizației.

3. ANEXA 3 -

ANTET

APROBAT

Denumire funcție
Nume și prenume

PROCEDURĂ OPERAȚIONALĂ
PRIVIND LUCRUL CU DPO
Cod: .....
Ediția I, .../..../...., Revizia

AVIZAT
PREȘEDINTELE COMISIEI DE MONITORIZARE
nume, prenume, semnătură

VERIFICAT
funcția conducătorului compartimentului
nume, prenume, semnătură

ELABORAT
funcția
nume, prenume, semnătură

CUPRINS

1. SCOPUL PROCEDURII:

Prezenta procedură operațională stabilește etapele și responsabilitățile pentru desfășurarea proceselor de lucru cu DPO

2. DOMENIUL DE APLICARE:

Prezenta procedură se aplică tuturor salariaților XXXX implicați în procese de prelucrare a datelor cu caracter personal, atât ale angajaților proprii cât și persoanelor vizate externe instituției (Cetățeni, Reprezentanți parteneri de contract, Terți).

3. DOCUMENTE DE REFERINȚĂ:

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 (Regulamentul general privind protecția datelor)

LEGE 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)

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 - Republicată

Decizii ale Autorității Naționale pentru Protecția Datelor cu Caracter Personal.

4. DEFINIȚII ȘI ABREVIERI

4.1. DEFINIȚII

4.1.1. **Datele cu caracter personal** - orice informații referitoare la o persoană fizică identificată sau identificabilă („persoană vizată”); o persoană fizică identificabilă este acea persoană care poate fi identificată, direct sau indirect, în special prin referire la un număr de identificare, cum ar fi un nume, număr de identificare, date de localizare, un identificator online, sau la unul sau la mai multe elemente specifice, proprii identității sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale;

4.1.2. **Prelucrarea datelor cu caracter personal -** 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;

4.1.3. **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;

4.1.4. **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;

4.1.5. **RSMSI persoană împuternicită de operator** – Responsabil al Sistemului de Management al Securității Informației și Persoana de Contact desemnată pentru preluarea raportărilor de evenimente/incidente de Securitate;

4.1.6. **Reprezentanți compartimente** – denumire utilizată în prezenta procedură pentru persoanele angajate în următoarele funcții: Șef serviciu/Șef compartiment pentru Juridic, IT, Financiar, HR, etc.

4.2. <u>ABREVIERI</u>

4.2.1. DPO - Responsabil cu Protecția Datelor

4.2.2. GDPR – Regulamentul nr.679 din 27 aprilie 2016

4.2.3. H – Hotărârea Conducătorului Instituției

4.2.4. RSMSI – Responsabil al Sistemului de Management al Securității informației

4.2.5. ANSPDCP – Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal

4.2.6. XXXX – Denumirea instituției (Operatorului de date)

5. <u>DESCRIEREA PROCEDURII</u>

5.1. INTERACȚIUNEA/LUCRUL CU DPO

Toți angajații instituției, în special angajații implicați în procese de prelucrare a datelor cu caracter personal pot interacționa cu DPO în vederea solicitării de suport pentru rezolvarea situațiilor specifice legate de prelucrarea datelor.

Una din interacțiunile principale este legată de rezolvarea cererilor persoanelor vizate atunci când aceștia își exercită un drept conform Regulamentului 2016/679.

Persoanele vizate își pot exercita drepturile prin depunerea unei cereri prin următoarele canale. Matricea responsabilităților este prezentată în tabelul următor:

Canal	HR	Lucrători	Secretara	Superior direct	Reprezentanți compartimente implicate	DPO	Management superior
În fața lucrătorilor		R*, G**		I	R, G**	R, C, G**	I
Mail la adresa gdpr@XXXX.ro					R, G**	R, C, G**	I
Personal prin depunerea cererii la registratura instituției			R*, G**	I	R, G**	R, C, G**	I
Poștă			R*, G**	I	R, G**	R, C, G**	I
Prin intermediul ANSPDCP			R*, G**		R, G**	R, C, G**	I
Prin intermediul compartimentului resurse umane în cazul angajaților	R, G**				R, G**	R, C, G**	I

* condiționat dacă el primește corespondența instituției
** doar pentru activitățile pentru care este responsabil
Legenda:
R – Responsabil – este cel responsabil de realizarea misiunii
G – Gestionar – este cel care gestionează realizarea misiunii, el fiind autoritatea
C – Consultat – este cel consultat, cel care deține calitatea de expert
I – Informat – este informat și notificat asupra rezultatelor, fără a fi consultat.

Prezenta procedură tratează doar lucrul cu DPO al angajaților implicați în procese de prelucrare a datelor și nu procesul aferent activității DPO, acela fiind conform procedurii – Cererea de acces a persoanei vizate la datele cu caracter personal care o privesc

5.2. LUCRUL CU DPO A LUCRĂTORILOR ATUNCI CÂND PERSOANA VIZATĂ ÎȘI EXERCITĂ UNUL DIN DREPTURI - ETAPE

- Atunci când persoana vizată (orice persoană care adresează o cerere în vederea exercitării unui drept conform Regulamentului GDPR), sau un reprezentant al acesteia își exercită unul din drepturi în fața unui lucrător al XXXX, acesta are obligația de a confirma identitatea persoanei vizate și a reprezentantului dacă e cazul prin solicitarea unui document care să ateste identitatea [act identitate, permis de conducere, pașaport, permis de rezidență, etc.], iar în cazul persoanelor reprezentate să solicite documentele care să ateste reprezentarea [document de reprezentare în original, act identitate, permis de conducere, pașaport, permis de rezidență, etc. al reprezentantului, precum și al reprezentatului];
- După confirmarea identității, lucrătorul XXXX are obligația de a realiza o copie a documentului care atestă identitatea persoanei vizate și a îl scana. În cazul persoanelor reprezentate, se va realiza copie scanata și a documentului care atestă reprezentarea, precum și documentului care atestă identitatea reprezentantului;
- Pentru toate cererile exercitate de persoana vizată, lucrătorii XXXX, au obligația de a transmite în scris, la adresa de email *gdpr@XXXX.ro* solicitarea persoanei vizate, precum și copiile scanate menționate anterior. În cc-ul solicitării scrise, lucrătorii XXXX au obligația de a ține informat superiorul direct;
- În cazul în care, DPO nu poate confirma identitatea persoanei vizate sau pe cea a reprezentantului (copia scanată a documentului care atestă identitatea lipsește, copia scanată nu este clară sau lizibilă), DPO solicită lucrătorului XXXX recontactarea persoanei vizate sau reprezentantului dacă e cazul pentru obținerea/reobținerea unui document pentru confirmarea identității;
- Lucrătorii XXXX au obligația de a contacta persoana vizată și a obține informațiile solicitate de DPO;
- După obținerea informațiilor lucrătorii XXXX transmit în scris lui DPO toate informațiile obținute;
- DPO, în vederea rezolvării cererilor persoanelor vizate, colaborează cu toate compartimentele XXXX în vederea obținerii informațiilor necesare pentru rezolvarea cererii în timpul legal – A se vedea 6.4.;

- După rezolvarea cererii persoanei vizate, DPO pregătește răspuns semnat și scanat, pe care îl transmite și lucrătorului care a inițiat cererea, menținând informat superiorul direct al acestuia;
- Lucrătorul XXXX poate contacta telefonic, sau pe e-mail (în cazul în care deține informația) persoana vizată, comunicând răspunsul oficial al XXXX privind cererea adresată, specificând că va primi în scris la adresa indicată în cerere sau în sistem, sau cea din copia actului de identitate și adresa/răspunsul oficial în original;
- DPO, în același timp, transmite persoanei vizate răspunsul oficial al XXXX privind cererea, prin poștă, cu confirmare de primire.

5.3. LUCRUL CU DPO AL SUPERIORILOR DIRECȚI AI LUCRĂTORILOR - ETAPE

- Pe toată perioada desfășurării procesului de rezolvare cerere persoană vizată, superiorul direct al lucrătorului care a inițiat cererea este menținut în cc-ul comunicării pentru informare;
- În cazul în care, superiorul direct are un punct de vedere pe care dorește să îl comunice, acesta are libertatea de a-l exprima, indiferent de stadiul cererii;
- În cazul în care, rezoluția DPO privește rectificarea/ modificarea/ștergerea datelor persoanelor vizate în sistemele la care are acces subalternul, superiorul direct primește de la DPO indicații specifice în acest sens;
- Superiorul direct comunică activitatea lucrătorului precum și alte detalii dacă sunt necesare în vederea realizării operațiilor în sisteme informatice;
- După realizarea operațiilor de rectificare/modificare/ștergere în sistemele la care lucrătorii au acces, superiorul direct informează DPO că operația a avut loc cu succes.

5.4. LUCRUL CU DPO A REPREZENTANȚILOR COMPARTIMENTELOR IMPLICAȚI ÎN PROCESUL DE OBȚINERE INFORMAȚII ÎN VEDEREA REZOLVĂRII CERERILOR PERSOANELOR VIZATE

5.4.1. Termen de răspuns

- Toți reprezentanții compartimentelor implicate în obținerea informațiilor necesare rezolvării cererilor persoanelor vizate, trebuie să respecte timpul de răspuns furnizat de DPO atunci când adresează cererea.

5.4.2. Etapele procesului

- Etapele procesului de mai jos, se aplică indiferent de canalul pe care este primită cererea și indiferent de persoana vizată care o adresează (intern – angajați, externi – cetățeni, etc.)
- După primirea cererii formulate de persoana vizată sau de reprezentant, confirmarea identității și înțelegerea obiectului cererii, DPO solicită în scris informații tuturor reprezentanților compartimentelor care pot fi implicate (în general sunt toate – mai ales dacă este vorba de o cerere de acces la datele cu caracter personal). DPO are obligația de a specifica termenul de răspuns intern, astfel încât să se asigure că termenul final de răspuns nu este depășit. Aceste activități se realizează conform procedurii Cererea de acces a persoanei vizate la datele care o privesc;
- Rezolvarea cererii, ar putea presupune și o întâlnire inițială cu reprezentanții compartimentelor relevante pentru a se parcurge solicitarea, dacă este necesar;
- Reprezentanții compartimentelor care dețin informațiile trebuie să colecteze și să transmită informațiile solicitate până la termenul limită impus de DPO;
- Colectarea poate consta în :
    - ✓ Colectarea datelor specificate de persoane vizată sau
    - ✓ Căutarea tuturor bazelor de date și a tuturor sistemelor de fișiere relevante (fișiere manuale) în cadrul instituției, inclusiv toate fișierele de back-up și arhivate (computerizat sau manual) și toate dosarele și arhivele de e-mail;
- Pe parcursul rezolvării cererii pot fi organizate alte întâlniri pentru a se revizui informațiile;
- DPO poate stabili dacă există informații care pot face obiectul unei exceptări;
- În cazul în care cererea persoanei este una de acces la date, se pot solicita informații despre persoana vizată și terților (operatori asociați, persoane împuternicite de operator, terți operatori) unde se transmit datele;
- Reprezentanții compartimentelor implicate au obligația de a asigura tot suportul necesar, mai ales că aceștia colaborează în mod direct cu terțele părți;
- După obținerea tuturor informațiilor, DPO redactează răspunsul la cererea persoanei vizate conform procedurii Cererea de acces a persoanei vizate la datele care o privesc pe care îl transmite pentru avizare reprezentanților compartimentelor care au fost implicate la soluționarea cererii persoanei vizate.

- Reprezentanții compartimentelor implicate au obligația de a formula observații, comentarii, dacă este cazul și de a acorda avizul răspunsului formulat de DPO.
- DPO, în același timp, transmite persoanei vizate răspunsul oficial al XXXX privind cererea, prin poștă, cu confirmare de primire.
- În cazul în care cererea este inițiată de un angajat al XXXX, DPO transmite răspunsul reprezentantului Resurse Umane care informează angajatul referitor la răspuns.

5.5. LUCRUL CU DPO A REPREZENTANTILOR COMPARTIMENTELOR IMPLICATE IN ACTIUNI CE PRIVESC DATELE/DREPTURILE PERSOANELOR VIZATE

- Drepturile pe care le pot exercita persoanele vizate conform Regulamentului privind protecția datelor sunt:

Drept	Art. Reg.	Definiție	Condiționat de	Informații suplimentare
Dreptul de a fi informat	Art. 13, 14	oferă dreptul persoanei vizate de a fi informată cu privire la datele ce vor fi colectate, scopul, de către cine, unde vor fi transferate datele;	Nu este limitat la nimic – informarea trebuie să conțină datele din sistemele IT, din sistemele de evidență fizică – dosare, sistemele de back-up, arhive electronice sau fizice	Notificarea privind prelucrarea datelor cu caracter personal trebuie să furnizeze toate informațiile relevante.
Dreptul de acces	Art. 15	oferă posibilitatea persoanei vizate de a avea o copie a datelor cu caracter personal pe care o instituție le deține și se referă la ea	Nu este limitat la nimic – informarea trebuie să conțină datele din sistemele IT, din sistemele de evidenta fizică – dosare, sistemele de back-up, arhive electronice sau fizice	Persoanele vizate au dreptul de a ști si vedea datele personale deținute de un operator, precum și de a obține o copie a acestora
Dreptul de rectificare	Art.5(1)(d), 16	oferă posibilitatea persoanei vizate de a solicita corecția sau actualizarea datelor cu caracter personal dacă acestea sunt greșite sau inexacte	-	Persoanele vizate pot solicita rectificarea datelor inexacte sau incomplete
Dreptul la ștergere (dreptul de a fi uitat)	Art.17	oferă posibilitatea persoanei vizate de a solicita ștergerea datelor sale	Consimțământ, Necesitate contractuală	Se poate opune ștergerii în următoarele situații: - pentru exercitarea dreptului la liberă exprimare și la informare; - pentru respectarea unei obligații legale - pentru îndeplinirea unei sarcini executate în interes public sau în cadrul exercitării unei autorități

				oficiale cu care este învestit operatorul - din motive de interes public în domeniul sănătății publice - în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice - pentru constatarea, exercitarea sau apărarea unui drept în instanță
Dreptul de a restricționa prelucrarea	Art.18	oferă posibilitatea persoanei vizate de a solicita întreruperea prelucrării datelor în cazul în care există motive să se procedeze astfel	Dovada că prelucrarea violează drepturile și libertățile fundamentale	-
Notificarea destinatarilor privind rectificarea, ștergerea datelor sau restricționarea prelucrării	Art. 19	Obligația operatorului de a notifica destinatarii referitor la orice rectificare sau ștergere a datelor cu caracter personal sau restricționare a prelucrării efectuate în conformitate cu articolul 16, articolul 17 alineatul (1) și articolul 18, cu excepția cazului în care acest lucru se dovedește imposibil sau presupune eforturi disproporționate.	-	-
Dreptul la portabilitatea	Art. 20	oferă posibilitatea persoanei vizate de a obține datele sale	Consimțământ, Necesitate contractuală. Atenție, datele în	(a) Prelucrarea se bazează pe consimțământ în temeiul

datelor		într-un format structurat, utilizat în mod curent și care poate fi citit automat și are dreptul de a transmite aceste date altui operator	format fizic (pe hârtie) nu sunt incluse	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
Dreptul de a se opune prelucrării	Art. 21	oferă posibilitatea persoanei vizate de a solicita oprirea prelucrării	Motivele prelucrării sunt legitime și imperioase care justifică prelucrarea și prevalează intereselor, drepturilor și libertăților persoanei vizate	-
Dreptul de a se opune prelucrării în scopul marketingului direct	Art.21(2-3)	oferă posibilitatea persoanei vizate de a solicita oprirea prelucrării	-	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
Automatizarea procesului decizional și a profilării	Art. 22	oferă posibilitatea persoanei vizate de a nu face obiectul unei decizii bazate exclusiv pe prelucrarea automată, inclusiv crearea de profiluri, care produce efecte juridice care	-	De obicei, se bazează pe profilarea care are un efect „semnificativ” sau „legal”

		privesc persoana vizată sau o afectează în mod similar într-o măsură semnificativă		
Dreptul de a-și retrage consimțământul oricând	Art. 7 (3)	oferă posibilitatea persoanei vizate de a își retrage consimțământul oricând	Scopul prelucrării trebuie să fie consimțământ, altfel nu are sens	Retragerea consimțământului nu afectează legalitatea prelucrării efectuate pe baza consimțământului înainte de retragerea acestuia
Dreptul de a fi informat cu privire la încălcarea securității datelor	Art. 33	oferă posibilitatea persoanei vizate de a fi informată atunci când încălcarea securității este susceptibilă să genereze un risc ridicat pentru drepturile și libertățile sale.	Încălcarea este susceptibilă să genereze un risc ridicat.	Informarea persoanei vizate nu este necesară atunci când: - operatorul a implementat măsuri de protecție tehnice și organizatorice adecvate - operatorul a luat măsuri ulterioare prin care se asigură că riscul ridicat nu mai este susceptibil să se materializeze; - ar necesita un efort disproporționat. În această situație, se efectuează în loc o informare publică sau se ia o măsură similară
Dreptul la o cale de atac judiciară eficientă împotriva unei autorități de supraveghere	Art. 78	oferă fiecărei persoane fizice sau juridice 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	-	-

Dreptul la o cale de atac judiciară eficientă împotriva unui operator sau unei persoane împuternicite de operator	Art.79	oferă posibilitatea persoanei vizate dreptul de a exercita o cale de atac judiciară eficientă în cazul în care consideră că drepturile de care beneficiază în temeiul GDPR au fost încălcate ca urmare a prelucrării datelor sale cu caracter personal	-	-
Dreptul de a fi reprezentat	Art.80	oferă posibilitatea persoanei vizate de a mandata un organism, o organizație sau o asociație fără scop lucrativ să depună plângerea în numele său, să exercite în numele său drepturile menționate la articolele 77, 78 și 79, precum și să exercite dreptul de a primi despăgubiri menționat la articolul 82	-	-
Dreptul la despăgubiri	Art. 82	oferă posibilitatea persoanei care a suferit un prejudiciu material sau moral ca urmare a unei încălcări a regulamentului GDPR să obțină despăgubiri de la operator sau de la persoana împuternicită de operator pentru prejudiciul suferit	Condiționat de decizia unei autorități competente	-

- Disponibilitatea drepturilor pentru fiecare bază legală este:

Baza legală	Art.	Dreptul la ștergere	Dreptul la portabilitate	Dreptul de a obiecta
Consimțământ	Art. 6 (a)	DA	DA	NU, dar își poate retrage consimțământul
Executarea unui contract	Art. 6 (b)	DA	DA	NU
Obligație legală	Art. 6 (c)	NU	NU	NU
Interes vital	Art. 6 (d)	DA	NU	NU
Interes public	Art. 6 (e)	NU	NU	DA
Interes legitim	Art. 6 (f)	DA	NU	DA

- Având în vedere drepturile persoanelor vizate, precum și disponibilitatea drepturilor pentru fiecare bază legală a prelucrării, atunci când persoana vizată își exercită unul din drepturi, reprezentanții compartimentelor implicate, împreuna cu DPO decid ce trebuie realizat din punct de vedere intern în instituție.
- Reprezentanții compartimentelor implicate în soluționarea cererilor persoanelor vizate colaborează cu DPO pe tot parcursul rezolvării cererii prin punerea la dispoziție a informațiilor necesare, a resurselor umane și tehnice necesare și se asigură că obiectivul este îndeplinit.
- Pe tot parcursul realizării a unor astfel de procese, există suportul și implicarea managementului superior.
- Răspunsul la cererea persoanelor vizate conține și informații referitoare la acțiunile întreprinse în acest sens, ca atare reprezentanții sunt direct responsabili de aceste operații.
- Reprezentanții compartimentelor semnează Lista avizare răspuns la cererea persoanei vizate – Anexa 1.

5.6. LUCRUL DPO CU RSMSI

- Atunci când are loc un eveniment/incident de securitate ce privește date cu caracter personal RSMSI anunță DPO (în acest caz fiind Coordonatorul Echipei

de Răspuns privind Încălcarea datelor cu caracter personal), privind evenimentul/incidentul.

- Pe toată perioada de stopare și implementare de acțiuni corective, RSMSI colaborează în legătură strânsă cu DPO de a identifica acțiuni de stingere a incidentului, acțiuni preventive care ar putea fi implementate, de a măsura eficacitatea acțiunilor de stopare, a implementa măsuri corective și de continuitate adecvate.
- În cazul în care evenimentul/incidentul a dus la o încălcare a datelor cu caracter personal ce trebuie raportată ANSPDPC și persoanelor vizate, RSMSI furnizează informațiile relevante Echipei de Răspuns în caz de Încălcare a Datelor. Informațiile ce trebuie puse la dispoziție sunt conform procedurii - Procedura de răspuns în caz de încălcare a datelor și notificare.
- RSMSI va participa la toate ședințele tehnice relevante soluționării evenimentului/incidentului de securitate ce privește încălcarea datelor cu caracter personal.

5.7. LUCRUL CU DPO A ECHIPEI DE RĂSPUNS ÎN CAZ DE ÎNCĂLCARE A DATELOR

- Echipa de Răspuns în Caz de Încălcare a Datelor este o echipă multi-disciplinară alcătuită din persoane cu experiență și competență din compartimentul IT, Juridic, DPO și Resurse Umane. Echipa răspunde la orice încălcare a datelor suspectă/presupusă, vulnerabilitate de securitate sau incident de securitate (în continuare în text, denumite în mod colectiv: "încălcarea datelor”).
- Echipa de Răspuns în Caz de Încălcare a Datelor este condusă de către DPO. În cazuri excepționale, Echipa de Răspuns poate fi condusă de o altă persoană desemnată managerul XXXX.
- Dacă este necesar, Conducătorul Echipei de Răspuns poate implica părți externe organizației.
- Coordonatorul Echipei de Răspuns, în funcție de încălcarea datelor, poate implica reprezentanții compartimentelor care prelucrează sau sunt în relație directă cu prelucrarea datelor personale afectate de încălcare.
- Reprezentanții compartimentelor implicate suplimentar vor fi anunțați în scris de către DPO că exista o încălcare și suportul lor este necesar.
- Toate persoanele implicate în soluționarea încălcării specifice au obligația de a colabora, a asigura prezența și resurse umane în vederea soluționării încălcării specifice a datelor.
- Soluționarea specifică a fiecărei încălcări se realizează conform proceselor descrise în Procedura de răspuns în caz de încălcare a datelor și notificare.

5.8. **LUCRUL CU DPO A REPREZENTANȚILOR TUTUROR COMPARTIMENTELOR PRIVIND CHESTIUNI LEGATE DE PRELUCRAREA DATELOR CU CARACTER PERSONAL**

5.8.1. Responsabilitatea față de prelucrarea datelor cu caracter personal se extinde la nivelul întregii organizații și este dovedită prin implementarea și aplicarea de politici și proceduri, precum și prin alocarea de resurse astfel încât să se creeze cadrul organizațional și tehnic necesar pentru prelucrarea datelor cu caracter personal.

5.8.2. În toate procesele instituției care presupun:

a) prelucrări de date cu caracter personal
b) punerea în aplicare a politicilor privind protecția datelor
c) formarea și conștientizarea permanentă
d) aprobarea procedurilor în care sunt gestionate date cu caracter personal (exemplu: notificările privind prelucrarea datelor, gestionarea cererilor persoanelor vizate, colectarea și manipularea datelor cu caracter personal, tratarea reclamațiilor, gestionarea incidentelor de securitate, transmiterea datelor terților, etc.)
e) inventarierea datelor cu caracter personal
f) gestionarea riscurilor și problemelor de securitatea a datelor cu caracter personal
g) îndrumări legislative și de reglementare privind chestiunile legate de protecția datelor
h) interpretarea și aplicarea diverselor derogări aplicabile prelucrării datelor
i) realizarea evaluării impactului privind protecția datelor, inclusiv probele de securitate atunci când datele nu se află în premisele instituției
j) partajarea datelor cu operatori asociați, persoane împuternicite de operator, terți
k) gestiunea contractelor din punct de vedere date cu caracter personal
l) punerea în aplicare a practicilor și codurilor privind protecția datelor
m) soluționarea incidentelor privind încălcări ale securității datelor cu caracter personal
n) completarea, depunerea și gestiunea notificărilor autorității de supraveghere,

reprezentanții compartimentelor implicate au obligația de a lucra cu DPO, de a solicita avizul sau revizuirea de către DPO a documentelor

relevante, de a pune la dispoziția DPO toate informațiile necesare și de a întreprinde acțiuni corective și preventive dacă este cazul.

5.9. LUCRUL CU DPO A MANAGEMENTULUI SUPERIOR

- XXXX fiind un operator de date responsabil, recunoaște și susține la nivel de management superior aplicarea principiilor GDPR și asigură că datele cu caracter personal ale angajaților, cetățenilor, colaboratorilor și ale terțelor persoane fizice sunt prelucrate în condiții de integritate, confidențialitate și securitate.
- Managementul superior lucrează cu DPO în general prin organizarea de ședințe periodice de status, sau solicitarea de raportări diverse privind gradul de conformare, raportări diverse privind cererile persoanelor vizate, și orice altă raportare ce ține de protecția datelor cu caracter personal.
- Managementul superior susține prin resurse tehnice, umane sau financiare demersurile inițiate de DPO și de restul compartimentelor în vederea menținerii conforme a sistemului de protecție a datelor cu caracter personal în cadrul instituției.

6. RESPONSABILITĂȚI

6.1. Manager/Director general

- Aprobă prezenta procedură

6.2. Lucrători din compartimentele care intră în relație cu persoana vizată

- Informează persoanele vizate privind prelucrarea datelor cu caracter personal de către XXXX;
- Informează persoanele vizate despre drepturile lor;
- Primește cererile persoanelor vizate și le operează în sistemele informatice;
- Solicită persoanelor vizate, care depun o cerere, un document care să ateste identitatea;
- Transmit cererea persoanei vizate, precum și documentele care atestă identitatea, DPO – ului;
- Informează persoana vizată despre răspunsul la cererea de exercitare a unuia din drepturi;
- Realizează modificări/corecții/ștergeri asupra datelor cu caracter personal în sistemele informatice la care au acces;
- Menține informat superiorul direct atunci când primește o cerere a unei persoane vizate.

***6.3*. Superior direct al lucrătorilor**

- Se menține informat privind cererile persoanelor vizate în fața lucrătorilor;
- Exprimă punct de vedere dacă e cazul atunci când se solicită modificarea/ rectificarea/ ștergerea datelor;
- Asigură suportul necesar lucrătorilor;
- Confirmă că datele au fost modificate/rectificate/șterse cu succes.

***6.4*. Reprezentanți compartimente**

- Punerea în aplicare a politicilor privind protecția și securitatea datelor cu caracter personal în cadrul compartimentului de care este responsabil;
- Realizarea registrelor privind inventarul datelor cu caracter personal cu suport DPO;
- Realizarea evaluării impactului privind protecția datelor cu suport DPO;
- Identificarea riscurilor privind protecția datelor cu suport DPO;
- Avizează procedurile în care sunt gestionate date cu caracter personal;
- Implicare continuă în gestionarea riscurilor și problemelor de securitate a datelor cu caracter personal;
- Solicită îndrumări legislative și de reglementare privind chestiunile legate de protecția datelor în activitatea compartimentului de care este responsabil;
- Solicită aviz DPO și Juridic privind orice clauză contractuală privind protecția datelor;
- Implicat în evaluarea persoanelor împuternicite de operator, operatori asociați, terți;
- Implicat în procesul continuu de conformare la sistemul de management al datelor cu caracter personal implementat în cadrul instituției.

***6.5*. Reprezentant Compartiment Resurse Umane**

- Responsabil de informarea angajaților privind prelucrările de date cu caracter personal pe care le realizează instituția în raport cu angajații proprii;
- Responsabil de obținerea consimțământului angajaților atunci când prelucrarea necesită consimțământ;
- Responsabil de primirea cererilor angajaților privind drepturile acestora;
- Responsabil de transmiterea cererii de exercitare a unui drept al angajaților DPO-ului;
- Responsabil de modificarea/corecția/ștergerea datelor angajaților.

6.6. **Echipa de Răspuns în Caz de Încălcare a Datelor (conform Hotărârii nr...../.....)**

- Validează/triază încălcările de date;
- Asigură o investigație corectă și imparțială (inclusiv a verificărilor digitale, dacă este necesar);
- Inițiază, conduce, documentează și încheie analiza în caz de încălcare de date;
- Identifică cerințele de remediere și urmărește implementarea lor;
- Raportează constatările către top management;
- Coordonează activitatea cu autoritățile corespunzătoare dacă este necesar;
- Coordonează activitățile interne și externe;
- Asigură că persoanele vizate afectate sunt notificate corespunzător – dacă este necesar;
- Analizează fiecare incident înregistrat în Registrul Încălcărilor de Date și, dacă este necesar, recomandă acțiuni corective și preventive;
- Se convoacă pentru fiecare încălcare a datelor cu caracter personal și este condusă de Conducătorul Echipei de Răspuns în Caz de Încălcare a Datelor.

6.7. **DPO**

- Conform contractului de externalizare servicii;
- Coordonarea Echipei de Răspuns în Caz de Încălcare a Datelor.

6.8. **Director executiv**

- Recunoaște și susține la nivel de management superior aplicarea principiilor GDPR și asigură că datele cu caracter personal ale angajaților, cetățenilor, colaboratorilor și ale terților persoane fizice sunt prelucrate în condiții de integritate, confidențialitate și securitate;
- Susține prin resurse tehnice, umane și financiare demersurile inițiate de DPO și de restul compartimentelor în vederea menținerii pentru conformitate a sistemului de protecție a datelor cu caracter personal în cadrul instituției.

6.9. **Auditor intern/Auditor extern (la cererea XXXX)**

- Verifică prin audituri interne modul cum sunt respectate cerințele din prezenta procedură;
- Primul audit va fi efectuat în maximum trei luni de la implementarea prezentei proceduri, ulterior se va reveni la intervalul standard de desfășurare a misiunilor de audit, de minim o dată pe an;

- Întocmește raportul de audit intern și include acțiunile corective, preventive stabilite de auditat;
- Transmite auditat-ului și conducerii organizației în maxim 5 zile de la finalizarea auditului raportul de audit și face recomandări pentru îmbunătățirea procesului;
- În cazuri temeinic justificate se pot contracta auditori externi.

7. DISPOZIȚII FINALE

- Reglementările prezentei proceduri sunt obligatorii și intră în vigoare pentru toți salariații XXXX conform Formularului de distribuire a procedurii de la data aprobării, aceștia fiind obligați să le respecte începând cu data comunicării conținutului.
- Comunicarea se va face prin intermediul Specialistului de Proceduri Operaționale și ISO (acolo unde nu există comunicarea se face prin intermediul RSMSI sau compartiment registratură).
- Instruirea prevederilor prezentei proceduri se va efectua de către managerii de departamente/compartimente urmând ca dovada de instruire să fie transmisă către Specialistul Proceduri Operaționale și ISO (acolo unde nu există comunicarea se face prin intermediul RSMSI sau compartiment registratură) la termenul stabilit de conducerea instituției.
- Nerespectarea de către salariați a oricărei dispoziții conținute în prezenta procedură constituie abatere disciplinară, iar sancțiunea se aplică în conformitate cu prevederile Regulamentului Intern aplicabil. De asemenea angajații răspund patrimonial, în temeiul normelor și principiilor răspunderii civile contractuale, pentru pagubele materiale produse instituției din vina și în legătură cu munca lor, pagube ce provin din nerespectarea obligațiilor prevăzute în prezenta procedură.

8. Formular analiză procedură

Nr.crt	Compartiment	Conducător compartiment	Aviz favorabil		Aviz nefavorabil		
			Semnătura	Data	Observații	Semnătura	Data

9. FORMULAR EVIDENŢĂ MODIFICĂRI

Nr. Crt.	Ed.	Data ediției	Rev.	Data reviziei	Pag.	Descriere modificare	Semnătura conducătorului compartimentului
1	1	…….	0	-	-	Întocmită conform OSGG nr.600/2018	

10. Formular distribuire procedură

Compartiment	Conducător compartiment Nume și prenume	Data primirii	Semnătura	Data retragerii	Data intrării în vigoare a procedurii	Semnătura

4. ANEXA 4 -

PRECIZĂRI
privind modul de completare al INVENTARULUI prelucrărilor de date cu caracter personal

CUM VA FI COMPLETAT TEMPLATE-UL?

1. **Foaia I – Inventar date**

SECȚIUNI A – E – Organizație/departament & procese relevante] - In această secțiune proprietarul procesului va completa numele departamentului și toate procesele și sub-procesele relevante dacă e cazul, care utilizează date personale.

- Departament sau Unitate operativă/Funcția pe care o îndeplinește (exemplu: Departamentul de Resurse Umane se numește Resurse Umane și Administrativ. Pentru a separa activitățile departamentului este de preferat să se introducă numele unității operative și funcția pe care o îndeplinește)
- Numele procesului – se va introduce numele procesului care utilizează date cu caracter personal
- Nume sub-proces – dacă e cazul se va introduce numele sub-procesului care utilizează date cu caracter personal (exemplu: procesul de angajare a unei noi persoane este un proces mare, compus din mai multe sub-procese. Procesul este inițiat de nevoia unui departament de a angaja o nouă persoană. După publicarea anunțului de angajare, departamentul de resurse umane începe a primi aplicații prin diverse canale – prin intermediul site-ului web al organizației, prin intermediul agențiilor de recrutare, prin intermediul site-urilor web de locuri de muncă. Aplicările pentru ocuparea locului de muncă, conțin de obicei CV-ul candidatului și scrisoarea de intenție. Aceste documente conțin date personale)
- Proprietar proces – se va introduce numele responsabilului de proces.

SECȚIUNI F – Z – Detalii date personale – În această secțiune proprietarul procesului va completa informația solicitată de către template referitoare la datele personale procesate în cadrul procesului menționat.

- Numele suportului care conține date personale – poate fi hardware, software, rețele, oameni, documente (electronice, fizice) sau canale de transmitere a documentelor
- Descrierea suportului – descrierea scurtă a suportului care conține datele personale
- Scopul prelucrării datelor cu caracter personal – o valoare va fi selectată din dicționar (verificați foaia 3 din formatul documentului)
- Temeiul prelucrării conform Art. 6 din RGPD – va fi o valoare selectată din dicționar (foaia 4 din formatul documentului)
- Temeiul prelucrării conform Art. 9 din RGPD – va fi o valoare selectată din dicționar (foaia 5 din formatul documentului)
- Datele sunt prelucrate doar în scopurile în care au fost colectate inițial sau și altele? Daca da, menționați / se vor menționa și alte scopuri
- Profilare? - se va specifica dacă datele colectate sunt utilizate în scopuri de profilare așa cum este definit în RGPD
- Volumetria – se va specifica numărul persoanelor vizate de acea prelucrare
- Tipul suportului care conține date personale – poate fi: copie fizică, fișier electronic (specificați tipul), suport media/dispozitiv detașabil (specificați tipul)
- Ale cui date personale sunt colectate, utilizate și procesate? – o valoare va fi selectată din dicționar (foaia 8 din formatul documentului)
- Ce tipuri de date personale sunt colectate, utilizate și procesate? – una sau mai multe valori vor fi selectate din dicționar (foaia 7 din formatul documentului)
- Date personale (Y/N)
- Date personale sensibile (Y/N)
- Date ale clienților sensibile (Y/N)
- Clasificarea datelor – o valoare va fi selectată: Confidențiale, Neconfidențiale, De uz intern
- Integritatea datelor – o valoare va fi selectată: Înaltă, Medie, Joasă
- Disponibilitatea datelor – o valoare va fi selectată: Înaltă, Medie, Joasa
- La cine se afla în custodie (dacă nu este proprietarul procesului)
- Perioada de reținere a datelor cu caracter personal – se va specifica perioada de reținere în ani
- Introduceți numele fiecărei aplicații în cadrul acestui proces care este utilizată pentru a procesa datele personale, dacă este cazul

SECȚIUNI AA – AD – Nivelul curent de protecție – În această secțiune proprietarul procesului, cu ajutorul Departamentului de IT Suport (dacă e cazul) va completa nivelul curent de protecție al datelor cu caracter personal procesate în cadrul procesului.

- La origine (descriere) – atunci când informația este primită sau creată)

Pentru copie tipărită:

Păstrați în seiful ignifug
Țineți sub cheie tot timpul
Țineți sub cheie peste noapte
Țineți în dulap / depozit (nu este blocat)
Păstrat pe birou
...

Pentru copia electronică:
Stocat pe unitățile locale pe laptop neprotejat
Stocat pe unitățile locale pe laptop, fișierul este protejat prin parolă
Stocat pe unitatea de rețea de pe laptop neprotejat
Stocat pe unitatea de rețea de pe laptop, fișierul este protejat prin parolă
Stocat pe PC neprotejat
Stocat pe PC, fișierul este protejat prin parolă
Stocat pe laptop criptat sau PC

- Daca informația este mutată (descriere) – atunci când informația este mutată sau arhivată)
  a) Unde este mutată informația

  b) Nivelul de protecție în noua locație

Pentru copie tipărită:
Păstrați în seiful ignifug
Țineți sub cheie tot timpul
Țineți sub cheie peste noapte
Țineți în dulap / depozit (nu este blocat)
Păstrat pe birou
...

Pentru copia electronică:
Stocat pe unitățile locale pe laptop neprotejat
Stocat pe unitățile locale pe laptop, fișierul este protejat prin parolă
Stocat pe unitatea de rețea de pe laptop neprotejat
Stocat pe unitatea de rețea de pe laptop, fișierul este protejat prin parolă
Stocat pe PC neprotejat
Stocat pe PC, fișierul este protejat prin parolă
Stocat pe laptop criptat sau PC
Alte măsuri de protecție – dacă e cazul.

2. **Foaia II – Alte întrebări**

SECȚIUNI A – E - Organizație/departament & procese relevante – Această secțiune trebuie să fie asemănătoare cu cea din Foaia 1. Această Foaie reprezintă o extindere a celei anterioare.

SECȚIUNI F – G – Întinderea procesului – În această secțiune proprietarul procesului va specifica dacă procesul se desfășoară doar la nivelul subsidiarei din România sau la nivelul subsidiarei din România și subsidiarei din altă țară

- Procesul se desfășoară doar la nivelul subsidiarei din România sau la nivelul subsidiarei din România și subsidiarei din alta țară (Y – România/N – România și altă țară
- Vă rugăm furnizați locația subsidiarei – Se va selecta una sau mai multe valori din dicționar (foaia 11 din formatul documentului)

SECȚIUNI H – K –Sursele de date cu caracter personal – În această secțiune proprietarul procesului va specifica sursele de date folosite în procesul curent

- Oricare din datele personale colectate, utilizate sau procesate provin de la persoane cu vârsta sub 16 ani? (Y/N)
- Cumpărați sau utilizați licență pentru datele cu caracter personal (gratuit sau în schimbul unei plăți) de la terțe părți? (Y/N)
- Vă rugăm furnizați numele terților părți de unde cumpărați sau licențiați date cu caracter personal

SECȚIUNI L – U – Schimb de date cu caracter personal – În această secțiune proprietarul procesului va specifica dacă pe procesul curent are loc un schimb de date cu caracter personal

- Identificați filialele companiei în care colegii sau alți lucrători primesc sau au acces la datele personale utilizate în procesul dvs. de afaceri. Notă: accesul este definit ca fiind capabil să "vadă" datele.
- Pentru ce scopuri colegii sau alți lucrători au acces la datele cu caracter personal. Va fi o descriere
- Terțe părți primesc sau au acces la datele cu caracter personal? (Y/N)
- Vă rugăm furnizați numele furnizorului care are acces la datele cu caracter personal
- În ce țară/i primește sau are acces acest furnizor la datele cu caracter personal
- Partenerii de afaceri (de exemplu, joint venture sau colaboratorii sau subcontractanții) primesc sau au acces la datele personale? Notă: accesul este definit ca fiind capabil să "vadă" datele. (Y/N)
- Vă rugăm să furnizați numele partenerilor care primesc sau au acces la datele cu caracter personal
- În ce țară/i primește sau are acces acest partener la datele cu caracter personal

- ❖ Faceți schimb de date cu caracter personal cu agenții guvernamentale, ca de exemplu sistemul național de sănătate, o agenție de protecție socială, etc.
- ❖ Vă rugăm să furnizați numele agenției/agențiilor guvernamentale cu care faceți schimburi de date cu caracter personal

5. ANEXA 5 -

ANTET

NOTA DE INFORMARE PERSOANE VIZATE

Conform cerințelor Regulamentului (UE) 2016/679/27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și

privind libera circulație a acestor date, XXXX are obligația de a administra în condiții de siguranță și numai pentru scopurile specificate, datele personale pe care ni le furnizați despre dumneavoastră, un membru al familiei dumneavoastră ori o altă persoană.

XXXX colectează și prelucrează date cu caracter personal în următoarele scopuri:

a) <u>specifice domeniului de activitate al proiectului .....:</u>
   - ……..
   - ……
b) <u>în scopuri administrative:</u>
   a. evidența petenților;
   b. gestiune economico-financiară;
   c. resurse umane;

Datele dumneavoastră ne sunt necesare în scopul derulării activităților din cadrul proiectului în condiții de eligibilitate. Refuzul dumneavoastră de a furniza anumite date poate determina imposibilitatea furnizării de către XXXX a serviciilor prevăzute în proiect.

Informațiile înregistrate sunt destinate utilizării de către XXXX și sunt comunicate numai următorilor destinatari: angajații desemnați ai organizației, persoana vizată, parteneri contractuali ai organizației, instituții publice autorizate să prelucreze date cu caracter personal (de ex. AM, ANAF, REVISAL, etc.).

Aveți oricând posibilitatea să vă retrageți acest consimțământ și să vă bucurați în continuare de serviciile asigurate prin proiect.

Conform Regulamentului (UE) 2016/679/27 aprilie 2016, beneficiați de:

- dreptul la transparență,
- dreptul de a fi informat,
- dreptul de acces la date,
- dreptul la rectificare,
- dreptul la ștergerea datelor („dreptul de a fi uitat”)*,
- dreptul la restricționarea prelucrării,
- dreptul la portabilitatea datelor,
- dreptul de a nu fi supus unei decizii automate (inclusiv crearea de profiluri),
- dreptul de a se adresa justiției/ ANSPDCP.

Pentru exercitarea acestor drepturi, vă puteți adresa cu o cerere scrisă, datată și semnată la sediul XXXX din ……. sau la email …….@.....

Datele sunt colectate direct de la dumneavoastră, membrii ai familiei, ori împuterniciți în cadrul unor relații de muncă (de către organizația unde lucrați) sau dacă faceți parte din grupul țintă al proiectului. Ele se colectează fie direct (de ex. prin completarea documentelor de angajare sau participare la diverse activități din cadrul proiectului), fie în cadrul unui raport comercial încheiat de organizația beneficiară a proiectului și partenerii săi de contract angrenați în realizarea acestuia.

În cazul în care datele dumneavoastră sunt transferate pe teritoriul Uniunii Europene sau al altor țări din afara acesteia ne asigurăm că și acestea respectă prevederile legale privind protecția datelor cu caracter personal și există o legislație compatibilă și acceptată de Uniunea Europeană.

Pentru mai multe detalii privind prelucrarea datelor cu caracter personal, vă rugăm să accesați site-ul nostru și să descoperiți rubrica de Politică de Confidențialitate.

Observație:
*orice persoană are dreptul de a se opune, pentru motive legitime, la prelucrarea datelor ce o privesc. Acest drept de opoziție poate fi exclus pentru anumite prelucrări prevăzute de lege (de ex.: prelucrări efectuate de serviciile financiare și fiscale, de politie, justiție, securitate socială sau legislația europeană pe linia acordării fondurilor de finanțare a proiectelor).

Prin urmare, această mențiune nu poate figura dacă prelucrarea are un caracter obligatoriu;

XXXX

6. ANEXA 6 -

ANTET

DECLARAŢIE

cu privire la prelucrarea și transmiterea datelor cu caracter personal

Subsemnatul/a_____,
CNP_____, posesor al BI/CI/Pașaport cu seria ____, nr. _____, eliberat de _____, la data de __ .__ ._____, domiciliat în localitatea _____, adresa _____,
În conformitate cu prevederile legale incidente în materia protecției prelucrării datelor cu caracter personal, declar pe propria răspundere că sunt de acord cu

prelucrarea și stocarea datelor cu caracter personal pe care le furnizez, în proiectul finanțat de _____yyy_____, în scopul desfășurării proiectului, scopuri statistice și studii de cercetare, de către _____xxx_____.
Titlul proiectului: .....
Am luat la cunoștință faptul că în conformitate cu prevederile legale în vigoare, am drept de acces, rectificare, ștergere, restricționare, opoziție portabilitate datelor și de a nu face obiectul unui proces individual automatizat, inclusiv crearea de profiluri. De asemenea, cunosc faptul că pot să-mi exercit aceste drepturi adresându-mă __xxx_____ conform legislației în vigoare privind protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date.
De asemenea, declar că sunt de acord cu transmiterea datelor cu caracter personal către _____yyy_____, conform legislației specifice pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date.
De asemenea, sunt de acord cu prelucrarea ulterioară încheierii programului/proiectului sau acțiunii, a datelor mele personale de către _____xxx_____ în scopuri statistice și de arhivare.
Am luat la cunoștință de faptul că pot să-mi retrag oricând prezentul consimțământ și că revocarea acestuia nu afectează legalitatea utilizării datelor înainte de retragerea consimțământului (nu are efect retroactiv).

Nume și prenume _____

Semnătura _____ Data _____

Abrevieri:
xxx beneficiar proiect
yyy finanțatorul proiectului

7. ANEXA 7 -

ANTET INSTITUȚIE

APROBAT

Denumire funcție
Nume și prenume

PROCEDURĂ *OPERAȚIONALĂ*
PRIVIND *CEREREA DE ACCES A PERSOANEI VIZATE LA DATELE CU CARACTER PERSONAL CARE O PRIVESC*
Cod: .....
Ediția I, .../..../...., Revizia

AVIZAT
PREȘEDINTELE COMISIEI DE MONITORIZARE
nume, prenume, semnătură

VERIFICAT
funcția conducătorului compartimentului
nume, prenume, semnătură

ELABORAT
funcția
nume, prenume, semnătură

CUPRINS

11. SCOPUL PROCEDURII:

- Stabilirea regulilor care trebuie respectate pentru soluționarea cererilor de acces a persoanelor vizate la datele personale deținute și prelucrate de XXXX, în termenul prevăzut de lege și cu respectarea prevederilor legale privind protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date;
- Stabilirea responsabilităților privind întocmirea, avizarea și aprobarea documentelor aferente acestor activități.

12. DOMENIUL DE APLICARE:

Prezenta procedură se aplică activității de primire și soluționare a cererilor de acces la datele personale, de către toate persoanele cu atribuții în acest sens.

13. REFERINȚE NORMATIVE:

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 (Regulamentul general privind protecția datelor)

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 - Republicată

LEGE 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)

Legea nr. 682 din 28 noiembrie 2001 privind ratificarea Convenției pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal, adoptată la Strasbourg la 28 ianuarie 1981

Legea nr. 506 din 17 noiembrie 2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice.

14. DEFINIȚII ȘI ABREVIERI

XXXX – denumirea organizației

15. DESCRIEREA PROCEDURII

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 are ca scop protejarea drepturilor și libertăților fundamentale ale persoanelor fizice, ale căror date personale sunt colectate, înregistrate, stocate sau dezvăluite. Conform art.15 din Regulament, persoanele fizice au dreptul de a obține informații despre datele personale proprii pe care le prelucrează operatorul, atât prin mijloace automate, cât și pe baza sistemelor de evidență manuale inclusiv stocate*(inclusiv imaginile stocate în procesul de supraveghere video – acolo unde este cazul)*.

Dreptul de acces al persoanei vizate

(1) Persoana vizată are dreptul de a obține din partea operatorului o confirmare că se prelucrează 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, menționat la articolul 22 alineatele (1) și (4), 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 în temeiul articolului 46 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.

Definiții:

- **date cu caracter personal** - orice informații referitoare la o persoană fizică identificată sau identificabilă („persoană vizată”); o persoană fizică identificabilă este acea persoană care poate fi identificată, direct sau indirect, în special prin referire la un număr de identificare, cum ar fi un nume, număr de identificare, date de localizare, un identificator online, sau la unul sau la mai multe elemente specifice, proprii identității sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale;

- **persoana vizată** - persoana ale cărei date personale sunt prelucrate și stocate în bazele de date/ sistemele de evidență manuale/automate ale XXXX
- **cerere de acces a persoanei vizate** - cererea scrisă, semnată și datată, prin care persoana vizată își exercită dreptul de acces la „datele personale" deținute și prelucrate de operator, drept prevăzut de Regulamentul 679/2016 —art. 15.

15.1. GESTIONAREA CERERII

În sensul prezentei proceduri, cerere de acces a persoanei vizate poate însemna orice cerere scrisă prin care o persoană solicită informații despre datele personale care o privesc sau despre datele personale ale altei persoane pe care o reprezintă în mod legal, cereri soluționate în fluxul normal al îndeplinirii atribuțiilor de serviciu.

În activitățile desfășurate pentru îndeplinirea atribuțiilor curente, anumite servicii/compartimente gestionează deja un volum considerabil de solicitări/petiții/cereri de comunicare a unor informații personale și aplică proceduri specifice pre-existente pentru soluționarea acestora, fără a fi necesară clasificarea acestor cereri ca cereri de acces în sensul Regulamentului 679/2016. Aceste servicii/compartimente vor prelucra petițiile/ cererile de comunicare a informațiilor personale, care le sunt repartizate conform competențelor, respectând prevederile legale de protecție a persoanelor în activitatea de prelucrare a datelor personale, precum și dispozițiile prezentei proceduri. De asemenea, vor ține evidența acestor cereri și modul de soluționare în Registrul de Evidență special introdus pentru această activitate. Lunar, pe data de 5 ale fiecărei luni, serviciile/compartimentele cu atribuții în soluționarea cererilor de acces la date personale vor informa Compartimentul de Protecție a Datelor Personale sau Responsabilul cu protecția datelor cu privire la numărul acestor cereri și stadiul soluționării, furnizând și copii ale documentelor rezultate (cererea de acces, răspunsul către persoana vizată).

Cererea de acces a persoanei vizate poate fi depusă în formă scrisă la Ghișeul de relații cu publicul/Registratura instituției, prin completarea formularului dedicat, sau poate fi trimisă prin poștă în orice formă scrisă, în ambele situații va fi înregistrată de către Ghișeul de relații cu publicul/Registratura instituției și repartizată serviciilor/compartimentelor competente.

Dacă **cererea de acces a persoanei vizate** se face explicit în baza dreptului de acces prevăzut la art. 15 din Regulamentul 679/2016, și/sau pe formularul tip, cererea va fi direcționată către Responsabilul cu Protecția Datelor. În cazul în care datele solicitate de persoana vizată (sau de reprezentantul legal al acesteia) implică pentru soluționare mai multe servicii/compartimente, Responsabilul cu Protecția Datelor va trimite copii ale cererii/formularului de cerere la toate serviciile/compartimentele implicate. Aceste copii vor fi semnate de către Responsabilul cu Protecția Datelor și vor conține termenul de soluționare, astfel încât

să nu se depășească termenul limită de răspuns. Toate serviciile/compartimentele care primesc o copie a acestei cereri o vor prelucra în termenul menționat și vor remite răspunsul Responsabilului cu Protecția Datelor. Responsabilul cu Protecția Datelor are ca sarcină prelucrarea răspunsurilor primite de la serviciile/compartimentele implicate, astfel încât să remită persoanei vizate un răspuns complet în termenul legal de 30 de zile.

Evidența centralizată a cererilor de acces la date personale se ține de către Responsabilul de Protecție a Datelor în Registrul Cererilor de Acces (model Anexa 6).

În cazul în care solicitarea scrisă de acces la datele personale, nu conține toate informațiile necesare pentru:

a. identificarea corectă a persoanei vizate (sau a reprezentantului legal)
b. identificarea adecvată a datelor solicitate sau a locației lor,

Responsabilul cu Protecția Datelor sau serviciul/compartimentul căruia i s-a repartizat spre soluționare cererea, după caz, va contacta, în scris, solicitantul (persoana vizată sau reprezentantul legal) pentru a-i comunica (model Anexa 3) problema apărută și a-l informa că pentru soluționarea cererii este necesară furnizarea tuturor informațiilor cuprinse în formularul de cerere acces (model Anexa 5) pe care îl poate găsi la ghișeul de relații cu publicul sau on-line pe site-ul instituției.

În cazul în care solicitarea inițială de acces la datele personale se face telefonic, serviciul/compartimentul care va recepționa cererea are obligația să comunice persoanei vizate că dreptul de acces se poate exercita doar prin depunerea unei cereri în formă scrisă, datată și semnată și va informa persoana vizată asupra locației unde poate găsi formularul corespunzător. Se vor înscrie în Registrul de Evidență data, numele și prenumele persoanei care a făcut solicitarea și modul de soluționare (în speță: amânare acces, date incomplete) iar printr-o notă de informare se vor transmite datele Responsabilului cu Protecția Datelor.

Informațiile incluse în răspunsul elaborat, pentru a fi trimis persoanei vizate, nu vor conține nici un fel de date despre o terță persoană sau care să permită persoanei vizate să identifice o terță persoană — cu excepția cazului în care a fost obținut consimțământul expres și neechivoc al terței persoane.

În situația în care persoana vizată solicită a doua oară sau de mai multe ori în decursul aceluiași an accesul la datele personale care o privesc în temeiul Regulamentului 679/2016, aceasta va trebui să achite taxele, eferente furnizării de date, stabilite conform prevederilor legale la nivelul instituției.

15.2. PRELUCRAREA CERERII DE ACCES A PERSOANEI VIZATE ȘI COLECTAREA INFORMAȚIILOR

15.2.1. <u>Cine poate face o cerere de acces?</u>

Cererea de acces poate fi făcută de:

- persoana vizată (inclusiv personalul angajat al instituției)
- reprezentantul legal al persoanei vizate

15.2.2. Ce se consideră a fi o cerere de acces validă?

- Criterii

Cererea de acces trebuie să fie în formă scrisă, datată și semnată, redactată fie individual, fie prin completarea formularului tip adoptat prin această procedură. Ea va cuprinde următoarele elemente:

- informații suficiente astfel încât operatorul să poată identifica și localiza datele solicitate
- informații suficiente care să satisfacă cerința de verificare a identității persoanei vizate
- consimțământul expres și neechivoc al persoanei vizate
- informații care să indice faptul că invocă dreptul de acces prevăzut de Regulamentul 679/2016 (menționarea Regulamentului 679/2016, Legii 190/2018 sau a ”dreptului legal de acces")

- Informații obligatorii pentru exercitarea dreptului legal de acces la date personale:
  - Detalii privind persoana vizată:
    - ✓ numele și prenumele (nume anterior)
    - ✓ adresa completă
    - ✓ data și locul nașterii
    - ✓ CNP
    - ✓ Telefon
    - ✓ adresa de email (opțional)
    - ✓ o scurtă descriere a datelor/informațiilor solicitate
  - Numele, prenumele și adresa completă a reprezentantului legal (dacă este cazul)
  - Dovada identității (vezi următorul paragraf)

15.2.3. Verificarea identității persoanei vizate

Verificarea identității solicitantului (persoana vizată sau reprezentantul legal) este obligatorie și se va face:

- fie prin verificare directă la ghișeu/registratură, caz în care persoana care va prelua cererea va confirma identitatea persoanei vizate pe baza confruntării cu documentele de identitate furnizate,
- fie prin verificare ulterioară de către serviciile/compartimentele implicate în soluționarea cererii.

Verificarea identității solicitantului este necesară în scopul:

- de a obține o dovadă certă a identității solicitantului;
- de a obține o dovadă certă a relației dintre solicitant și persoana vizată, acolo unde cererea se face în numele persoanei vizate;
- de a proteja informațiile împotriva unui acces neautorizat sau ilegal;
- de a asigura persoana vizată că operatorul își ia toate măsurile tehnice și organizatorice pentru a păstra confidențialitatea datelor cu caracter personal; și
- de a evita consumul de timp și resurse pentru prelucrarea informațiilor ce urmează a fi comunicate, în cazul în care există și cea mai mică posibilitate de a nu obține o identificare satisfăcătoare la finalul procesului.

Certificarea identității se face pe baza:

- BI/ CI sau certificat de naștere (după caz) (vezi tabel mai jos)

Certificarea accesului autorizat la datele personale ale unui minor (persoana vizată) se face pe baza certificatului de naștere.

În cazul în care există suspiciuni serioase că o persoană încearcă să obțină date personale prin substituire de identitate sau că nu ar avea dreptul de acces la datele personale din motive de siguranță a persoanei vizate, operatorul trebuie să adopte măsuri în consecință. Astfel, serviciul/compartimentul implicat în preluarea cererii va urma procedura existentă și va informa Responsabilul cu Protecția Datelor.

Certificarea identității se face la ghișeu/registratură. În cazul în care solicitarea este primită prin poștă, verificarea identității se va face de către fiecare serviciu/compartiment implicat în soluționarea cererii.

CERINȚE PENTRU IDENTIFICARE

Cerere de acces a persoanei vizate, sub incidența Regulamentului 679/2016

Solicitant	**Documente necesare identificării**
Persoana vizată care solicită accesul la datele personale care o privesc	• Copie a actului de identitate • Copie certificat naștere
Reprezentant legal al persoanei vizate	• Copie act identitate al reprezentantului legal • Împuternicire notarială
Părinții minorului care solicită în numele minorului	• Copie a certificatului de naștere • Acte identitate părinți
Avocat împuternicit de persoana vizată	• Împuternicire avocațională • Copie a actului de identitate a persoanei vizate • Consimțământul expres și neechivoc al persoanei vizate

15.2.4. Preluarea cererii de acces

Cererea de acces se poate depune la Ghișeul de Relații cu Publicul/Registratura instituției sau se poate trimite prin poștă la adresa afișată pe site-ul XXXX.

15.2.5. Fixarea termenului de răspuns

La preluarea cererii se va nota data primirii, precum și numele și prenumele persoanei solicitante, astfel încât să se poată monitoriza timpul de răspuns. Pe copia cererii se va nota data limită la care răspunsul trebuie trimis persoanei vizate. Conform reglementărilor legale în vigoare operatorul este obligat să răspundă solicitantului în termen de 30 de zile.

15.2.6. Repartizarea cererii spre soluționare

a. În cazul în care cererea se face în exercitarea „dreptului legal de acces" pe baza art. 15 din Regulamentul 679/2016, Registratura instituției o va repartiza Responsabilului cu Protecția Datelor.
b. Celelalte situații de solicitare a datelor personale de către persoana vizată se înscriu în activitățile curente ale XXXX și vor fi repartizate serviciilor/compartimentelor competente să le soluționeze, conform atribuțiilor stabilite prin R.O.F, pe baza procedurilor proprii.

Pot exista situații în care o cerere de informații personale este mai complexă și necesită un răspuns coordonat de Responsabilul cu Protecția Datelor. Din practica curentă, asemenea solicitări sunt puțin frecvente.
Exemple de situații care pot implica solicitări complexe:

- Cererea presupune colectarea informațiilor din mai multe surse (servicii/compartimente ale XXXX)
- Cererea presupune dezvăluirea datelor despre terți, care nu și-au dat consimțământul sau care nu pot fi contactați pentru luarea consimțământului.

➢ **Localizarea informațiilor solicitate**

În situația menționată la punctul 2.6. - a., Responsabilul cu Protecția Datelor va identifica serviciile/compartimentele care dețin informații despre persoana vizată și va trimite acestora o cerere spre soluționare însoțită de o copie a cererii de acces. (model Anexa 1)

15.3. ELABORAREA RĂSPUNSULUI

În orice faza a elaborării răspunsului șefii serviciilor/compartimentelor implicate vor avea în vedere definiția datelor cu caracter personal respectând obligațiile ce le revin în păstrarea confidențialității și integrității acestora.
Înainte de formularea răspunsului trebuie să se asigure că:

- informația transmisă nu reprezintă originalul unui document;

- informația transmisă nu include date personale despre o altă persoană — dacă e cazul, aceasta se anonimizează/elimină din răspunsul către persoana vizată;
- informația este inteligibilă

15.3.1. Datele personale/ informațiile care intră sub incidența acestei proceduri

Regulamentul 679/2016 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.
Sistem de evidentă a datelor cu caracter personal este considerată orice structură organizată de date cu caracter personal, accesibilă potrivit unor criterii determinate, indiferent dacă această structură este organizată în mod centralizat ori descentralizat sau este repartizată după criterii funcționale ori geografice.

Astfel, datele cu caracter personal care vor face obiectul acestei proceduri sunt datele persoanei vizate care au fost:

- stocate în bazele de date deținute de XXXX
- înregistrate în dosarele personale ale angajaților
- înregistrate în alte sisteme de evidență manuale
- imagini (înregistrate prin sistemul de supraveghere video – acolo unde este cazul)

15.3.2. Examinarea datelor personale/ informațiilor ce urmează a fi transmise persoanei vizate

După localizarea și colectarea informațiilor ce privesc persoana vizată, pe care XXXX le deține și le prelucrează, acestea vor fi analizate în detaliu de către șefii serviciilor/compartimentelor care dețin baza de date și, după caz, verificate de Responsabilul cu Protecția Datelor, pentru a stabili dacă pot fi comunicate. Această analiză se aplică de la caz la caz, pentru fiecare informație în parte.

- Se va verifica dacă datele înregistrate în baza de date/sistemul de evidență se referă la persoana vizată și nu la altă persoană cu același nume.
- Se vor elimina datele care se repetă
- Se comunică doar informațiile despre persoana vizată (cea care face obiectul cererii de acces). În cazul în care un document conține date despre mai multe persoane, inclusiv despre persoana vizată, informația referitoare la terțe părți nu se comunică persoanei vizate acestea se anonimizează
- Nu se comunică informații care ar prejudicia prevenirea sau cercetarea unei infracțiuni.

În procesul de analiză, Responsabilul cu Protecția Datelor va oferi asistență serviciilor/compartimentelor, în situația în care apar neclarități.

15.3.3. Redactarea și trimiterea răspunsului

După colectarea tuturor informațiilor deținute de operator despre persoana vizată, serviciile/compartimentele implicate sau Responsabilul cu Protecția Datelor va redacta documentul final, în forma în care va fi trimis persoanei vizate (model Anexa 2).

Răspunsul va cuprinde:

- 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, în special destinatari din țări terțe sau organizații internaționale (pentru aceștia din urmă se informează garanțiile adecvate referitoare la transfer);
- 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;
- 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;
- dreptul de a depune o plângere în fața unei autorități 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, menționat la articolul 22 alineatele (1) și (4) din Regulament, 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.

Informațiile transmise trebuie să fie redactate în formă inteligibilă.
După îndeplinirea cerințelor susmenționate, în susbsolul paginii va fi introdusă o Notă de informare cu următorul text:

*”prelucrarea datelor cu caracter personal din prezenta adresă se va supune prevederilor Regulamentului 679/2016 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), iar **DESTINATARUL** își va asuma măsuri tehnice și organizaționale corespunzătoare pentru protecția acestora.”*

- **Răspunsul în situația în care nu au fost găsite informațiile solicitate**

În cazul în care nu se găsesc informații despre persoana vizată, în bazele de date sau în sistemele de evidență ale XXXX, se va redacta un răspuns care să comunice acest fapt persoanei vizate (model Anexa 4).

In cazul în care nici una din datele localizate nu poate fi comunicată, persoana vizată va fi informată că operatorul nu a identificat date care să facă obiectul comunicării.

Răspunsul final, în forma în care va fi transmis persoanei vizate, se va păstra în copie la serviciile/compartimentele care l-au soluționat sau la Responsabilul cu Protecția Datelor, astfel încât să se poată identifica imediat în cazul în care persoana vizată ridică obiecții cu privire la conținutul transmis.

15.3.4. Finalizarea cererii

Transmiterea răspunsului se va face în modalitatea și la adresa indicată de persoana vizată la momentul depunerii cererii de acces.
Modalități posibile:

- prin poșta, prin intermediul Registraturii/Ghișeul de relații cu publicul;
- prin e-mail, prin intermediul protectia-datelor@XXXX.ro (*se va trece adresa stabilită la nivelul instituției pentru protecția datelor*);
- la Ghișeul de Relații cu Publicul, sediul XXXX

După transmiterea corespondenței finale, se va nota în Registrul Cererilor de Acces data la care a fost finalizată cererea.

15.4. DREPTUL DE INTERVENȚIE

15.4.1. Orice persoană vizată are dreptul de a obține de la operator, la cerere și în mod gratuit:

a) după caz, rectificarea, ștergerea („dreptul de a fi uitat”), restricționarea prelucrării, portabilitatea datelor, opoziția prelucrării, de a nu face obiectul unei decizii bazate exclusiv pe prelucrarea automată, inclusiv crearea de profiluri;
b) notificarea către terții cărora le-au fost dezvăluite datele a oricărei operațiuni efectuate conform lit. a) dacă această notificare nu se dovedește imposibilă sau nu presupune un efort disproporționat față de interesul legitim care ar putea fi lezat.

15.4.2. Pentru exercitarea dreptului prevăzut la punctul 4.1 persoana vizată va înainta operatorului o cerere întocmită în formă scrisă, datată și semnată. In 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.

15.4.3. Operatorul este obligat să comunice măsurile luate în temeiul punctului 6.1, precum și, dacă este cazul, numele terțului căruia i-au

fost dezvăluite datele cu caracter personal referitoare la persoana vizată, în termen de 30 de zile de la data primirii cererii, cu respectarea eventualei opțiuni a solicitantului exprimate potrivit punctului 6.2.

(Regulamentul (UE) 679/2016 al Parlamentului European și al Consiliului 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 - Art. 15)

Orice persoană are dreptul de a solicita corectarea informațiilor eronate, dacă le va constata în răspunsul la cererea de acces.

În acest caz, va completa formularul corespunzător (model Anexa 5), iar soluționarea acestei cereri se va supune prezentei proceduri.

15.5. EVIDENȚA CERERILOR DE ACCES

Cererile de acces vor fi înregistrate de către Responsabilul cu Protecția Datelor care are sarcina de a ține evidența acestora și de furniza situația statistică la solicitarea Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Persoanl.

Fiecare cerere de acces va fi păstrată într-o mapă distinctă, alături de celelalte documente care au folosit soluționării acesteia. Aceste mape se vor închide în fișet/dulap închis cu cheie și acolo unde este posibil, sigilat .

- Fiecare mapă va conține următoarele:
  - copii ale corespondenței dintre operator și persoana vizată, dintre operator și alte părți implicate
  - evidența oricăror convorbiri telefonice cu persoana vizată
  - evidența deciziilor luate de operator și modul prin care s-au luat aceste decizii
  - copii ale informațiilor trimise persoanei vizate

Toate documentele care au făcut obiectul soluționării cererii vor fi reținute pe o perioadă de 1 an, în caz că sunt necesare și alte operații privind asigurarea exercitării dreptului de acces al persoanei vizate, după care vor fi distruse prin procedură aprobată la nivelul instituției.

- Registrul Cererilor de Acces va cuprinde cel puțin următoarele:

a) data la care a fost primită/preluată cererea
b) denumirea serviciului/compartimentului implicat în soluționare
c) numele și prenumele persoanei vizate
d) data răspunsului trimis
e) informațiile transmise
f) timpul necesar soluționării cererii de acces.

Registrul Cererilor de Acces este utilizat în scopul monitorizării numărului de cereri care au fost adresate operatorului, a persoanelor care au solicitat accesul (astfel încât să se respecte dreptul la gratuitate) și a costurilor implicate.

16. RESPONSABILITĂȚI

Această procedură își propune să asigure respectarea și îndeplinirea obligațiilor ce revin XXXX în calitate de operator de date, așa cum sunt ele prevăzute de lege.
Consecințele nerespectării prevederilor legale atrag aplicarea unor sancțiuni contravenționale, atât la nivel de operator, cât și la nivel de utilizator/personal angajat al operatorului. De aceea este necesar ca operatorul să se asigure că au fost comunicate persoanei vizate toate informațiile solicitate, dar numai informațiile care se supun acestei proceduri. Această comunicare trebuie să respecte termenul legal de 30 de zile.
Responsabili privind respectarea acestei proceduri se fac, după caz, șefii următoarelor structuri:

- Structura Responsabilă cu Protecția Datelor cu Caracter Personal (*acolo unde există*) sau Responsabilul cu Protecția Datelor
- Serviciul Secretariat și Relații cu Publicul acolo unde există sau Registratura instituției
- Biroul/compartimentul Comunicare și Relații Publice *(acolo unde există*)
- Serviciile/compartimentele implicate în soluționarea cererii de acces

Șeful fiecărui serviciu/compartiment implicat în soluționarea cererii

- verifică respectarea acestei proceduri și a variantei/variantelor revizuite, în cadrul structurii pe care o conduce/coordonează.

Persoanele care utilizează această procedură:

- aplică forma inițială, precum și varianta/variantele revizuită/revizuită de la data intrării în vigoare a acesteia/acestora.

DISPOZIȚII FINALE

- Procedura va fi difuzată personalului care execută sau participă la activitatea/activitățile respectivă/respective descrise de către emitent, însoțită de anexele l-6 .
- Actuala procedură va fi revizuită în cazul în care apar modificări organizatorice sau alte reglementări legale cu caracter general și intern pe baza cărora se desfășoară activitatea/activitățile care face/fac obiectul acestei proceduri.
- Pe perioada absenței de la serviciu a persoanelor care utilizează prezenta procedură în forma inițială sau revizuită, aplicarea acesteia se va realiza și de înlocuitorii acestor persoane.

17. Formular analiză procedură

Nr .crt	Compartiment	Conducător compartiment	Aviz favorabil		Aviz nefavorabil		
			Semnătura	Data	Observații	Semnătura	Data

18. FORMULAR EVIDENŢĂ MODIFICĂRI

Nr. Crt.	Ed.	Data ediției	Rev.	Data reviziei	Pag.	Descriere modificare	Semnătura conducătorului compartimentului
1	1	…….	0	-	-	Întocmită conform OSGG nr.600/2018	

19. FORMULAR DISTRIBUIRE PROCEDURĂ

Compartiment	Conducător compartiment Nume și prenume	Data primirii	Semnătura	Data retragerii	Data intrării în vigoare a procedurii	Semnătura

20. ANEXE

- Anexa 1 – Model adresă de înaintare spre soluționare
- Anexa 2 – Model adresă de răspuns la cererea persoanei vizate
- Anexa 3 – Model adresă de solicitare informații suplimentare la cererea persoanei vizate
- Anexa 4 – Model de adresă de răspuns lipsă informații solicitate
- Anexa 5 – Formular cerere acces/intervenție la datele personale
- Anexa 6 – Registrul de evidență a cererilor persoanelor vizate

Model adresă de înaintare spre soluționare

ANTET INSTITUȚIE ANEXA 1

Către

SERVICIUL/COMPARTIMENTUL .....
În atenția șefului serviciului/compartimentului,

Vă remitem alăturat, în copie, cererea de acces la date personale, ce intră sub incidența Regulamentului (UE) 679/2016 al Parlamentului European și al Consiliului 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 de protecție a datelor) și a Legii nr.190/2018 privind măsuri de punere în aplicare a acestui Regulament.

Ca urmare a faptului că am identificat posibilitatea ca informațiile solicitate să se regăsească în evidența serviciului/compartimentului dumneavoastră, vă rugăm să dispuneți măsurile necesare pentru ca aceste informații să parvină Compartimentului

de Protecție a Datelor Personale/Responsabilului cu protecția datelor, în format hârtie și în format electronic (via INTRANET/adresa dpo@.....), în termen de/ la data de .....

În situația în care apar neclarități sau dificultăți care să împiedice soluționarea cererii, vă rugăm să ne contactați la.....

Model adresă de răspuns la cererea persoanei vizate

ANTET INSTITUȚIE ANEXA 2

Stimată/ Stimate .....

Ca urmare a solicitării dumneavoastră de acces la datele personale care vă privesc, din data de ..... înregistrată la registratura instituției sub nr. ..... am finalizat localizarea informațiilor solicitate în sistemele de evidență și în bazele de date deținute de XXXX.

Pe baza datelor pe care ni le-ați furnizat, vă confirmăm că XXXX prelucrează datele dumneavoastră și a identificat cele menționate în formularul atașat.

Informațiile pe care vi le furnizează XXXX sunt prelucrate în conformitate cu prevederile Regulamentului (UE) 679/2016 al Parlamentului European și al Consiliului 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 de protecție a datelor) și a Legii nr.190/2018 privind măsuri de punere în aplicare a acestui Regulament, în scopul .....

Formularul atașat conține sursa informațiilor și destinatarii, către care au fost comunicate aceste date, pe baza atribuțiilor legale.

Vă asigurăm că respectăm în totalitate drepturile prevăzute de prevederile legale susmenționate și vă rugăm să ne contactați pentru nelămuriri.

Cu deosebită stimă,

Model adresă de solicitare informații suplimentare la cererea persoanei vizate

ANTET INSTITUȚIE ANEXA 3

Stimată/ Stimate .....

Vă mulțumim pentru solicitarea de acces la datele cu caracter personal care vă privesc, sub incidența Regulamentului (UE) 679/2016 al Parlamentului European și al Consiliului 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 de protecție a datelor) și a Legii nr.190/2018 privind măsuri de punere în aplicare a acestui Regulament, din data de .....înregistrată la registratura unității sub nr .....

Pentru a putea soluționa cererea dumneavoastră, vă rugăm să completați informațiile necesare în formularul atașat, pe care să-l remiteți, ulterior completării, XXXX alături de o dovadă a identității dumneavoastră (copie a actului de identitate). Date de contact: str. .....

În urma răspunsului dvs., informațiile furnizate de dumneavoastră prin completarea formularului vor fi utilizate pentru a identifica datele solicitate în sistemele de evidență/ bazele de date gestionate de XXXX.

După identificarea acestora, răspunsul la cererea de acces vă va parveni în 30 zile de la preluarea formularului, conform prevederilor legale.

Cu deosebită stimă,

Model de adresă de răspuns lipsă informații solicitate

ANTET INSTITUȚIE ANEXA 4

Stimată/ Stimate .....

Ca urmare a solicitării dumneavoastră de acces la datele personale care vă privesc, din data de ....., am finalizat localizarea informațiilor solicitate în sistemele de evidență și în bazele de date deținute de XXXX.

Pe baza datelor pe care ni le-ați furnizat, vă confirmăm că nu a fost identificată nicio informație, cu privire la persoana dumneavoastră, care face obiectul comunicării obligatorii în baza Regulamentului (UE) 679/2016 al Parlamentului European și al Consiliului 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 de protecție a datelor) și a Legii nr.190/2018 privind măsuri de punere în aplicare a acestui Regulament.

Vă asigurăm că respectăm în totalitate drepturile prevăzute de prevederile legale susmenționate și vă rugăm să ne contactați pentru nelămuriri.

Cu deosebită stimă,

Formular cerere acces/intervenție la datele personale

ANTET INSTITUȚIE ANEXA 5

FORMULAR CERERE ACCES/INTERVENȚIE LA DATELE PERSONALE
(pentru exercitarea drepturilor prevăzute la art. 7, 12-22 din GDPR)

Detalii privind persoana vizată (titularul cererii):

Modalitate de adresare:	
Nume, prenume:	
Modalitate de contact (adresa de	

e-mail sau adresa poștală):	
ID client (dacă este cazul):	

Obiectul cererii:

Vă rugăm să selectați care este obiectul cererii:

- ☐ *Retragere a consimțământului pentru prelucrarea de date cu caracter personal*
- ☐ *Cerere de acces la datele cu caracter personal prelucrate*
- ☐ *Cerere de actualizare/rectificare a datelor cu caracter personal prelucrate*
- ☐ *Cerere de ștergere a datelor cu caracter personal prelucrate*
- ☐ *Cerere de restricționare a prelucrării datelor cu caracter personal*
- ☐ *Cerere de portare a datelor cu caracter personal prelucrate*
- ☐ *Cerere de opoziție la prelucrarea datelor cu caracter personal*
- ☐ *Cerere privind prelucrările automate și crearea de profile*

Categoriile de date cu caracter personal care fac obiectul cererii:

Detalii privind cererea dumneavoastră:

Semnatura (în cazul cererilor trimise prin serviciul poștal):	
Nume, prenume:	
Data:	

După completare, vă rugăm să trimiteți acest formular:

- Prin e-mail, pe adresa: .....@.....*(adresa de protectie date)*
- Prin serviciul poștal, la adresa: .....*(adresa sediului social)*

Model - Registrul de evidență a cererilor persoanelor vizate

ANTET INSTITUȚIE

ANEXA 6

Nr. crt.	Numărul și data înregistrării	Numele, prenumele și adresa persoane/ reprezentantului legal	Motivul solicitării (pe scurt)	Data soluționării	Soluția adoptată	Modalitatea de răspuns	Mențiuni privind clasarea lucrării	Obs.

NOTĂ:
Pentru ca documentul să fie lizibil este recomandat a se tipări pe format A3 Landscape.

8. ANEXA 8 -

ANTET

REGISTRU PENTRU ÎNREGISTRAREA CONSIMȚĂMINTELOR ACORDATE DE PERSOANELE VIZATE

Nr. și data înregistrării	Numele și prenumele persoanei vizate	Scopul pentru care a fost acordat	Data retragerii (sau distrugerii - nu mai există scopul)	Observații

9. ANEXA 9 -

ANTET

REGISTRUL DE EVIDENȚĂ A SOLICITĂRILOR PERSOANEI VIZATE

Nr. crt.	Numărul și data înregistrării	Numele, prenumele și adresa persoanei/ reprezentantului legal	Motivul solicitării (pe scurt)	Data soluționării	Soluția adoptată	Modalitatea de răspuns	Mențiuni privind clasarea lucrării	Obs.

10. ANEXA 10 -

ANTET

A P R O B
Funcția
Nume și prenume

POLITICA DE PROTECȚIE A PRELUCRĂRII DATELOR CU CARACTER PERSONAL
Cod: .....
Ediția I, .../.../....., Revizia

A V I Z A T
PREȘEDINTELE COMISIEI DE MONITORIZARE
Nume și prenume

ÎNTOCMIT
RESPONSABIL CU PROTECȚIA DATELOR
Nume și prenume

CUPRINS

Titlul I. Scopul Politicii[1]

Art. 1. Scopul Politici îl reprezintă conformitatea cu dispozițiile 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) și a legislației naționale în domeniu.

Art. 2. Politica se constituie ca instrument prin care organizația se asigură că personalul propriu, colaboratorii și partenerii care prelucrează date cu caracter personal pentru sau în numele acesteia sunt conștienți de îndatoririle ce le revin și se conformează procedurilor întocmite și obligațiilor ce decurg din legislația privind protecția datelor cu caracter personal.

Art. 3. Scopul procedurilor îl constituie:

a) stabilirea unui set unitar de reguli, măsuri tehnice și organizatorice adecvate pentru reglementarea aplicării unitare a măsurilor necesare pentru asigurarea protecției datelor cu caracter personal în cadrul îndeplinirii atribuțiilor de serviciu;
b) stabilirea regulilor care trebuie urmate pentru soluționarea cererilor formulate de persoana vizată cu privire la datele cu caracter personal stocate și prelucrate de organizație, sau în numele acesteia, stabilirea responsabilităților privind întocmirea, avizarea, aprobarea și transmiterea documentelor aferente acestei activități.

Titlul II. Domeniul de aplicare

Art. 4. Procedurile se aplică de către tot personalul, în executarea activităților specifice, potrivit fișei postului.

Titlul III. Referințe normative

Art. 5. În stabilirea Politicii s-a făcut apel la următoarele referințe normative:

- 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);
- Legea nr. 190/2018 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 2002/58/CE a Parlamentului European și a Consiliului din 12 iulie 2002 privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice (Directiva asupra confidențialității și comunicațiilor electronice);

[1] Politica de prelucrare și protecție a datelor cu caracter personal – în text **Politica**

- Decizia-cadru 2008/977/JAI a Consiliului din 27 noiembrie 2008 privind protecția datelor cu caracter personal prelucrate în cadrul cooperării polițienești și judiciare în materie penală;
- Directiva (UE) 2016/680 a Parlamentului European și a Consiliului 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
- Carta drepturilor fundamentale a Uniunii Europene (”carta”) articolul 8 și Tratatul privind funcționarea Uniunii Europene (TFUE) articolul 16 alineatul (1) care prevăd dreptul oricărei persoane la protecția datelor cu caracter personal care o privesc;
- DIRECTIVA (UE) 2016/681 A PARLAMENTULUI EUROPEAN ȘI A CONSILIULUI din 27 aprilie 2016 privind utilizarea datelor din registrul cu numele pasagerilor (PNR) pentru prevenirea, depistarea, investigarea și urmărirea penală a infracțiunilor de terorism și a infracțiunilor grave;
- DECIZIA Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal nr. 174 din 18 octombrie 2018, privind lista operaţiunilor pentru care este obligatorie realizarea evaluării impactului asupra protecţiei datelor cu caracter personal.

DEFINIȚII ȘI ABREVIERI

- Definițiile se regăsesc în anexa 1
- RGPD - 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 (Regulamentul general privind protecția datelor);
- XXXX – denumirea organizației (Operatorului de date)
- DPO – Responsabil cu protecția datelor
- S.I.C. – Sistemul Informatic și de Comunicații

Titlul IV. Descrierea procedurilor

Secțiunea I. Prelucrarea datelor cu caracter personal

Art. 6. Principii generale

(1) Prelucrarea datelor cu caracter personal se realizează cu respectarea regulilor generale și speciale prevăzute de 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 (Regulamentul general privind protecția datelor), a deciziilor

cu caracter normativ emise de Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal, denumită în continuare Autoritatea națională și a procedurilor proprii elaborate de organizație.

(2) Datele cu caracter personal sunt colectate și prelucrate în cadrul documentelor (pe suport hârtie) prin sistemul de evidență manuală, în format electronic prin sistemul de evidență automat/informatic *sau prin intermediul sistemului de supraveghere video (se trece doar acolo unde este cazul)*.

(3) XXXX stabilește ca principală responsabilitate prelucrarea legală și corectă a datelor cu caracter personal, în considerarea respectării drepturilor și libertăților fundamentale ale persoanei, iar regulile instituite prin intermediul prezentelor proceduri trebuie să asigure confidențialitatea acestei categorii de informații.

(4) Personalul XXXX prelucrează datele cu caracter personal cu aplicarea principiilor legalității, necesității, confidențialității și proporționalității.

(5) XXXX promovează principiile prelucrării datelor cu caracter personal, prevăzute în art. 5 din Regulamentul 679/2016, potrivit cărora datele cu caracter personal trebuie să fie:

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 fără a fi 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, în conformitate cu articolul 89 alineatul (1) („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, în conformitate cu articolul 89 alineatul (1), 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”).

(6) Operatorul este responsabil de respectarea acestor principii și poate demonstra această respectare (”responsabilitate”).

(7) XXXX, prin intermediul regulilor implementate la nivelul organizației, promovează principiul respectării drepturilor prevăzute de Regulamentul 679/2016, respectiv, dreptul la

informare, dreptul de acces, dreptul la rectificare și dreptul la ștergerea datelor (dreptul de a fi uitat), dreptul la restricționarea prelucrării, dreptul la portabilitatea datelor, dreptul de opoziție, dreptul de a nu fi supus unui proces decizional individual automatizat, inclusiv crearea de profiluri, dreptul de a se adresa cu o plângere la autoritatea de supraveghere și dreptul de a se adresa justiției.

Art. 7. Reguli specifice ale prelucrării de date cu caracter personal

(1) XXXX prelucrează date cu caracter personal, potrivit legii, în următoarele scopuri:

c) specifice domeniului de activitate:
   a. constituirea și gestionarea bazei de date privind grupul țintă căruia i se adresează proiectul .....
   b. .....*se trec toate scopurile în care prelucrează date cu caracter personal*.....
   c. …….
d) în scopuri administrative:
   a. evidența petenților;
   b. gestiune economico-financiară;
   c. resurse umane;
   d. monitorizarea și supravegherea video (a accesului în sediu *sau în alte locuri/scopuri*) – acolo unde este cazul.

(2) Datele 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;

(3) În scopul îndeplinirii atribuțiilor prevăzute de legislația în vigoare pe linia .....*se trec toate activitățile în care se prelucrează date personale conform cerințelor proiectului*..... XXXX colectează și prelucrează următoarele categorii de date cu caracter personal:

a) numele și prenumele
b) nume anterior
c) prenumele tatălui și prenumele mamei
d) sexul
e) data și locul nașterii
f) cetățenia
g) codul numeric personal
h) seria și numărul actului de identitate
i) semnătura
j) starea civilă
k) date biometrice
l) telefon/fax
m) reședința/domiciliul

n) *profesia*
o) *loc de muncă*
p) *imagine*
q) *alte date necesare derulării activităților specifice*

categoriile de date cu caracter personal prelucrate se stabilesc de fiecare organizație în parte conform temeiul legal de prelucrare și a activităților specifice proiectului. Lista enunțată nu este exhaustivă urmând a fi determinată de fiecare organizație în parte.....

(4) Prelucrarea datelor cu caracter personal se realizează după obținerea consimțământului persoanei vizate, înscris în formularul tipizat de cerere, sau fără consimțământul persoanei în situațiile strict prevăzute de legislația în vigoare. (*Aici fiecare organizație inserează temeiul legal de prelucrare pentru fiecare activitate în parte.)*

(5) În cadrul prelucrării datelor cu caracter personal efectuată de XXXX, în scopurile declarate, termenul de păstrare a acestora este:

a) Datele din registrele manuale se arhivează
    a. ....ani pentru.....
    b. ....ani pentru.....*(de preferat a se trece termenele prevăzute de legislația în vigoare și cuprinse în Nomenclatorul Arhivistic al organizației sau legislația europeană incidentă pentru FESI)*
b) Datele înregistrate pe suport digital se arhivează
    a. ....ani pentru.....
    b. ....ani pentru.....*(de preferat a se trece termenele prevăzute de legislația în vigoare și cuprinse în Nomenclatorul Arhivistic al organizației sau legislația europeană incidentă pentru FESI)*

(6) XXXX poate permite, în condițiile legii, personalului autorităților publice centrale sau locale accesul la datele cu caracter personal prelucrate de organizație, dacă este necesar pentru îndeplinirea atribuțiilor prevăzute de lege.

(7) In vederea asigurării securității prelucrărilor de date cu caracter personal, se întreprind măsuri care presupun:

a) aplicarea măsurilor tehnice și organizatorice adecvate pentru protejarea acestor date împotriva distrugerilor accidentale sau ilegale, pierderii, modificării, dezvăluirii sau accesului neautorizat;
b) asigurarea cerințelor minime de securitate stabilite de legislația în vigoare.

(8) În vederea asigurării condițiilor menționate la alin (7) lit. a) vor fi respectate întocmai, după caz, următoarele proceduri:

a) Procedură – *fluxul procesului de recrutare, angajare și gestionare dosare personale pentru angajații proprii, anexa nr. 4;*
b) Procedură – *fluxul procesului de alocare a diverselor mijloace tehnice și modul de parolare, anexa nr.5;*
c) Procedură – *Fluxul procesului de obținere/acordare adeverințe, anexa nr.6;*
d) Procedură – *Activitatea de arhivare, durata de stocare și destinația ulterioară a documentelor, anexa nr.7;*

e) Procedură – *efectuarea copiilor de siguranță ale bazelor de date care conțin date cu caracter personal, anexa nr.8;*
f) Procedură – *Cererea de acces a persoanei vizate la datele cu caracter personal care o privesc, anexa nr.9;*

(9) Procedurile prevăzute la alin.(8) trebuie aduse la cunoștința personalului organizației și a personalului nou-încadrat în cadrul instructajului realizat anterior acordării drepturilor de utilizator al sistemului informatic. Înainte de începerea activităților de prelucrare a datelor cu caracter personal, utilizatorul trebuie să semneze o declarație de confidențialitate pe propria răspundere privind respectarea normelor de protecție a acestor date.

(10) Supravegherea prin mijloace audio și/sau video, fixe sau mobile, în scopuri administrative proprii (asigurarea securității incintelor, supravegherea desfășurării unor activități specifice etc.) a unor spații publice din cadrul sediilor organizației, a celor perimetrale sau adiacente propriilor sedii constituie o prelucrare a datelor personale. Această operațiune se efectuează pe baza Politicii de supraveghere video. În acest caz este obligatorie avizarea personalului propriu și a publicului cu privire la existența sistemului de supraveghere, la scopul prelucrării datelor cu caracter personal și cu privire la datele de identificare ale operatorului.

(11) Instalarea de mijloace audio și/sau video se realizează astfel încât să nu fie vizualizat interiorul altor imobile sau căile de acces la acestea aflate în zona adiacentă echipamentelor de supraveghere, fiind limitat la maximum spațiul public afectat.

Art. 8. Categoriile de destinatari ai datelor cu caracter personal prelucrate de XXXX sunt:

a) Persoana vizată;
b) Reprezentanți legali ai persoanei vizate;
c) *.....se trec toate autoritățile și organizațiile partenere unde se transmit date personale....*

Art. 9. Comunicarea datelor cu caracter personal

(1) XXXX primește și soluționează, cererile persoanelor fizice și juridice care au ca obiect furnizarea unor informații ce intră sub incidența Regulamentului 679/2016.

(2) Datele personale gestionate de XXXX se comunică la cererea persoanei vizate sau a împuterniciților acesteia, la solicitarea instituțiilor cu atribuții în domeniul apărării, ordinii publice și siguranței naționale, precum și a altor persoane juridice în condițiile legii.

(3) Solicitările privind comunicarea datelor din sistemele de evidență automate și neautomate gestionate de XXXX trebuie să îndeplinească următoarele cerințe:

a) să fie adresate în formă scrisă, cu precizarea exactă a categoriilor de date cu caracter personal care necesită a fi prelucrate sau, după caz, a drepturilor pe care solicitantul înțelege să le exercite; în situația solicitărilor persoanei vizate depuse în exercitarea drepturilor prevăzute de lege, cererea trebuie să fie scrisă, datată și semnată;

b) să conțină datele necesare identificării persoanei fizice sau juridice care le solicită, precum și motivarea, scopul și durata prelucrării;
c) să cuprindă mențiuni sau să fie însoțite de documente care să facă dovada existenței temeiului legal justificat al solicitării;

(4) Cererile care nu conțin elementele prevăzute la lit. c) se restituie pentru completare, iar cele care nu se încadrează în condițiile prevăzute de lege sau de tratatele la care România este parte se resping, menționându-se motivele pentru care comunicarea datelor cu caracter personal nu este posibilă;

(5) Pot face obiectul comunicării doar datele cu caracter personal colectate direct sau indirect de către XXXX în scopul/scopurile necesare desfășurării activității proprii. Se interzice comunicarea datelor obținute de la alte instituții sau organisme publice, cu excepția situațiilor expres prevăzute de lege.

(6) In situațiile prevăzute în mod expres de lege, datele cu caracter personal pot fi comunicate din oficiu.

(7) Dezvăluirea către terți și transferul de date se efectuează cu informarea persoanei vizate, cu excepția situațiilor prevăzute expres de lege.

(8) Datele asupra cărora persoanele vizate au exercitat și li s-a recunoscut dreptul de opoziție nu pot face obiectul comunicării;

(9) Înainte de comunicarea datelor, XXXX, prin utilizatorii desemnați, verifică dacă acestea sunt exacte, complete și actualizate. In cazul în care se constată că datele nu sunt corecte sau actualizate, acestea nu vor fi comunicate și se vor dispune măsuri pentru actualizarea, rectificarea sau ștergerea acestora, după caz.

(10) Datele primite de la alți operatori, organisme publice ori private, nu trebuie să fie prelucrate pentru alte scopuri decât cele specificate în cererea de comunicare sau, după caz, în nota de transmitere.

(11) În situația transmiterii datelor cu caracter personal către terți se va menționa obligația acestora de a nu le prelucra în alte scopuri decât cel pentru care a fost efectuată comunicarea, cu excepția situației în care există consimțământul persoanei vizate sau după solicitarea și primirea acceptului scris din partea XXXX.

(12) Documentele care conțin date cu caracter personal, transmise persoanei vizate, vor avea înscrisă în subsolul paginii mențiunea: *„ Datele dumneavoastră sunt prelucrate de XXXX, în conformitate cu Regulamentul (UE) 679/2016, în scopul îndeplinirii atribuțiilor legale de operator (persoană împuternicită)...se trece situația reală... Datele pot fi dezvăluite unor terți în condițiile legii. Vă puteți exercita dreptul de acces, dreptul la rectificare și dreptul la ștergerea datelor (dreptul de a fi uitat), dreptul la restricționarea prelucrării, dreptul la portabilitatea datelor, dreptul de opoziție, dreptul de a nu fi supus unui proces decizional individual automatizat, inclusiv crearea de profiluri, printr-o cerere scrisă, semnată și datată, trimisă pe adresa organizației. De asemenea aveți dreptul de a vă adresa cu o plângere la Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal sau justiției, potrivit legii”.*

(13) Comunicarea trebuie să cuprindă numai datele solicitate expres și doar dacă a fost determinat dreptul terțului de a prelucra acea categorie de date, indiferent de

existența sau nu în evidențele XXXX a altor categorii de date cu caracter personal referitoare la persoana vizată.

(14) In situația în care solicitarea are ca obiect prelucrarea de date cu caracter personal în scopul instrumentării unei cauze penale sau civile, datele solicitate se comunică doar organului de urmărire penală sau instanței de judecată;

(15) Dacă datele cu caracter personal solicitate fac parte din categoria informațiilor clasificate, comunicarea acestora se face cu respectarea strictă a prevederilor legislației privind protecția informațiilor clasificate.

Art. 10. Reguli de prelucrare

(1) Verificarea în sistemele de evidență manuale, automate și, după caz, în dosarele de personal se efectuează de către personalul anume desemnat în baza fișei de post sau prin dispoziții rezolutive ale conducerii XXXX.

(2) Cu excepția verificării în sistemele de evidență automate unde sistemul este cel care trebuie să genereze fișierul de acces, consemnarea rezultatului verificărilor se efectuează pe baza unor formulare pentru redactarea răspunsurilor care vor fi înregistrate în Registrul special întocmit.

(3) Circuitul formularelor, documentelor și a dosarelor de personal se realizează prin înregistrarea acestora și predarea pe bază de semnătură în condici sau/și registre, conform procedurilor specifice emise la nivelul operatorului.

Art. 11. Consimțământul persoanei vizate

(1) Nici o prelucrare de date cu caracter personal nu poate fi efectuată fără consimțământul persoanei vizate.

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

a) 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;
b) prelucrarea este necesară în vederea îndeplinirii unei obligații legale care îi revine operatorului;
c) prelucrarea este necesară pentru a proteja interesele vitale ale persoanei vizate sau ale altei persoane fizice;
d) prelucrarea este necesară pentru îndeplinirea unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice cu care este învestit operatorul;
e) 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.

(3) În domeniul prelucrării datelor cu caracter personal, consimțământul persoanei vizate reprezintă orice manifestare de voință liberă, specifică, informată și lipsită de

ambiguitate a persoanei vizate prin care aceasta acceptă, printr-o declarație sau printr-o acțiune fără echivoc, ca datele cu caracter personal care o privesc să fie prelucrate.

(4) Consimțământul poate fi obținut numai după ce persoana vizată a fost complet și exact informată cu privire la scopul prelucrării datelor cu caracter personal care o privesc (Anexa nr.4 - Notă de informare).

(5) Consimțământul trebuie dat în mod expres, într-o formă care să permită dovedirea acestuia de către operator.

Secțiunea II. Solicitarea accesului la datele cu caracter personal

Art. 12. Dreptul de acces la date

(l) Orice cerere scrisă prin care o persoană solicită informații despre datele cu caracter personal care o privesc sau despre datele cu caracter personal ale altei persoane pe care o reprezintă în mod legal, se înregistrează în registrul special destinat și, conform dispoziției rezolutive a conducătorului organizației, se transmite departamentelor cu competențe în soluționarea acesteia.

(2) Responsabilul cu protecția datelor cu caracter personal este informat cu privire la orice cerere efectuată de către persoana vizată în temeiul Regulamentului (UE) 679/2016.

(3) Responsabilul cu protecția datelor cu caracter personal stabilește dacă o solicitare se încadrează în categoria ”cereri de acces la date cu caracter personal” și intră sub incidența RGPD, și monitorizează activitatea de soluționare a acestora.

(4) O cerere, pentru a se încadra în categoria ”cereri de acces la date cu caracter personal”, efectuată în temeiul RGPD, trebuie să fie scrisă, datată și semnată; astfel, determinarea naturii juridice a solicitării se face prin raportare la conținutul acesteia, nefiind obligatorie, de exemplu, menționarea în cuprinsul acesteia a RGPD sau existența titulaturii specifice („cerere pentru exercitarea dreptului de acces") ori indicarea în mod expres a dreptului a cărui exercitare se urmărește; în aceste condiții, o cerere în cuprinsul căreia nu există nicio mențiune cu privire la RGPD sau cu privire la exercitarea dreptului de acces va fi încadrată în categoria cererilor de acces dacă persoana vizată solicită, de exemplu, confirmarea și/sau comunicarea categoriilor de date cu caracter personal prelucrate cu privire la persoana sa de către operator sau comunicarea scopurilor prelucrărilor efectuate ori dacă, pentru soluționarea cererii, este necesară consultarea log-urilor etc.

(5) O cerere îndeplinește condițiile prevăzute de RGPD (scrisă, datată și semnată) dacă, în mod rezonabil, se poate constata îndeplinirea acestora; astfel, o cerere transmisă prin intermediul fax-ului sau prin intermediul poștei electronice (scanată în format .pdf) este de natură să îndeplinească aceste condiții.

(6) Orice persoană vizată are dreptul de a obține de la operator, la cerere și în mod gratuit, confirmarea faptului că datele care o privesc sunt sau nu sunt prelucrate de acesta.

(7) XXXX este obligată, în situația în care prelucrează date cu caracter personal care privesc solicitantul, să comunice acestuia, împreună cu confirmarea, cel puțin următoarele informații:

a) scopurile prelucrării, categoriile de date avute în vedere și 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;
b) 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;
c) existența dreptului de a solicita operatorului rectificarea sau ștergerea datelor cu caracter personal ori restricționarea prelucrării datelor referitoare la persoana vizată sau a dreptului de a se opune prelucrării;
d) dreptul de a depune o plângere la autoritatea națională de supraveghere a prelucrării datelor cu caracter personal;
e) în cazul în care datele cu caracter personal nu sunt colectate de la persoana vizată, orice informații disponibile privind sursa acestora;
f) 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.

(8) În cererea transmisă, solicitantul poate arăta dacă dorește ca informațiile să îi fie comunicate la o anumită adresă sau printr-un serviciu de corespondență care să asigure că predarea i se va face numai personal. Cât privește modalitatea de comunicare prin poștă electronică a informațiilor solicitate, aceasta nu are siguranță deplină, astfel că prin alegerea sa solicitantul își asumă riscurile legate de comunicarea electronică de informații (interceptare, modificare, pierdere, distrugere, întârziere în primirea datelor etc.). În această situație, persoana vizată trebuie să fie informată asupra tuturor riscurilor la care este expusă o asemenea comunicare, pentru a consimți expres și neechivoc în alegerea acestei modalități (subliniem că modelul de cerere de acces, pus la dispoziția persoanelor vizate în mod orientativ, informează persoana vizată în mod clar asupra acestor aspecte).

(9) În cazul în care solicitarea nu îndeplinește condițiile prevăzute de lege, solicitantul este informat cu privire la faptul că dreptul de acces se poate exercita doar prin depunerea unei cereri în formă scrisă, datată și semnată.

(10) Odată cu soluționarea unei cererii se aduce la cunoștința persoanelor vizate că au dreptul de a se adresa Autorității naționale de supraveghere sau justiției pentru apărarea drepturilor garantate de lege.

(11) XXXX este obligată să comunice informațiile solicitate într-un termen rezonabil dar nu mai târziu de 30 zile de la data primirii cererii.

Secțiunea III. Categorii de incidente și soluționarea acestora

Art. 13. (1) Toți utilizatorii XXXX au acces la date cu caracter personal strict în exercitarea atribuțiilor de serviciu și nu pot să le prelucreze decât pe baza procedurilor interne.

(2) Administratorul de sistem este obligat să aplice măsurile tehnice și organizatorice adecvate pentru protejarea datelor cu caracter personal împotriva distrugerii accidentale

sau ilegale, pierderii, modificării, dezvăluirii sau accesului neautorizat, întrucât prelucrarea comportă transmisii de date în cadrul unei rețele, precum și împotriva oricărei alte forme de prelucrare ilegală.

(3) Incidentele în legătură cu protecția datelor cu caracter personal pot fi:

a) incidente tehnice (electronice);
b) incidente operaționale (fizice);
c) incidente administrative (procedurale).

(4) Incidentul de securitate în domeniul protecției datelor cu caracter personal, stocate sau transmise, reprezintă orice eveniment, acțiune, inacțiune sau împrejurare de natură să afecteze confidențialitatea, integritatea sau disponibilitatea acestor date.

(5) În principal, constituie incident de securitate:

a) pierderea, sustragerea, înlocuirea, alterarea, dezvăluirea sau distrugerea neautorizată ori accidentală a datelor cu caracter personal;
b) forțarea accesului, accesul neautorizat sau interzicerea accesului autorizat la datele cu caracter personal;
c) modificarea neautorizată și nejustificată a datelor cu caracter personal;
d) copierea neautorizată pe suport de date extern sau executarea de fotocopii ale documentelor care conțin date cu caracter personal fără avizul responsabilului cu protecția datelor cu caracter personal și aprobarea șefului departamentului/compartimentului;
e) nerespectarea regulilor privind depozitarea, manipularea sau distrugerea mediilor de stocare în uz pe care sunt stocate date cu caracter personal;
f) nerespectarea prevederilor, metodologiilor, instrucțiunilor și dispozițiilor privind prelucrarea datelor cu caracter personal;
g) distrugerea mediilor de stocare scoase din uz, fără a respecta prevederile actelor normative care reglementează domeniul protecției datelor cu caracter personal.
h) rețele interne nesecurizate;
i) nerespectarea cerințelor legale privind primirea și distribuirea corespondenței în domeniul datelor cu caracter personal;
j) producerea altor evenimente care afectează confidențialitatea, integritatea și disponibilitatea informațiilor clasificate stocate, procesate sau transmise în SIC.

(6) Fiecare incident este investigat de către o comisie formată din Responsabilul cu protecția datelor cu caracter personal desemnat la nivelul organizației, un reprezentant al departamentului control/audit/calitate, administratorul bazei de date și șeful nemijlocit al lucrătorului implicat în incident, fiind luate deîndată măsuri de limitare pe cât posibil a prejudiciilor apărute în urma producerii incidentelor apărute.

(7) Investigația stabilește:

a) dacă au fost respectate procedurile privind prelucrarea datelor cu caracter personal;
b) dacă au fost compromise datele cu caracter personal;
c) dacă există persoane care au avut acces la datele cu caracter personal la care se referă incidentul de securitate și stabilirea identității acestora;

d) măsuri preventive, corective sau dacă este cazul măsuri disciplinare.

(8) În cazul în care se constată că au fost compromise datele cu caracter personal se aplică prevederile legale în vigoare.

Secțiunea IV. Cerințele minime de securitate a prelucrării de date cu caracter personal

Art. 14. Cerințele minime de securitate a prelucrărilor de date cu caracter personal stau la baza adoptării și implementării de către XXXX a măsurilor tehnice și organizatorice necesare pentru păstrarea confidențialității și integrității datelor cu caracter personal sunt:

(1) *Identificarea și autentificarea utilizatorului*

a) Prin utilizator se înțelege personalul XXXX cu drept de acces la bazele de date cu caracter personal.
b) Pentru buna desfășurare a activității informatice în cadrul XXXX, cât și pentru asigurarea confidențialității datelor, a documentelor prelucrate și stocate pe echipamentele de calcul din dotare, precum și protecția și securitatea rețelei informatice, se impune accesarea aplicațiilor din sistemul informatic al XXXX prin identificarea și autentificarea utilizatorilor.
c) Identificarea și autentificarea în sistem se realizează prin introducerea unui cod de identificare de la tastatura (user-name) — atribuit de către Administratorul sistemului — însoțită de introducerea unei parole.
d) Utilizatorii autorizați ai sistemului informatic răspund pentru securitatea parolelor și a conturilor personale. Codurile de identificare și parolele sunt unice, personale și netransmisibile. Se interzice folosirea lor în comun, de către mai mulți utilizatori.
e) Parolele sunt importante pentru securitatea sistemelor informatice. Ele constituie prima linie de protecție pentru conturile utilizatorilor. Gradul de securitate asigurat de o parolă crește proporțional cu numărul de caractere al acesteia, precum și cu utilizarea atât a literelor, cifrelor și caracterelor speciale; este obligatoriu ca utilizatorul să-și seteze o parolă de minim 8 caractere alfanumerice (obligatoriu cel puțin 3 categorii de caractere din următoarele: litere mici, litere mari, cifre și caractere speciale (*, &, #, etc.)) care să nu conțină date personale (de ex: numele sau prenumele, data nașterii, prenumele membrilor de familie, etc.) sau părți ale numelor acestora și să nu fie folosite pentru a accesa servicii publice (mail, Messenger sau alte conturi pe Internet), sau alte aplicații de interes profesional. Introducerea acestora nu se afișează în clar, pe ecran. Parola nu poate fi schimbată de către utilizator în primele 24 de ore de la ultima setare, sistemul memorând ultimele 24 de parole pentru a nu putea fi refolosite.
f) Durata de valabilitate a parolei este de 90 de zile; înainte de expirarea parolei cu 14 zile utilizatorul va fi înștiințat cu privire la necesitatea schimbării acesteia.
g) O parolă prost aleasă poate duce la compromiterea securității întregii rețele. Prin urmare, este obligatorie respectarea condiției de creare a unei parole cât mai complexe.
h) Este obligatorie schimbarea periodică a parolei și ori de câte ori există posibilitatea ca aceasta să își fi pierdut caracterul confidențial. Este interzisă folosirea parolelor anterioare. Schimbarea parolelor se face numai de către deținătorul acesteia.
i) Parolele nu trebuie să fie inserate în mesajele de poștă electronică sau în alte forme de comunicare electronică; de asemenea, parolele nu vor fi comunicate telefonic; nu

este recomandată divulgarea formatului unei parole (în discuțiile cu alte persoane) sau divulgarea parolei în chestionare sau în formulare de securitate.

j) Parolele nu trebuie partajate cu nimeni din organizație și trebuie tratate ca fiind informații confidențiale ale organizației.
k) Se va evita folosirea opțiunii ”Remember password” (”Reține parola").
l) Se interzice transcrierea / păstrarea parolei, la vedere sau în alt mod decât cel prevăzut mai sus ori diseminarea / transmiterea acestora către alte persoane.
m) Documentele care conțin coduri de identificare și parole de acces vor fi arhivate numai dacă acestea nu se mai află în uz.
n) La părăsirea stației de lucru este obligatorie deconectarea utilizatorului (Log off) sau blocarea calculatorului pe contul de utilizator conectat (tasta Windows+L). Deblocarea stației se va putea face doar de către utilizatorul conectat sau administratorul de sistem în caz de necesitate. Această practică este indicată pentru asigurarea securității informațiilor prelucrate și prevenirea accesului neautorizat la aceste informații.
o) La apariția unei situații de modificare a competențelor sau raporturilor de serviciu, la comunicarea Departamentului Resurse Umane sau, unde este cazul, a șefului de departament/ compartiment, administratorul de sistem ia măsuri de revocare/suspendare a conturilor de acces, astfel încât prelucrarea datelor cu caracter personal să se facă numai de către personalul autorizat și numai în exercitarea atribuțiilor de serviciu ale acestora.
p) Acordarea de permisiuni suplimentare, restrângerea permisiunilor sau dezactivarea conturilor se face în baza solicitărilor scrise din partea șefilor de departamente/compartimente, în care aceștia vor menționa și motivul acordării, restrângerii permisiunilor sau dezactivării contului utilizatorului respectiv. Personalul de specialitate al departamentului/compartimentului IT al XXXX va răspunde în scris de realizarea cerințelor.
q) La crearea contului de utilizator, specialistul IT setează o parolă temporară, care va fi comunicată în scris — în mod corespunzător titularului de cont, utilizatorul fiind obligat de către sistem să și-o schimbe la prima logare (conectare).
r) Conturile de utilizator care nu au fost folosite mai mult de 90 de zile vor fi dezactivate.

(2) *Tipul de acces*

a) Tipurile de acces și operațiunile permise acestuia, strict necesare pentru îndeplinirea atribuțiilor de serviciu, se stabilesc conform atribuțiilor din fișa postului fiecărui utilizator.
b) Se interzice accesul dezvoltatorilor de aplicații software/ personalului de întreținere a sistemelor informatice la orice fel de date cu caracter personal; în aceste situații, se pun la dispoziția programatorilor/personalului de întreținere numai date anonime.

(3) *Păstrarea și utilizarea programelor de sistem și aplicație*

a) Instalarea oricărui produs software este interzisă a fi efectuată de către personal neautorizat.
b) Orice instalare sau dezinstalare de produse software se realizează numai de către administratorul de sistem.

c) Este interzisă instalarea oricărui produs software care ar putea periclita securitatea rețelei, cât și introducerea - de către utilizatori - a unor programe răuvoitoare în rețea (viruși, viermi, cai troieni, bombe e-mail).
d) Nicio stație care prelucrează date cu caracter personal nu va fi conectată la INTERNET.

(4) *Atribuții și Responsabilități*

a) Administratorii de securitate/sistem:

1. elaborează și propun modificări ale politicii de securitate a S.I.C.-ului ;.
2. elaborează și propun pentru aprobare regulamentele, normele și procedurile de securitate a S.I.C.-ului;
3. elaborează proceduri pentru identificarea și monitorizarea activității utilizatorilor S.I.C.;
4. tratează incidentele de securitate în scopul minimizării efectului distructiv al acestora asupra sistemului S.I.C., cât și a minimizării efectelor negative sau a incorectei funcționări a echipamentelor;
5. instruiesc și evaluează periodic utilizatorii în ceea ce privește cunoașterea și respectarea prevederilor Politicii de securitate, a normelor, regulamentelor sau procedurilor de securitate, prin aplicarea conformă a acestora;

b) Atribuții ale utilizatorilor:

1. să cunoască și să respecte prevederile tuturor regulilor, măsurilor și/sau procedurilor privind securitatea sistemului informatic;
2. să răspundă direct de securitatea și conținutul informațiilor și resursele informatice și de comunicații încredințate;
3. să se asigure că informațiile în posesia cărora intră, sunt transmise numai persoanelor autorizate;
4. le este interzisă mutarea tehnicii de calcul, repoziționarea cablurilor de rețea sau de alimentare, instalarea sau dezinstalarea echipamentelor periferice; aceste operațiuni se realizează prin solicitare scrisă și numai de către administratorul de sistem;
5. să întrețină corespunzător tehnica de calcul din componența sistemului informatic (menținerea curățeniei suprafețelor exterioare, evitarea șocurilor mecanice, etc.);
6. să nu introducă în organizație echipamente de calcul sau memorii externe personale (care nu fac parte din sistemul informatic al XXXX); este interzisă scoaterea din organizație a acestor echipamente de calcul sau memorii externe;
7. să informeze persoana vizată atunci când datele cu caracter personal sunt colectate direct de la aceasta, în condițiile legii, cu privire la: identitatea și datele de contact ale operatorului și, după caz, ale reprezentantului acestuia; datele de contact ale responsabilului cu protecția datelor, după caz; scopurile în care sunt prelucrate datele cu caracter personal, precum și temeiul juridic al prelucrării; în cazul în care prelucrarea se face în temeiul articolului 6 alin. (1) lit. (f), interesele legitime urmărite de operator sau de o parte terță; destinatarii sau categoriile de destinatari ai datelor cu caracter personal; dacă este cazul, intenția operatorului de a transfera date cu caracter personal către o țară terță sau o organizație internațională și

existența sau absența unei decizii a Comisiei privind caracterul adecvat sau, în cazul transferurilor menționate la art.46 sau 47 sau la art.49 alin. (1) al doilea paragraf, o trimitere la garanțiile adecvate sau corespunzătoare și la mijloacele de a obține o copie a acestora, în cazul în care acestea au fost puse la dispoziție;

8. să prelucreze numai datele cu caracter personal necesare îndeplinirii atribuțiilor de serviciu și să acorde sprijin responsabilului cu protecția datelor cu caracter personal pentru realizarea activităților specifice ale acestuia/acesteia;
9. să păstreze confidențialitatea datelor prelucrate, a contului de utilizator, a parolei/codului de acces la sistemele informatice/baze de date prin care sunt gestionate date cu caracter personal;
10. să respecte măsurile de securitate, precum și celelalte reguli stabilite prin proceduri proprii;
11. să informeze de îndată conducerea XXXX despre împrejurări de natură a conduce la o diseminare neautorizată de date cu caracter personal sau despre o situație în care au fost accesate/prelucrate date cu caracter personal prin încălcarea normelor legale, despre care a luat la cunoștință;
12. la sfârșitul programului este obligatorie închiderea calculatoarelor și a imprimantelor, precum și a celorlalte echipamente periferice, dacă este cazul.

(5) *Folosirea computerelor, aplicațiilor informatice*

a) Utilizarea aplicațiilor informatice se face numai în conformitate cu procedurile, normele de lucru și metodologiile de exploatare aprobate.
b) Accesarea informațiilor stocate în bazele de date se realizează numai în interesul îndeplinirii atribuțiilor profesionale, iar furnizarea acestor informații este permisă numai în conformitate cu prevederile legale.
c) Utilizatorii trebuie să anunțe administratorul de sistem când observă:

1. posibilă problemă / breșă în sistemul de securitate al SIC;
2. o posibilă întrebuințare greșită sau încălcare a regulamentelor în vigoare;
3. o funcționare anormală a echipamentelor de calcul.

d) Utilizatorii, prin acțiunile lor, nu trebuie să încerce să compromită protecția sistemelor informatice și de comunicații și nu trebuie să desfășoare, deliberat sau accidental, acțiuni care pot afecta confidențialitatea, integritatea și disponibilitatea informațiilor de orice tip în cadrul sistemului informatic.

e) Utilizatorii nu trebuie să încerce să obțină acces la date sau programe din SIC-urile pentru care nu au autorizație.
f) Utilizatorilor autorizați li se interzice să permită altor persoane, inclusiv altor utilizatori autorizați, accesarea sistemului informatic cu contul și parola lor sau cu alte elemente de identificare personală.
g) Conturile și parolele asociate sunt personale. Utilizatorii au obligația de a schimba parola propriului cont ori de câte ori există suspiciunea că aceasta este cunoscută și de alte persoane.
h) Utilizatorii nu trebuie să facă copii neautorizate sau să distribuie materiale protejate

prin legile privind proprietatea intelectuală (copyright).

i) Accesul în încăperile în care se află echipamente care prelucrează date cu caracter personal este strict limitat la utilizatorii cu atribuții în acest domeniu.
j) Accesul pentru intervenții tehnice, reparații sau activități de deservire la echipamentele informatice, este permis numai angajaților care dețin autorizații de acces, fiind însoțiți permanent de către un angajat anume desemnat de către șeful departamentului/compartimentului.
k) Accesul angajaților altor organizații care efectuează lucrări de construcții, reparații și întreținere a clădirii, instalațiilor sau utilităților în zonele administrative ori în zonele de securitate se realizează cu documente de acces temporar eliberate de șeful departamentului/compartimentului administrativ, pe baza actelor de identitate, la solicitarea reprezentanților autorizați ai instituțiilor în cauză.
l) Accesul persoanelor din afara organizației în zona administrativă sau în zonele de securitate este permis numai însoțite de persoane anume desemnate, cu permis de acces eliberat la punctul de control-acces, pe baza documentelor de legitimare, după ce au fost înregistrate în registrul de acces în organizație.
m) Este interzis accesul în sediul organizației cu aparate de fotografiat, filmat, înregistrat audio-video, de copiat din baze de date informatice sau de comunicare la distanță.
n) Sistemul de control-acces asigură prevenirea pătrunderii neautorizate în sediul serviciului, sectoarele și locurile unde sunt gestionate informații clasificate.
o) Accesul la stațiile de lucru este permis numai personalului autorizat, și numai în baza datelor de acces (cont de utilizator si parolă).
p) Produsul software antivirus este instalat pe toate serverele și stațiile și se actualizează automat zilnic; acesta este administrat și monitorizat de către personalul de specialitate al XXXX.

(6) *Instruirea personalului*

a) Instruirea personalului cu privire la protecția și prelucrarea datelor cu caracter personal și libera circulație a acestor date se efectuează în cadrul programului de pregătire continuă sau ori de câte ori este nevoie, conform dispozițiilor primite.

(7) *Imprimarea datelor*

a) Tipărirea la imprimantă a datelor cu caracter personal se va realiza numai de utilizatori autorizați pentru această operațiune.
b) Utilizatorii sunt obligați sa respecte procedurile interne specifice, precum și Politica de securitate în sistemul informatic.

Titlul V. DISPOZIȚII FINALE

Art. 15. Documentul se difuzează întregului personal al XXXX.

Art. 16. Procedurile vor fi revizuite în cazul în care apar modificări organizatorice sau ale reglementărilor legale cu caracter general și intern pe baza cărora se desfășoară activitățile care fac obiectul acestor proceduri.

Art. 17. Pe perioada absenței de la serviciu a persoanelor care utilizează procedurile în forma inițială sau revizuită, aplicarea acestora se va realiza și de înlocuitorii acestor persoane.

Art. 18. Anexele 1 și 2 se păstrează la emitent.

Art. 19. Prezenta procedură intră în vigoare la data aprobării de către conducerea XXXX.

Art. 20. Anexele 1 – 9 fac parte integrantă din prezenta politică.

TITLUL VI. FORMULARE

1. Formular analiză politică

Nr .crt	**Compartiment**	**Conducător compartiment**	**Aviz favorabil**		**Aviz nefavorabil**		
			Semnătura	Data	**Observații**	Semnătura	Data

2. FORMULAR EVIDENŢĂ MODIFICĂRI

Nr. Crt.	Ed.	Data ediției	Rev.	Data reviziei	Pag.	Descriere modificare	Semnătura conducătorului compartimentului

1	1	…….	0	-	-	Întocmită conform OSGG nr.600/2018	

3. Formular distribuire politică

Compartiment	**Conducător compartiment Nume și prenume**	**Data primirii**	**Semnătura**	**Data retragerii**	**Data intrării în vigoare a procedurii**	**Semnătura**

TITLUL VII. ANEXE:

Anexa nr. 1 – Definiții
Anexa nr. 2 - Nota de informare persoane vizate.
Anexa nr. 3 - Ghid pentru exercitarea drepturilor de către persoanele vizate
Anexa nr. 4 - Procedura – Fluxul procesului de recrutare, angajare și gestionare dosare personale
Anexa nr. 5 - Procedura – Fluxul procesului de alocare a diverselor mijloace tehnice și modul de parolare
Anexa nr. 6 - Procedura – Fluxul procesului de obținere/acordare adeverințe
Anexa nr.7 - Procedura – Activitatea de arhivare, durata de stocare și destinația ulterioară a documentelor
Anexa nr. 8 - Procedura – efectuarea copiilor de siguranță ale bazelor de date care conțin date cu caracter personal
Anexa nr. 9 - Procedura – Cererea de acces a persoanei vizate la datele cu caracter personal care o privesc

ANTET **Anexa nr.1**

DEFINIȚII

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. **Prelucrarea datelor cu caracter personal** – 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. **Consimțământul persoanei vizate** – înseamnă orice manifestare de voință liberă, specifică, informată și lipsită de ambiguitate a persoanei vizate prin care aceasta acceptă, printr-o declarație sau printr-o acțiune fără echivoc, ca datele cu caracter personal care o privesc să fie prelucrate;
4. **Stocarea** – păstrarea pe orice fel de suport a datelor cu caracter personal culese;
5. **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;
6. **Persoană împuternicită de operator** – înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care prelucrează datele cu caracter personal în numele operatorului;
7. **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;
8. **Destinatar** – înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism căreia (căruia) 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;

9. **Date anonime** – date care, datorită originii sau modalității specifice de prelucrare, nu pot fi asociate cu o persoană identificată sau identificabilă;
10. **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;
11. **Sistem de evidență a datelor cu caracter personal** – 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;

ANTET Anexa nr.2

NOTA DE INFORMARE PERSOANE VIZATE

Conform cerințelor Regulamentului (UE) 2016/679/27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date, XXXX are obligația de a administra în condiții de siguranță și numai pentru scopurile specificate, datele personale pe care ni le furnizați despre dumneavoastră, un membru al familiei dumneavoastră ori o altă persoană.

XXXX colectează și prelucrează date cu caracter personal în următoarele scopuri:

a) <u>specifice domeniului de activitate al proiectului .....:</u>
   - ……..
   - ……
b) <u>în scopuri administrative:</u>
   a. evidența petenților;
   b. gestiune economico-financiară;
   c. resurse umane;

Datele dumneavoastră ne sunt necesare în scopul derulării activităților din cadrul proiectului în condiții de eligibilitate. Refuzul dumneavoastră de a furniza anumite date poate determina imposibilitatea furnizării de către XXXX a serviciilor prevăzute în proiect.

Informațiile înregistrate sunt destinate utilizării de către XXXX și sunt comunicate numai următorilor destinatari: angajații desemnați ai organizației, persoana vizată, parteneri contractuali ai organizației, instituții publice autorizate să prelucreze date cu caracter personal (de ex. AM, ANAF, REVISAL, etc.).

Aveți oricând posibilitatea să vă retrageți acest consimțământ și să vă bucurați în continuare de serviciile asigurate prin proiect.

Conform Regulamentului (UE) 2016/679/27 aprilie 2016, beneficiați de:

- dreptul la transparență,
- dreptul de a fi informat,
- dreptul de acces la date,
- dreptul la rectificare,
- dreptul la ștergerea datelor („dreptul de a fi uitat”)*,
- dreptul la restricționarea prelucrării,

- dreptul la portabilitatea datelor,
- dreptul de a nu fi supus unei decizii automate (inclusiv crearea de profiluri),
- dreptul de a se adresa justiției/ ANSPDCP.

Pentru exercitarea acestor drepturi, vă puteți adresa cu o cerere scrisă, datată și semnată la sediul XXXX din ……. sau la email …….@.....

Datele sunt colectate direct de la dumneavoastră, membrii ai familiei, ori împuterniciți în cadrul unor relații de muncă (de către organizația unde lucrați) sau dacă faceți parte din grupul țintă al proiectului. Ele se colectează fie direct (de ex. prin completarea documentelor de angajare sau participare la diverse activități din cadrul proiectului), fie în cadrul unui raport comercial încheiat de organizația beneficiară a proiectului și partenerii săi de contract angrenați în realizarea acestuia.

În cazul în care datele dumneavoastră sunt transferate pe teritoriul Uniunii Europene sau al altor țări din afara acesteia ne asigurăm că și acestea respectă prevederile legale privind protecția datelor cu caracter personal și există o legislație compatibilă și acceptată de Uniunea Europeană.

Pentru mai multe detalii privind prelucrarea datelor cu caracter personal, vă rugăm să accesați site-ul nostru și să descoperiți rubrica de Politică de Confidențialitate.

Observație:
*orice persoană are dreptul de a se opune, pentru motive legitime, la prelucrarea datelor ce o privesc. Acest drept de opoziție poate fi exclus pentru anumite prelucrări prevăzute de lege (de ex.: prelucrări efectuate de serviciile financiare și fiscale, de politie, justiție, securitate socială sau legislația europeană pe linia acordării fondurilor de finanțare a proiectelor).

Prin urmare, această mențiune nu poate figura dacă prelucrarea are un caracter obligatoriu;

XXXX

ANTET **Anexa nr.3**

GHID

pentru exercitarea drepturilor de către persoanele vizate ale căror date cu caracter personal sunt prelucrate de către XXXX

XXXX prelucrează date cu caracter personal în scopurile:

1. .....
2. .....
3. .....

Legea nr. 190/2018 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) se aplică prelucrărilor de date cu caracter personal, efectuate prin mijloace automate și/sau manuale.

Definiții

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;

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;

Autoritatea națională de supraveghere este Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP), cu sediul în București str. B-dul G-ral Gheorghe Magheru 28-30 sector 1, autoritate publică cu personalitate juridică, autonomă și independentă față de orice altă autoritate publică, precum și față de orice persoană fizică sau juridică.

Potrivit prevederilor Regulamentului 679/2016, drepturile ce revin persoanei vizate sunt prevăzute în mod expres:

- dreptul la informare - art. 13-14;
- dreptul de acces la date — art. 15;
- dreptul la rectificare — art. 16;
- dreptul la ștergerea datelor (dreptul de a fi uitat) – art. 17;
- dreptul la restricționarea prelucrării – art. 18;
- dreptul la portabilitatea datelor – art. 20;
- dreptul la opoziție — art. 21;
- dreptul de a nu fi supus unui proces decizional automatizat, inclusiv crearea de profiluri – art. 22;
- dreptul de a depune o plângere în fața unei autorități de supraveghere — art. 77;
- dreptul la o cale de atac judiciară împotriva unei autorități de supraveghere – art. 78;
- dreptul la o cale de atac împotriva unui operator sau unei persoane împuternicite de operator – art. 79.

Informarea persoanei vizate este reglementată prin art. 13-14 din Regulamentul nr. 679/2016.

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

- identitatea și datele de contact ale operatorului și, după caz, ale reprezentantului acestuia;
- datele de contact ale responsabilului cu protecția datelor, după caz;
- scopurile în care sunt prelucrate datele cu caracter personal, precum și temeiul juridic al prelucrării;
- categoriile de date cu caracter personal vizate;
- destinatarii sau categoriile de destinatari ai datelor cu caracter personal, după caz;
- dacă este cazul, intenția operatorului de a transfera date cu caracter personal către un destinatar dintr-o țară terță sau o organizație internațională și existența sau absența unei decizii a Comisiei privind caracterul adecvat sau, în cazul transferurilor menționate la articolul 46 sau 47 sau la articolul 49 alineatul (1) al doilea paragraf, o trimitere la garanțiile adecvate sau corespunzătoare și la mijloacele de a obține o copie a acestora, în cazul în care acestea au fost puse la dispoziție.

Dreptul de acces la date este prevăzut în art. 15 din Regulamentul 679/2016.

Orice persoană vizată are dreptul de a obține de la operator, la cerere și în mod gratuit, confirmarea faptului că datele care o privesc sunt sau nu sunt prelucrate de acesta. Operatorul este obligat, în situația în care prelucrează date cu caracter personal care privesc solicitantul, să comunice acestuia, împreună cu confirmarea, cel puțin 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, în special destinatari din țări terțe sau organizații internaționale;
- 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;
- 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;
- dreptul de a depune o plângere în fața unei autorități 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, menționat la articolul 22 alineatele (1) și (4), 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. Operatorul este obligat să comunice informațiile solicitate, în termen de 15 zile de la data primirii cererii.

Dreptul la rectificare a datelor este reglementat prin art. 16 din Regulamentul 679/2016.

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.

Dreptul la ștergerea datelor (dreptul de a fi uitat) este prevăzut la art. 17 din Regulamentul 679/2016.

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:

- datele cu caracter personal nu mai sunt necesare pentru îndeplinirea scopurilor pentru care au fost colectate sau prelucrate;
- 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;
- persoana vizată se opune prelucrării în temeiul articolului 21 alineatul (1) și nu există motive legitime care să prevaleze în ceea ce privește prelucrarea sau persoana vizată se opune prelucrării în temeiul articolului 21 alineatul (2);
- datele cu caracter personal au fost prelucrate ilegal;

- 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;
- datele cu caracter personal au fost colectate în legătură cu oferirea de servicii ale instituției informaționale menționate la articolul 8 alineatul (1).

Dreptul la restricționarea prelucrării este prevăzut la art. 18 din Regulamentul 679/2016.

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

- persoana vizată contestă exactitatea datelor, pentru o perioadă care îi permite operatorului să verifice exactitatea datelor;
- prelucrarea este ilegală, iar persoana vizată se opune ștergerii datelor cu caracter personal, solicitând în schimb restricționarea utilizării lor;
- 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
- persoana vizată s-a opus prelucrării în conformitate cu articolul 21 alineatul (1), pentru intervalul de timp în care se verifică dacă drepturile legitime ale operatorului prevalează asupra celor ale persoanei vizate.

În cazul în care prelucrarea a fost restricționată în temeiul alineatului precedent, 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.

O persoană vizată care a obținut restricționarea prelucrării în temeiul primului alineat este informată de către operator înainte de ridicarea restricției de prelucrare.

Dreptul la portabilitatea datelor este prevăzut la art. 20 din Regulamentul 679/2016.

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:

- 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
- prelucrarea este efectuată prin mijloace automate.

Dreptul de opoziție este prevăzut la art. 21 din Regulamentul nr. 679/2016.

Persoana vizată are dreptul de a se opune în orice moment, din motive întemeiate și legitime legate de situația sa particulară, ca date care o vizează să facă obiectul unei prelucrări, cu excepția cazurilor în care există dispoziții legale contrare. In caz de opoziție justificată prelucrarea nu mai poate viza datele în cauză. Persoana vizată are dreptul de a

se opune în orice moment, în mod gratuit și fără nici o justificare, ca datele care o vizează să fie prelucrate în scop de marketing direct, în numele operatorului său al unui terț, sau să fie dezvăluite unor terți într-un asemenea scop.

Dreptul de a nu fi supus unui proces decizional automatizat, inclusiv crearea de profiluri este prevăzut la art. 22 din Regulamentul 679/2016.

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.

Această prevedere nu se aplică în cazul în care decizia:

- este necesară pentru încheierea sau executarea unui contract între persoana vizată și un operator de date;
- 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
- are la bază consimțământul explicit al persoanei vizate.

Dreptul de a depune o plângere în fața unei autorități de supraveghere este prevăzut la art. 77 din Regulamentul nr. 679/2016.

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.

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.

Dreptul la o cale de atac judiciară împotriva unei autorități de supraveghere este prevăzut la art. 78 din Regulamentul 679/2016.

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.

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 în temeiul articolelor 55 și 56 nu tratează o plângere sau nu informează persoana vizată în termen de trei luni cu privire la progresele sau la soluționarea plângerii depuse în temeiul articolului 77.

Acțiunile introduse împotriva unei autorități de supraveghere sunt aduse în fața instanțelor din statul membru în care este stabilită autoritatea de supraveghere.

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.

Dreptul la o cale de atac împotriva unui operator sau unei persoane împuternicite de operator este prevăzut la art. 79 din Regulamentul 679/2016.

Fără a aduce atingere vreunei căi de atac administrative sau nejudiciare disponibile, inclusiv dreptului de a depune o plângere la o autoritate de supraveghere în temeiul articolului 77, 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.

Acțiunile introduse împotriva unui operator sau unei persoane împuternicite de operator sunt prezentate în fața instanțelor din statul membru unde operatorul sau persoana împuternicită de operator 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 sau persoana împuternicită de operator este o autoritate publică a unui stat membru ce acționează în exercitarea competențelor sale publice.

Pentru exercitarea drepturilor prevăzute de Regulamentul 679/2016, referitoare la prelucrări de date cu caracter personal efectuate în cadrul XXXX puteți transmite o cerere întocmită în formă scrisă, datată și semnată la adresa .....sau o puteți depune personal la .....

XXXX, în calitate de operator de date cu caracter personal este obligată să comunice informațiile solicitate, în termen de 30 zile de la data primirii cererii.

În vederea apărării drepturilor prevăzute de Regulamentul nr. 679/2016, persoanele ale căror date cu caracter personal fac obiectul unei prelucrări efectuate în cadrul XXXX, pot înainta plângere către A.N.S.P.D.C.P. la sediul acesteia din Strada B-dul G-ral Gheorghe Magheru 28-30 sector 1 București, e-mail : anspdcp@dataprotection.ro.

Plângerea se poate face direct sau prin reprezentant.

Plângerea către A.N.S.P.D.C.P. nu poate fi înaintată mai devreme de 30 zile de la înaintarea unei solicitări/sesizări cu același conținut către XXXX.

Pentru informații suplimentare ne puteți contacta la: numărul de telefon:.....

e-mail: .....

11. ANEXA 11 -

REGULAMENT DE ORDINE INTERIOARĂ

ANEXA

privind protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date conform prevederilor Regulamentului UE 2016/679

I. DISPOZIŢII GENERALE

Art.1. Prezenta anexă la Regulamentul de Ordine Interioară este întocmit de *(denumirea organizației)* cu consultarea angajaților și se aplică tuturor angajaților din cadrul organizației indiferent de atribuțiile pe care le îndeplinesc, locul de muncă și de durata contractului de muncă.

Art.2. Prezenta Anexa transpune, în general, prevederi din actele normative, precum:

- 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 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 .

II. DREPTURI, OBLIGAȚII ŞI RELAŢII DE SERVICIU

A. Drepturi și obligații privind prelucrarea datelor cu caracter personal

Art.3. Drepturile și obligațiile angajatorului

3.1. In conformitate cu prevederile Regulamentului nr. 679/27.04.2016 adoptat de Parlamentul European și Consiliul Uniunii Europene pentru aprobarea normelor privind protecția în ceea ce privește prelucrarea datelor cu caracter personal, precum și a normelor referitoare la libera circulație a acestui tip de date cu caracter personal (RGPD), *(denumirea organizației)*, este operator de date personale.

3.2. Acesta are dreptul să colecteze, să înregistreze, să organizeze, să stocheze, să extragă, să consulte, să utilizeze sau să proceseze în orice alt mod, oricare și toate datele cu caracter personal furnizate de angajat.

Art.4. Cum colectează Angajatorul datele cu caracter personal ale Angajatului?

4.1. Datele cu caracter personal sunt puse la dispoziție de Angajat, la angajare, dar și ulterior, ori de câte ori intervin schimbări în situația personală care conduc la modificări ale documentelor de identitate și actelor de stare civilă, componența familiei, evenimente în familie, schimbări ale adresei de domiciliu sau reședință, schimbări în calificarea profesională, absolvirea de noi cursuri de specializare și calificare, schimbări în situația medicală, etc., la eliberarea actelor de identitate noi, dar și în alte circumstanțe asemănătoare.

4.2. Angajatorul poate colecta date cu caracter personal cu privire angajat în anumite împrejurări, inclusiv:

a) în momentul în care solicită acordarea de concedii;
b) în momentul în care solicită sprijin din partea Angajatorului;
c) în momentul în care utilizează rețeaua internet disponibilă pentru atribuțiile de serviciu;
d) la transmiterea și/sau primirea corespondenței e-mail de serviciu;
e) pentru participarea la evenimente sau cursuri puse la dispoziție de Angajator;
f) pentru autorizare în cadrul procedurilor de acces în clădire;
g) pentru derularea unor proceduri judiciare sau de executare silită asupra veniturilor angajatului, din partea terților;
h) la stabilirea unor împrejurări care afectează activitatea și/sau obiectivele Angajatorului, cum ar fi: concurența neloială, conflictul de interese, abaterile disciplinare, fapte de natură penală;
i) pentru identificarea abaterilor de la regulile stabilite de Angajator, conform legii;
j) pentru asigurarea de măsuri privind supravegherea sănătății Angajaților;
k) pentru controlul obligatoriu de medicina muncii și derularea activității de supraveghere în domeniul sănătății și securității în muncă;
l) pentru controlul psihologic obligatoriu;
m) la evaluarea și monitorizarea performanței profesionale, respectiv pentru stabilirea atribuțiilor și responsabilităților;
n) atunci când Angajații comunică cu alți Angajați între structurile de personal organizate sau cu alte persoane fizice și entități juridice în interesul activităților Angajatorului;
o) evidență contabilă și salarizare, stabilirea și plata taxelor și impozitelor prevăzute de lege, stabilirea și acordarea altor drepturi prevăzute de lege pentru Angajați, evidența vechimii în muncă și a stagiilor de cotizare, arhivarea dosarului de personal și a evidenței contabile în legătură cu salariul și componentele acestuia, în scopul prevenirii fraudelor, etc.

4.3. În anumite situații, Angajatorul colectează date cu caracter personal cu privire la angajat de la o sursă terță. Spre exemplu, de la entități juridice cu care angajații au avut relații de muncă, de asociere, afiliere, legături de afaceri, agenții guvernamentale, birouri de credit, furnizori de informații sau servicii sau din arhivele publice (Portalul instanțelor de judecată, Registrul Comerțului, ANAF, DITL, altele).

Art.5. Ce date colectează Angajatorul?

5.1. Pentru a ne îndeplini obiectul de activitate, pentru îndeplinirea obligațiilor legale și în scopul pentru care ați fost angajat, nu colectăm mai multe date cu caracter

personal față de cât este necesar și nu colectăm integral toate datele cu caracter personal de la fiecare persoană.

5.2. Datele cu caracter personal sunt informații referitoare la o persoană fizică, identificată sau identificabilă, direct sau indirect.

5.3. Angajatorul colectează și procesează următoarele categorii de date:

a) date de identificare: nume, prenume, CNP, seria și numărul actului de identitate, al pașaportului, al permisului de conducere, al cardului de sănătate și alte informații conținute în acestea (de exemplu, data și locul nașterii, cetățenia, sexul), adresa de domiciliu, adresa de corespondență, e-mail, telefon (fix, mobil, fax), identificator online, situație militară, date din actele de stare civilă, numărul de marcă;
b) profesia, numele și prenumele membrilor de familie și data nașterii (inclusiv copiii), numele și prenumele foștilor membri de familie, numele și prenumele unor terțe persoane aflate în legătură cu angajatul (conținute în hotărâri judecătorești sau în proceduri de executare silită), în întreținere, situația familială sau evenimente de familie;
c) locul muncii, experiență profesională (acte studii, calificări, specializări) notificări, preavize în caz de demisie și concediere, durata concediului de odihnă, condițiile de muncă, situații de conflict de interese ori de concurență neloială, rezultate obținute la testări, examene sau evaluări, conflicte la locul de muncă, conținutul clauzelor contractuale, planul de carieră al Angajatului, altele asemenea;
d) categorii de date cu caracter special, date privind confesiunea religioasă, apartenența sindicală, date privind starea de sănătate, date personale referitoare la fapte penale sau contravenții, date biometrice, date privind convingerile filozofice, opiniile politice, date privind viața sexuală sau orientarea sexuală.
e) informațiile care aparțin vieții dumneavoastră profesionale;
f) informații de natură financiară (de exemplu, venituri, taxe, ajutoare, istoricul veniturilor, data și numărul dosarului de pensie, datele bancare, conturile bancare, cardurile), veniturile și alte beneficii obținute de la Angajator, rețineri salariale, prejudicii produse Angajatorului sau terților, date privind plățile, cum ar fi datele necesare în vederea prelucrării plăților salariilor și a oricăror alte venituri; executări silite asupra veniturilor din salarii, plăți efectuate;
g) informații suplimentare prelucrate în mod obligatoriu într-un proiect sau raport sau comunicate în mod voluntar de către dumneavoastră, cum ar fi instrucțiuni acordate, solicitări și proiecte în care ați fost implicat, desfășurarea activității, integral;
h) informații privind acțiunile în instanță/executare îndreptate împotriva dumneavoastră sau inițiate de dumneavoastră în relațiile de muncă și de familie; acțiuni în instanță demarate împotriva dumneavoastră sau a rudelor și/sau afinilor dumneavoastră și interacțiunea cu dumneavoastră, care s-ar putea dovedi relevante în conflictul de interese;
i) informații colectate din surse publice, baze de date de integritate și birouri de credit, informații primite de la autorități sau persoane care exercită funcții sau servicii publice (avocați, notari, executori, alții);
j) orarul intrărilor și ieșirilor din sediile unde Angajatorul își desfășoară activitatea;
k) informații referitoare la locația efectuării anumitor operațiuni: alimentare card benzină/motorină, locații și deplasare monitorizată pentru autovehiculele aflate în proprietatea Angajatorului;
l) informații rezultate în urma înregistrării audio, și meta date stocate pe serverele Angajatorului;

m) semnătura;
n) orice alte informații care derivă din acestea în urma prelucrărilor efectuate de Angajator (cum ar fi: istoricul profesional, segmentarea pe categorii de Angajați, segmentarea pe categorii de vârstă a copiilor Angajaților);
o) orice alte informații care sunt necesare desfășurării activității Angajatorului.

Art.6 Cum utilizează datele Angajatorul?

6.1. Datele cu caracter personal ale Angajatului vor fi utilizate în evidența internă a *(denumirea organizației)*, și anume: evidențele financiar-contabile, evidența resurselor umane, REGES / REVISAL, SSM și SU etc., precum și în formele de evidență ale furnizorilor externi ai *(denumirea organizației)* care prestează servicii financiar-contabile, servicii SSM și SU *(acolo unde este cazul)*, servicii medicale, de eliberare tichete de masă, tichete cadou sau vouchere, de telefonie mobilă, evidențele trimise instituțiilor naționale (Casa de Pensii, Casa de Asigurări de Sănătate etc.), pentru evaluarea activității profesionale, pentru prevenirea și sancționarea abaterilor de la dispozițiile legale sau contractuale, în special a fraudelor, pentru localizarea bunurilor sustrase, pentru asigurarea pazei incintelor Angajatorului, pentru prevenirea și probarea eventualelor sustrageri ale bunurilor Angajatorului sau ale Angajaților, inclusiv pentru prevenirea și combaterea actelor de sabotaj intern, sustragere de informații ori pentru îndeplinirea unor obligații legale sau solicitări din partea instituțiilor statului, precum și pentru apărarea intereselor legitime ale Angajatorului.

6.2. Informațiile furnizate de Angajat vor fi stocate pe întreaga durată de existență a *(denumirea organizației)*, putând fi păstrate de entitatea rezultată în urma fuziunii, divizării / desprinderii (dacă este cazul), după cum urmează:.

a) Datele din cartea de identitate sau pașaport, din certificatul de naștere, din actele de studii, funcția ocupată în cadrul organizației și veniturile obținute – pentru 50 de ani, conform dispozițiilor legale privind arhivarea datelor necesare calculării drepturilor de pensie;
b) Datele de supraveghere video – 30 de zile de la înregistrare, după care sunt șterse automat de către sistem;
c) Toate celelalte categorii de datele – fie la împlinirea a 3 ani de la încetarea raporturilor de muncă, fie la finalizarea eventualelor dispute pentru care este necesară folosirea acestor date ca mijloace de probă.

6.3. Datele cu caracter personal furnizate de Angajat nu vor fi folosite în scop publicitar sau pentru a primi mesaje nesolicitate și nu vor fi transmise altor persoane, cu excepția cazurilor prevăzute în mod expres în lege.

Art.7 Drepturile și obligațiile Angajatului

7.1. În activitatea curentă Angajatul va interfera și va avea acces la informații și date cu caracter personal (orice date care conduc direct sau indirect la identificarea unei persoane sau o pot face identificabilă), acestea fiind orice tip de informații care fac referire la o persoană și pentru care este necesară păstrarea secretului profesional în scopul respectării legii.

7.2. Angajatul poate procesa date cu caracter personal atât în numele Angajatorului, aceasta fiind în calitate de operator, cât și în numele altor instituții care au calitatea de operator colaborator, le poate transmite unei persoane împuternicite de către

organizația Operator (Angajator) sau altor destinatari. Angajatul va utiliza datele cu caracter personal în limita atribuțiilor încredințate de Angajator.

7.3. Angajatul:

a) este obligat să respecte secretul profesional și confidențialitatea asupra oricăror aspecte ale activității sale, în condițiile legii, ale Regulamentului intern și ale procedurilor, politicilor de confidențialitate și instrucțiunilor primite din partea Angajatorului; această obligație include păstrarea secretului profesional cu privire la datele cu caracter personal la care a avut acces, respectiv:
   - date cu caracter personal referitoare la persoane vizate, reprezentanții organizației, angajați, angajații persoanelor împuternicite, angajații altor operatori de date și orice altă persoană fizică, așa cum acestea sunt menționate în procedurile și politicile interne comunicate periodic de Angajator; spre exemplu: numele și prenumele, data nașterii, locul nașterii, cod numeric personal, serie și număr carte de identitate, adresa domiciliului/rezidența, telefon, e-mail, corespondența primită/purtată, date despre copii, membri de familie, locuință, fotografii, înregistrări video și sistem CCTV, altele.
   - categorii de date cu caracter special, date cu caracter personal sensibile; spre ex: date referitoare la datele medicale, rasa, etnia, orientarea politică, religia, convingerile filozofice, apartenența sindicală, date privind starea de sănătate, date despre viața sexuală sau orientarea sexuală, date personale referitoare la fapte penale sau contravenții, date genetice și biometrice, altele.
   - informațiile care aparțin vieții private a unei persoane, precum și informațiile referitoare la viața profesională sau publică;

b) are obligația de respectare a procedurilor de securitate și a politicilor organizației, a tuturor normelor care îi vor fi comunicate în legătură cu postul ocupat, inclusiv cele cu privire la securitatea informațiilor și protecția datelor cu caracter personal;

c) are obligația de a respecta dreptul la propria imagine, la viață intimă, familială și privată a persoanelor cu care interferează în activitatea profesională, precum și secretul corespondenței;

d) trebuie să dea dovadă de onestitate, probitate, corectitudine, confidențialitate;

e) participă la toate formele specifice de pregătire și perfecționare profesională organizate sau plătite de Angajator, inclusiv la sesiunile de instruire cu privire la implementarea proceselor de protecție a datelor cu caracter personal;

f) respectă dispozițiile din documentele interne ale organizației, procedurile și politicile interne comunicate periodic de Angajator sau de persoanele desemnate în acest scop de Angajator, cum ar fi: regulament de ordine interioară, decizii, dispoziții, instrucțiuni de lucru;

g) este obligat să se supună controlului și evaluărilor periodice ale Angajatorului cu privire la protecția datelor cu caracter personal, modalitatea în care le prelucrează, scopul, categoriile de date prelucrate, mijloacele prelucrării, limitările utilizării datelor și orice detalii pe care Angajatorul va considera necesar să le auditeze, verifice, evalueze, controleze;

h) utilizează corect dotările și facilitățile puse la dispoziție de Angajator (mașină, telefon, card, computer etc), iar la încetarea raporturilor de muncă le restituie pe bază de proces-verbal de predare-primire, după ce în prealabil au fost eliminate toate elementele ce țin de viața privată a Angajatului și datele sale personale;

i) respectă toate regulile de securitate proprii organizației, dar și pe cele privind accesul în clădiri și spații aparținând acesteia, în locurile unde își desfășoară activitatea sau unde se deplasează în interes de serviciu, publice sau private, acceptând faptul că îndeplinirea atribuțiilor de serviciu are drept consecință prelucrarea datelor sale cu caracter personal de către Angajator sau de către alți operatori asociați sau împuterniciți - terți, iar în unele situații Angajatul poate face obiectul filmărilor, înregistrărilor audio (voce) sau video, fotografiilor, comunicărilor interne, dezvăluirii datelor despre familie, copii, date medicale sau orice alte date care trebuie procesate în scopul și în măsura necesară îndeplinirii unei obligații legale care revine operatorului sau al îndeplinirii obligațiilor contractuale ale Angajatorului; în măsura în care aceste prelucrări nu au drept temei îndeplinirea unei obligații legale sau a obligațiilor contractuale ce revin Angajatorului (sau alt temei prevăzut de RGPD), aceste prelucrări vor fi efectuate numai în temeiul consimțământului exprimat de angajat.

j) în condițiile în care este victima unui incident de securitate informațională sau cu privire la datele personale ale organizației ori dacă sesizează un incident cu privire la datele personale aparținând unei alte persoane față de care Angajatorul are obligații/răspunderi specifice unui operator sau împuternicit, va aduce la cunoștința Angajatorului incidentul, potrivit procedurilor specifice și în termenul înscris în procedură;

k) cooperează cu Angajatorul și/sau cu ceilalți angajați, atât timp cât este necesar, pentru a face posibilă realizarea oricăror măsuri sau cerințe dispuse de către Autoritatea Națională pentru Supravegherea și Protecția Datelor cu Caracter Personal;

l) cooperează, atât timp cât este necesar, cu Angajatorul și/sau cu ceilalți angajați sau prestatori, pentru a permite Angajatorului să se asigure că mediul de muncă și condițiile de lucru sunt sigure și fără riscuri pentru securitate și sănătate și pentru protecția datelor personale în domeniul său de activitate;

m) este dator să își decline calitatea și să își probeze identitatea în fața tuturor persoanelor cu care interferează în interes profesional, în interesul atribuțiilor și sarcinilor primite, dar și în fața instituțiilor și autorităților statului cu care poate intra în contact;

n) la încetarea raporturilor de muncă va preda integral, pe bază de proces-verbal, în vederea arhivării, toate documentele aferente activității depuse referitoare la datele cu caracter personal și securitatea informației. Predarea pe bază de proces verbal, numerotat și datat, a documentelor menționate mai sus are semnificația faptului ca începând cu acel moment Angajatul nu mai are acces și nu mai prelucrează datele cu caracter personal aferente activității depuse. Cu toate acestea, Angajatul este ținut în continuare de obligația de confidențialitate cu privire la securitatea informațiilor și protecția datelor cu caracter personal la care a avut acces în executarea atribuțiilor de serviciu. Obligațiile Angajatului de păstrare a confidențialității și de respectare a secretului profesional cu privire la securitatea informației și protecția datelor cu caracter personal la care a avut acces în exercitarea funcției/atribuțiilor de muncă subzistă încetării raporturilor de muncă fiind în continuare răspunzător de orice prelucrare ilegală și/sau dezvăluire neautorizată efectuată în legătură cu munca depusă sau datele cu caracter personal la care a avut acces;

o) la încetarea raporturilor de muncă, în ultima zi de lucru, va preda, pe bază de proces-verbal, toate instrumentele, dispozitivele, laptop, calculator, computer, telefon, unități externe de stocare, mașină, aferente activității depuse, dar după ce în

prealabil acestea au fost supuse proceselor de eliminare a stocării datelor cu caracter personal ale Angajatului.

Art.8 Drepturile Angajatului privind protecția datelor cu caracter personal furnizate Angajatorului *(denumirea organizației)* sunt următoarele:

8.1. **dreptul de acces la date** – orice persoană vizată are dreptul de a obține de la operatorul de date personale confirmarea faptului că datele care o privesc sunt/nu sunt prelucrate de către operatorul de date personale;

8.2. **dreptul la rectificare** – orice persoană vizată are dreptul la rectificarea datelor cu caracter personal inexacte care o privesc;

8.3. **dreptul la ștergerea datelor** (dreptul de a fi uitat) – orice persoană vizată are dreptul de a obține din partea operatorului de date personale ștergerea datelor cu caracter personal care o privesc, fără întârzieri nejustificate, în condițiile Regulamentului;

8.4. **dreptul la restricționarea prelucrării** – orice persoană vizată are dreptul de a obține din partea operatorului de date personale restricționarea prelucrării în condițiile prevăzute în Regulament;

8.5. **dreptul la portabilitatea datelor** -- orice persoană vizată are dreptul de a primi datele cu caracter personal care o privesc și pe care le-a furnizat operatorului de date personale 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 de date personale căruia i-au fost furnizate datele cu caracter personal în cazurile prevăzute în Regulament;

8.6. **dreptul de a retrage consimțământul** exprimat prin declarație privind furnizarea datelor personale, fără a afecta legalitatea prelucrării efectuate pe baza consimțământului înainte de retragerea acestuia, în condițiile Regulamentului;

8.7. **dreptul de a depune plângere** în fața unei autorități de supraveghere, în condițiile Regulamentului;

8.8. **dreptul la opoziție** – în orice moment, orice persoană vizată are dreptul de a se opune, din motive legate de situația particulară în care se află, prelucrării în temeiul articolului 6 alineatul (1) litera (e) sau (f), 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;

8.9. **dreptul de a nu face obiectul unei decizii bazate exclusiv pe prelucrarea automată** – orice persoană 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.

Pentru exercitarea unuia sau mai multor dintre drepturile enumerate mai sus, se poate transmite un e-mail la protectiedate@*(denumirea organizației)*.ro ori prin fax la numărul .....

12. ANEXA 12 -

ANTET

COMPLETARE ŞI MODIFICARE la FISA POSTULUI

Anexă la contractul individual de muncă înregistrat sub nr. _____

Angajatorul, ..., cu sediul în ....., înregistrată sub nr. ....., CUI/C.I.F. ....., reprezentată legal prin ..... în calitate de ....., prin Decizia ..... din data de ....., de modificare și completare a atribuțiilor angajaților în contextul 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) a decis completarea și modificarea fisei postului _____ ocupat de Angajatul

Dl/ Dna _____, posesor al cărții de identitate seria____ nr. _____, CNP _____**,** denumit în continuare **Angajatul,**

care a acceptat completarea şi modificarea fișei postului ocupat, după cum urmează:

1. Se adaugă în Fișa postului de _____ ocupat de Angajat, secțiunea:
„Alte responsabilități specifice postului", în următoarea formulare :
„În activitatea curentă Angajatul va interfera și va avea acces la informații și date cu caracter personal (orice date care conduc direct sau indirect la identificarea unei persoane sau o pot face identificabilă), acestea fiind orice tip de informații care fac referire la o persoană și pentru care este necesară păstrarea secretului profesional în scopul respectării legii.

Angajatul poate procesa date cu caracter personal în numele organizației Angajatoare, aceasta fiind în calitate de operator și le poate transmite unei persoane împuternicite de către organizația operator (Angajator), operatorilor asociați, altor destinatari. Angajatul va utiliza datele cu caracter personal în limita atribuțiilor încredințate de Angajator.
Angajatul:

- *este obligat să respecte secretul profesional și confidențialitatea asupra oricăror aspecte ale activității sale, în condițiile legii, ale Regulamentului de organizare și funcționare, ale Regulamentului de ordine interioară și ale procedurilor, politicilor de confidențialitate și instrucțiunilor primite din partea Angajatorului; această obligație include păstrarea secretului profesional cu privire la datele cu caracter personal la care a avut acces, respectiv:*
  - ✓ *date cu caracter personal referitoare la reprezentanții organizației, angajați, angajații persoanelor împuternicite, angajații altor operatori de date și orice altă persoană fizică, așa cum acestea sunt menționate în procedurile și politicile interne comunicate periodic de Angajator; spre exemplu: numele și prenumele, data nașterii, locul nașterii, cod numeric personal, serie și număr carte de identitate, adresa domiciliului/rezidență, telefon, e-mail, corespondența primită/purtată, date despre copii, membri de familie, locuință, fotografii, înregistrări video si sistem CCTV, altele.*
  - ✓ *categorii de date cu caracter special, date cu caracter personal sensibile; spre ex: date referitoare la datele medicale, rasa, etnia, orientarea politică, religia, convingerile filozofice sau de natură similară, apartenența sindicală, date privind starea de sănătate, date despre viața sexuală, CNP, date personale referitoare la fapte penale sau contravenții, date genetice și biometrice, altele.*
  - ✓ *informațiile care aparțin vieții private a unei persoane, precum și informațiile referitoare la viața profesională sau publică;*
- *are obligația de respectare a procedurilor de securitate și a politicilor organizației, a tuturor normelor care îi vor fi comunicate în legătură cu postul ocupat, inclusiv cele cu privire la securitatea informațiilor și protecția datelor cu caracter personal;*
- *are obligația de a respecta dreptul la propria imagine, la viață intimă, familială și privată al persoanelor cu care interferează în activitatea profesională, precum și secretul corespondenței;*
- *trebuie să dea dovadă de onestitate, probitate, corectitudine, confidențialitate;*
- *participă la toate formele specifice de pregătire și perfecționare profesională organizate sau plătite de Angajator, inclusiv la sesiunile de instruire cu privire la implementarea proceselor de protecție a datelor cu caracter personal;*
- *respectă documentele interne ale instituției, procedurile și politicile interne comunicate periodic de Angajator sau de persoanele desemnate în acest scop de Angajator, cum ar fi: regulament de ordine interioara, decizii, dispoziții, instrucțiuni de lucru;*
- *este obligat să se supună controlului și evaluărilor periodice ale Angajatorului cu privire la protecția datelor cu caracter personal, modalitatea în care le prelucrează, scopul, categoriile de date prelucrate, mijloacele prelucrării, limitările utilizării datelor și orice detalii pe care Angajatorul va considera necesar să le auditeze, verifice, evalueze, controleze;*
- *utilizează corect dotările și facilitățile puse la dispoziție de Angajator (telefon, card, computer etc), iar la încetarea raporturilor de muncă le restituie pe bază de proces-*

verbal de predare-primire, după ce în prealabil au fost eliminate toate elementele ce țin de viața privată a Angajatului și datele sale personale;

- *respectă toate regulile de securitate proprii organizației, dar și pe cele privind accesul în clădiri și spații aparținând organizației, în locurile unde își desfășoară activitatea sau unde se deplasează în interes de serviciu, publice sau private, acceptând faptul că îndeplinirea atribuțiilor de serviciu are drept consecință prelucrarea datelor sale cu caracter personal de către Angajator sau de către alți operatori asociați sau împuterniciți - terți, iar în unele situații Angajatul poate face obiectul filmărilor, înregistrărilor audio (voce) sau video, fotografiilor, comunicărilor interne, dezvăluirii datelor despre familie, copii, date medicale sau orice alte date care trebuie procesate în scopul si în măsura necesară îndeplinirii unei obligații legale care revine operatorului sau al îndeplinirii obligațiilor contractuale ale Angajatorului; în măsura în care aceste prelucrări nu au drept temei îndeplinirea unei obligații legale sau a obligațiilor contractuale ce revin Angajatorului (sau alt temei prevăzut de Regulamentul general privind protecția datelor, aceste prelucrări vor fi efectuate numai în temeiul consimțământului exprimat de angajat.*
- *în condițiile în care este victima unui incident de securitate informațională sau cu privire la datele personale ale instituției ori dacă sesizează un incident cu privire la datele personale aparținând unei alte persoane fata de care Angajatorul are obligații/răspunderi specifice unui operator sau împuternicit, va aduce la cunoștința Angajatorului incidentul, potrivit procedurilor specifice și în termenul înscris în procedură;*
- *cooperează cu Angajatorul și/sau cu ceilalți angajați, atât timp cât este necesar, pentru a face posibilă realizarea oricăror măsuri sau cerințe dispuse de către Autoritatea Națională pentru Supravegherea Prelucrării Datelor cu Caracter Personal;*
- *cooperează, atât timp cât este necesar, cu Angajatorul și/sau cu ceilalți angajați sau prestatori, pentru a permite Angajatorului să se asigure că mediul de muncă și condițiile de lucru sunt sigure și fără riscuri pentru securitate și sănătate și pentru protecția datelor personale în domeniul său de activitate;*
- *este dator să își decline calitatea și să își probeze identitatea în fața tuturor persoanelor cu care interferează în interes profesional, în interesul atribuțiilor și sarcinilor primite, dar și în fața instituțiilor și autorităților statului cu care poate intra în contact;*
- *la încetarea raporturilor de muncă va preda integral, pe bază de proces-verbal, în vederea arhivării, toate documentele aferente activității depuse referitoare la datele cu caracter personal și securitatea informației. Predarea pe bază de proces verbal, numerotat și datat, a documentelor menționate mai sus are semnificația faptului că începând cu acel moment Angajatul nu mai are acces și nu mai prelucrează datele cu caracter personal aferente activității depuse. Cu toate acestea, Angajatul este ținut în continuare de obligația de confidențialitate cu privire la securitatea informațiilor și protecția datelor cu caracter personal la care a avut acces în executarea atribuțiilor de serviciu. Obligațiile Angajatului de păstrare a confidențialității și de respectare a secretului profesional cu privire la securitatea informației și protecția datelor cu caracter personal la care a avut acces în exercitarea funcției/atribuțiilor de muncă subzistă încetării raporturilor de muncă fiind în continuare răspunzător de orice prelucrare ilegală și/sau dezvăluire neautorizată efectuată în legătură cu munca depusă sau datele cu caracter personal la care a avut acces;*

- *la încetarea raporturilor de muncă, în ultima zi de lucru, va preda, pe bază de proces-verbal, toate instrumentele, dispozitivele, laptop, calculator, computer, telefon, unități externe de stocare, aferente activității depuse, dar după ce în prealabil acestea au fost supuse proceselor de eliminare a stocării datelor cu caracter personal ale Angajatului."*

2. În completarea atribuțiilor și responsabilităților din Fișa postului, se adaugă secțiunea intitulată „Răspunderi/interdicții privind securitatea informației și datele cu caracter personal", în următoarea formulare:

„Angajatul poate răspunde penal, material, administrativ sau disciplinar pentru încălcarea atribuțiilor sau sarcinilor de muncă primite, pentru nerespectarea Regulamentelor instituției, a Politicilor privind protecția datelor cu caracter personal, a Procedurilor interne privind securitatea informației și a Procedurilor interne privitoare la păstrarea secretului profesional cu privire la datele cu caracter personal.

Interdicții:

- *Nu poate dezvălui către nici o persoană și pentru nici un motiv informații despre organizație, angajați, persoanele vizate date cu caracter personal, altele decât cele necesare pentru îndeplinirea atribuțiilor de muncă, potrivit cerințelor postului ocupat.*
- *Nu poate furniza relații nici unei autorități sau persoane cu privire la informațiile de care a luat cunoștință sau care i-au fost încredințate, inclusiv datele cu caracter personal la care a avut acces în exercitarea atribuțiilor de muncă, fără acordul prealabil, expres și scris din partea organizației, în condițiile legii, Regulamentelor și normelor specifice interne aplicabile.*

Răspunderi și sancțiuni:

Încălcarea atribuțiilor sau sarcinilor de serviciu primite și a Politicilor privind protecția datelor cu caracter personal, a Procedurilor interne privind securitatea informației și a Procedurilor interne privitoare la păstrarea secretului profesional cu privire la datele cu caracter personal atrag răspunderea juridică a angajatului, în oricare dintre formele prevăzute de legislația în vigoare.

*Angajații răspund **disciplinar** pentru nerespectarea prevederilor legii și ale reglementării legale privind activitatea persoanei juridice Angajatoare. Încălcarea de către Angajații organizației a prevederilor prezentei Politici, constituie abatere disciplinara și se sancționează, în funcție de gravitatea faptei.*

Constatarea abaterii disciplinare, cercetarea acesteia, procedura de judecată sunt prevăzute în: Codul Muncii și Regulamentul de ordine interioara al organizației.

*Pentru nerespectarea de către salariat a legii, a Regulamentului de ordine interioara, a Politicilor și Procedurilor de securitate, a Politicilor, Procedurilor și instrucțiunilor privind protecția datelor cu caracter personal, Angajatorul are dreptul de a recupera de la Angajați pagubele pricinuite, în temeiul răspunderii **patrimoniale**.*

*Dacă prin aceeași fapta, salariatul săvârșește o contravenție (prevăzută expres de lege), dar încalcă și normele de disciplină, cele două forme de răspundere juridică se pot cumula (răspunderea disciplinară și cea **contravențională**). Dacă fapta salariatului constituie o infracțiune, aceasta va fi sancționată conform legii penale, răspunderea **penală** a angajatului urmând a fi atrasă în condițiile legii.*

Prezentul act a fost întocmit, a intrat în vigoare și a fost semnat de părți astăzi, _____, în două exemplare originale.

ANGAJATOR, **ANGAJAT,**

.....organizația..... *nume și prenume*

prin *....funcția*

....nume și prenume.....…

13. ANEXA 13 -

ANTET

APROBAT

funcție
nume, prenume, semnătură

PROCEDURA DE RĂSPUNS ÎN CAZ DE ÎNCĂLCARE A DATELOR
Cod: .....

Ediția I, .../.../....., Revizia

AVIZAT
PREȘEDINTELE COMISIEI DE MONITORIZARE
nume, prenume, semnătură

ELABORAT DPO
funcția
nume, prenume, semnătură

Cuprins

1. Scopul procedurii

Prezenta procedură stabilește principiile și acțiunile generale pentru gestionarea cu succes a răspunsului la o încălcare a datelor, precum și pentru îndeplinirea obligațiilor privind notificarea către Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal și persoanele fizice, conform cerințelor Regulamentului 679/2016.
Această procedură oferă principii generale și un model de abordare pentru a răspunde și a atenua încălcări ale datelor cu caracter personal (o „încălcare a datelor cu caracter personal").
Această procedură se aplică și pentru orice alt tip de incident de securitate.

2. Domeniul de aplicare

Această procedură se aplică tuturor salariaților XXXX implicați în procese de prelucrare a datelor cu caracter personal, atât ale angajaților proprii cât și persoanelor vizate externe instituției (Clienți, Reprezentanți parteneri, etc).

3. Documente de referință

- 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 (Regulamentul general privind protecția datelor);
- LEGE nr. 190 din 18 iulie 2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 al Parlamentului European şi 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);
- Politica privind Securitatea Informațiilor;
- Politica de Protecție a Datelor cu Caracter Personal.

4. Definiții și Abrevieri

Definiții

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 datelor cu caracter personal 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;
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;
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;
Persoană împuternicită de operator înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care prelucrează datele cu caracter personal în numele operatorului;
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;

Abrevieri
RGPD – Regulamentul (UE) 679/2016
DPO – Responsabil cu protecția datelor
XXXX – denumirea organizației

5. Descrierea activităților

5.1. Procesul de răspuns în caz de încălcare a datelor

5.1.1. Acest proces este inițiat atunci când cineva observă că există o încălcare a datelor, situație în care, toți membrii Echipei de răspuns în caz de încălcare a datelor sunt notificați. Echipa este responsabilă să determine dacă încălcarea ar trebui considerată o încălcare a datelor cu caracter personal.

5.1.2. Echipa de răspuns în caz de încălcarea a datelor trebuie să fie pregătită să răspundă la o încălcare a datelor, 24/7, pe tot parcursul anului. Prin urmare, detaliile de contact pentru fiecare membru al Echipei de răspuns în caz de încălcarea a datelor, inclusiv datele personale de contact, vor fi stocate la

Registratură/Secretariat, urmând a fi utilizate pentru a convoca echipa de fiecare dată când se primește o notificare a unei încălcări de date.

5.1.3. Echipa de răspuns în caz de încălcarea a datelor se convoacă pentru fiecare încălcare de date raportată (și presupusă) și va fi condusă de către Conducătorul Echipei de Răspuns în Caz de Încălcarea a Datelor.

5.2. Notificarea de încălcare a datelor cu caracter personal: Persoana împuternicită către operator

5.2.1. Atunci când încălcarea datelor cu caracter personal afectează datele cu caracter personal care sunt procesate în numele unei terțe părți, Responsabilul cu Protecția Datelor al organizației care acționează ca o persoană împuternicită trebuie să raporteze orice încălcare a datelor cu caracter personal către operatorul/operatorii de date respectiv(i), fără întârzieri nejustificate.

5.2.2. Responsabilul cu Protecția Datelor va trimite notificarea către operator, care va include următoarele:

- ✓ Descrierea naturii încălcării
- ✓ Categoriile de date cu caracter personal afectate
- ✓ Numărul aproximativ al persoanelor vizate afectate
- ✓ Numele și datele de contact ale conducătorului Echipei de răspuns în caz de încălcare a datelor (Responsabilului cu Protecția Datelor)
- ✓ Consecințele încălcării datelor cu caracter personal
- ✓ Măsuri luate pentru a aborda încălcarea datelor cu caracter personal
- ✓ Orice informație referitoare la încălcarea datelor

5.3. Notificarea de încălcare a datelor cu caracter personal: Operatorul către Autoritatea de Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal

5.3.1. Atunci când încălcarea datelor cu caracter personal afectează datele cu caracter personal care sunt prelucrate de către organizație în calitate de operator, se efectuează următoarele acțiuni de către Responsabilul cu Protecția Datelor:

- ✓ Organizația trebuie să stabilească dacă încălcarea datelor cu caracter personal trebuie raportată Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal.
- ✓ Pentru a stabili riscul pentru drepturile și libertățile persoanei vizate afectate, Responsabilul cu Protecția Datelor trebuie să efectueze Evaluarea Impactului privind Protecția Datelor asupra activității de prelucrare afectată de încălcarea datelor
- ✓ Dacă încălcarea datelor cu caracter personal nu este probabil să ducă la un risc pentru drepturile și libertățile persoanelor vizate, nu este necesară nicio notificare. Cu toate acestea, încălcarea datelor ar trebui să fie înregistrată în Registrul Încălcărilor de Date.
- ✓ Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal trebuie notificată fără întârziere nejustificată, dar nu mai târziu de 72 de ore, în cazul în care încălcarea datelor cu caracter personal este

susceptibilă să ducă la un risc pentru drepturile și libertățile persoanelor vizate afectate de încălcarea datelor cu caracter personal. Orice motive posibile pentru întârzierea după 72 de ore trebuie comunicate Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal.

5.3.2. Operatorul va trimite Notificări către Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal care vor include următoarele:

- ✓ Descrierea naturii încălcării
- ✓ Categoriile de date cu caracter personal afectate
- ✓ Numărul aproximativ al persoanelor vizate afectate
- ✓ Numele și datele de contact ale Conducătorului Echipei de răspuns în caz de încălcare a datelor (Responsabilul cu protecția datelor)
- ✓ Consecințele încălcării datelor cu caracter personal
- ✓ Măsuri luate pentru a aborda încălcarea datelor cu caracter personal
- ✓ Orice informații referitoare la încălcarea datelor

5.4. Notificarea de încălcare a datelor cu caracter personal: Operatorul către Persoana Vizată

5.4.1. Managerul/Directorul general trebuie să evalueze împreună cu Echipa de Răspuns dacă încălcarea datelor cu caracter personal este susceptibilă să ducă la un risc ridicat pentru drepturile și libertățile persoanei vizate. Dacă da, trebuie să notifice fără întârziere nejustificată persoanele vizate afectate.

5.4.2. Notificarea către persoanele vizate trebuie să fie scrisă în limbaj clar și simplu și trebuie să conțină aceleași informații enumerate în punctul 5.2.2.

5.4.3. În cazul în care, datorită numărului de persoane vizate afectate, este în mod disproporționat dificil să fie notificată fiecare persoană vizată afectată, Managerul/Directorul general trebuie să ia măsurile necesare pentru a se asigura că persoanele vizate afectate sunt notificate prin utilizarea corespunzătoare a canalelor publice disponibile.

6. Responsabilități

- **Managerul/Directorul general**
  - ✓ Nominalizează prin Decizie o Echipă de Răspuns în caz de încălcare a datelor care ar trebui să aibă în componență persoane cu experiență și competență din departamentul IT, Juridic, Resurse Umane și Responsabilul cu protecția datelor (DPO) . Echipa trebuie să fie numită, indiferent dacă s-a produs sau nu o încălcare.
  - ✓ Aprobă prezenta procedură.
- **Echipa de răspuns în caz de încălcare a datelor**
  - ✓ Analizează orice încălcare a datelor suspectă/presupusă sau reală care afectează instituția, sens în care trebuie să implementeze:
    - Validarea încălcării de date;
    - Asigurarea că o investigație corectă și imparțială este inițiată, condusă, documentată și încheiată;

- Identificarea cerințelor de remediere și urmărirea soluționării deciziei luate;
- Raportarea constatărilor către top management;
- Coordonarea cu autoritățile corespunzătoare dacă este necesar;
- Asigurarea că persoanele vizate afectate sunt notificate corespunzător, dacă este cazul;
- Analizarea fiecărui incident înregistrat în Registrul Încălcărilor de Date și, dacă este cazul recomandarea acțiunilor preventive sau corective.

✓ Răspunde imediat, eficient și abil pentru încălcare reală a datelor care afectează instituția;

- **Conducătorul echipei de răspuns în caz de încălcare a datelor**
  - ✓ Acesta este de regulă Responsabilul cu protecția datelor (DPO) care va coordona activitatea echipei de răspuns în caz de încălcare a datelor;
  - ✓ Poate implica în componența echipei, dacă este cazul, părți externe (de ex. un furnizor de securitate informatică);
  - ✓ Poate adăuga personal suplimentar echipei în scopul soluționării unei încălcări specifice a datelor;
  - ✓ Este responsabil pentru documentarea tuturor deciziilor echipei.

7. Dispoziții finale

Reglementările prezentei proceduri sunt obligatorii și intră în vigoare pentru toți salariații instituției (conform formularului de distribuire a procedurii) de la data aprobării, aceștia fiind obligați să le respecte începând cu data comunicării și instruirii conținutului.
Comunicarea și instruirea se vor face cu suportul Conducătorul Echipei de Răspuns în caz de încălcare a datelor, prin intermediul Șefilor de departamente/ compartimente, urmând ca dovada de instruire să fie transmisă de către Șeful departamentului/compartimentului, la termenul stabilit de conducerea instituției și comunicat odată cu informarea.
Orice persoană care încalcă această Procedură poate face obiectul unor măsuri disciplinare interne (inclusiv până la încetarea contractului de muncă); și se pot confrunta, de asemenea, cu răspundere civilă sau penală în cazul în care acțiunea lor încalcă legea.

8. Formular de analiză procedură

Nr.crt	Compartiment	Conducător compartiment	Aviz favorabil		Aviz nefavorabil		
			Semnătura	Data	Observații	Semnătura	Data

9. FORMULAR EVIDENŢĂ MODIFICĂRI

Nr. Crt.	Ed.	Data ediției	Rev.	Data reviziei	Pag.	Descriere modificare	Semnătura conducătorului compartimentului
1	1	…….	0	-	-	Întocmită conform OSGG nr.600/2018	

10. Formular distribuire procedură

Compartiment	**Conducător compartiment Nume și prenume**	**Data primirii**	**Semnătura**	**Data retragerii**	**Data intrării în vigoare a procedurii**	**Semnătura**

14. ANEXA 14 -

ANTET

APROBAT
funcție
Nume, prenume, semnătură

PROCEDURA

ACTIVITATEA DE ARHIVARE, DURATA DE STOCARE ȘI DESTINAȚIA ULTERIOARĂ A DOCUMENTELOR
Cod: .....
Ediția I, .../..../...., Revizia

AVIZAT
PREȘEDINTELE COMISIEI DE MONITORIZARE
nume, prenume, semnătură

VERIFICAT
funcția conducătorului compartimentului
nume, prenume, semnătură

ELABORAT
funcția
nume, prenume, semnătură

CUPRINS

1. SCOPUL PROCEDURII

Scopul acestei proceduri este:

- Stabilirea unui set unitar de reguli pentru reglementarea activităților de arhivare, precum și de întocmire a inventarelor arhivistice în vederea depozitării dosarelor în locația amenajată la nivelul XXXX .
- Stabilirea responsabilităților privind întocmirea, avizarea și aprobarea documentelor aferente acestor activități.

2. DOMENIU DE APLICARE

Procedura se aplică de către toate compartimentele din cadrul XXXX pentru arhivarea și păstrarea tuturor documentelor pe suport hârtie.

Prezenta procedură nu se aplică pentru arhivarea documentelor în formă electronică.

3. DOCUMENTE DE REFERINȚĂ

Legea Arhivelor Naționale nr.16/1996, cu modificările și completările ulterioare;
Regulamentul de Ordine Interioară;
Ordinul 2634/2015 privind documentele financiar-contabile.

4. DEFINIȚII ȘI ABREVIERI

DEFINIȚII

Document – orice act, text scris sau tipărit, generat sau gestionat direct de către lucrător, un compartiment/departament din cadrul organizației;

Circuitul documentelor – drumul pe care îl parcurg documentele din momentul emiterii sau intrării lor în organizație până la arhivarea acestora;

Arhivare – activitatea de preluare, opisare, îndosariere, inventariere și depunere a documentelor create de XXXX în locația amenajată la nivelul organizației;

Unitate arhivistică – grupare de documente referitoare la aceeași problemă sau activitate, care poate constitui elementul de bază în descrierea și/sau administrarea unui fond sau a unei colecții;

Fond arhivistic – ansamblul documentelor de orice natură create și primite de către o persoană juridică pe parcursul existenței sau activității sale;

Nomenclator arhivistic – listă sistematică a documentelor create și primite de către o organizație, grupate în unități arhivistice, împreună cu termenele de păstrare ale acestora, constituită conform structurii organizației sau după categorii de activități și funcții îndeplinite.

ABREVIERI

XXXX – denumire organizație/entitate

5. DESCRIEREA PROCEDURII

La nivelul organizației, atât conducerea, cât și întregul personal, denumiți în continuare creatori și deținători de documente, răspund de evidența, inventarierea, selecționarea, păstrarea și folosirea documentelor. Fiecare creator de documente proprii, are obligația să țină evidența pe categorii de documente grupate pe termene de păstrare, conform Indicativului dosarului din Nomenclatorul arhivistic al instituției.

În XXXX este creat un sistem de păstrare/arhivare exhaustiv și actualizat a documentelor, potrivit unor reguli și proceduri stabilite, în vederea asigurării conservării lor în bune condiții și pentru a fi accesibile personalului competent în a le utiliza.

Prin urmare, conducerea organizației are obligația să asigure condițiile necesare cunoașterii și respectării de către angajați a reglementărilor legale privind accesul la documente și modul de gestionare a acestora.

Depozitarea documentelor se face în spații speciale care să ofere condiții corespunzătoare de rezistență, igienă, temperatură umiditate și de securitate. Pentru protejarea împotriva degradării, documentele se introduc în cutii de carton, mape, plicuri, tuburi etc. în raport de natura și dimensiunea lor.

Creatorii de documente sunt obligați să elibereze, potrivit legii, la cererea persoanelor fizice și a persoanelor juridice, certificate, copii și extrase de pe documentele pe care le creează, dacă acestea se referă la drepturi care îl privesc pe solicitant. Aceștia au obligația să comunice în scris, în termen de 30 de zile, Arhivelor Naționale documentele care atestă înființarea, reorganizarea sau desființarea, în condițiile legii, precum și măsurile dispuse în vederea arhivării documentelor create sau deținute de organizație.

5.1. Înregistrarea și evidența documentelor

La nivelul organizației sunt definite reguli clare și sunt stabilite proceduri cu privire la înregistrarea, expedierea, redactarea, îndosarierea, protejarea și păstrarea documentelor.

Înregistrarea documentelor se realizează într-un sistem unitar, în cadrul organizației și toate compartimentele din cadrul acesteia sunt obligate să înregistreze documentele intrate/ieșite ori întocmite pentru uz intern, cronologic, în ordinea primirii lor.

5.2. Nomenclatorul arhivistic

Creatorii și deținătorii de documente sunt obligați, ca anual, să grupeze documentele în unități arhivistice, potrivit specificului și termenelor de păstrare stabilite prin Nomenclatorul arhivistic. Aceștia au obligația de a întocmi Nomenclatorul arhivistic al documentelor create și deținute. Nomenclatorul arhivistic se întocmește de către fiecare creator pentru documentele proprii și ar trebui să-l constituie ca **Anexa 1** la prezenta procedură

5.3. Gruparea documentelor în dosare pe tematici și termene de păstrare

- **Gruparea documentelor**

În vederea predării dosarelor la arhiva organizației se efectuează următoarele operațiuni:

- documentele cuprinse în dosar se ordonează cronologic în următoarea ordine: actele mai vechi trebuie să se afle deasupra și cele mai noi dedesubt;
- se îndepărtează acele, clamele, agrafele metalice, filele nescrise, dublurile;
- documentele din fiecare dosar se leagă în coperte de carton, în așa fel încât să se asigure citirea completă a textului, datelor și rezoluțiilor;
- dosarele nu trebuie să aibă mai mult de 250-300 file; în cazul depășirii acestui număr, se constituie mai multe volume ale aceluiași dosar;
- filele dosarelor se numerotează în colțul din dreapta sus; în cazul dosarelor compuse din mai multe volume, filele se numerotează începând cu numărul 1 pentru fiecare volum;
- pe coperta dosarului se înscriu: denumirea organizației și a compartimentului creator, numărul de dosar din inventar, anul, indicativul din nomenclatorul, datele de început și de sfârșit, numărul de file, volumul și termenul de păstrare;
- pe o foaie nescrisă, adăugată la sfârșitul dosarului, sau pe prima pagină nescrisă a registrelor, lucrătorul de la compartimentul creator al dosarului face următoarea certificare: „Prezentul dosar (registru) conține ..... file”, în cifre și în paranteze, în litere, după care semnează și pune data certificării.

- **Constituirea dosarelor**

Toate categoriile de personal din cadrul organizației, care în exercitarea funcțiilor și atribuțiilor de serviciu au primit documente spre rezolvare, au întocmit documente sau au primit documente spre păstrare, au obligația să constituie dosare cu acestea, să inventarieze documentele la sfârșitul anului și să le predea persoanei cu responsabilități de arhivare din organizație, în vederea pregătirii acestora pentru predarea la arhivă.

Șeful unui compartiment poate reține documente în arhiva proprie a structurii pe care o conduce, fără a le preda la arhiva organizației, în al doilea an de la constituirea acestora, dacă acestea sunt necesare desfășurării activității curente sau în cazul în care dosarul nu a fost încheiat, cu obligația de a specifica acest lucru în lista de inventariere în dreptul dosarului/documentului respectiv, cât și în procesul verbal de predare-primire al documentelor – **ANEXA 3**.

- **Inventarierea documentelor**

Documentele se depun în arhivă pe bază de inventare, conform modelului prevăzut în **Anexa 2**. Inventarul cuprinde toate dosarele cu același termen de păstrare, create în cursul

unui an, de către un compartiment de muncă. Astfel, fiecare compartiment va întocmi atâtea inventare câte termene de păstrare sunt prevăzute în nomenclator, la compartimentul respectiv.

Ulterior, în baza nomenclatorului, dosarele constituite, respectiv unitățile arhivistice, create în anul precedent vor fi perfectate, copertate și inventariate, de persoana cu responsabilități pe linie de arhivare din cadrul organizației, pe formulare conform prezentei proceduri, pe termene de păstrare, în anul în curs, urmând să fie introduse în al doilea an de la constituirea acestora, la arhiva organizației.

Inventarele se întocmesc în 3 exemplare pentru documentele temporare și în 4 exemplare pentru documentele permanente, dintre care un exemplar rămâne la compartimentul care face predarea, iar celelalte se depun o dată cu dosarele la compartimentul de arhivă.

În cazul în care există dosare neîncheiate în anul respectiv, ca și cele care, din motive justificate, se opresc la compartimentele de muncă, se trec în inventarul anului respectiv, cu menționarea nepredării lor; în momentul predării lor ulterioare, în inventar se va menționa acest lucru.

În ce privește completarea rubricii „Conținutul dosarului", se vor preciza genurile (corespondența, rapoarte, facturi, decizii etc.) de documente, emitentul, destinatarul, problema sau problemele conținute și, după caz, perioada la care se referă.

Evidența dosarelor și a inventarelor introduse în arhivă se ține în registrul de evidență a intrărilor-ieșirilor, conform modelului prevăzut în **ANEXA 4**.

- **Procesul verbal de predare-primire a dosarelor/documentelor**

Procesul verbal de predare-primire a documentelor, se face în toate situațiile în care se realizează inventarierea documentelor în cadrul organizației și se întocmește de cel care predă documentele, respectiv:

- inventarierea anuală a dosarelor/documentelor se face de către întreg personalul din cadrul organizației pentru lucrările repartizate, create și date spre păstrare, în vederea predării persoanei responsabilă cu arhivarea;
- inventarierea în vederea predării/preluării dosarelor/documentelor, la încetarea/ modificarea/suspendarea raporturilor de muncă a personalul de conducere/de execuție se face de către persoana care se află în una dintre aceste situații, în vederea predării dosarelor/documentelor înlocuitorului de drept, persoanei numită/desemnată în acest sens sau unei comisii de preluare a documentelor/dosarelor;
- inventarierea în vederea predării/preluării dosarelor/documentelor de la compartimente la arhiva organizației se face de către persoana responsabilă cu arhivarea în cadrul compartimentului;

Procesul verbal de predare-primire a dosarelor/documentelor este documentul oficial care se întocmește la predarea/preluarea documentelor de către persoana responsabilă cu inventarierea documentelor astfel:

- la plecarea din compartimentul de muncă de către persoana care face predarea dosarelor/documentelor;

- la sfârșitul anului, după inventarierea anuală, de către personalul de execuție pentru documentele proprii, în vederea predării dosarelor/documentelor persoanei cu atribuții de arhivare din cadrul compartimentului;
- la predarea dosarelor/documentelor din compartiment la arhiva organizației, de către persoana cu atribuții de arhivare din cadrul compartimentului.

Procesul verbal de predare-primire a documentelor se întocmește în 2 exemplare. Pentru predarea documentelor cu termen de păstrare permanent, procesul-verbal de predare-primire a documentelor se întocmește în 3 exemplare.

Procesul verbal de predare-primire a documentelor trebuie să aibă înscris, în partea de sus, în stânga filei, compartimentul creator al documentelor respective. În cuprinsul procesului-verbal de predare-primire se va menționa perioada în care au fost create documentele, compartimentul și numărul dosarelor efectiv predate, numărul filelor inventarului, precum și semnătura de predare și cea de preluare a documentelor.

- **Arhivarea documentelor financiar-contabile**

XXXX are obligația păstrării în arhivă a registrelor de contabilitate, a celorlalte documente contabile, precum și a documentelor justificative care stau la baza înregistrărilor în contabilitate a operațiunilor economic-financiare.

Păstrarea documentelor justificative, a registrelor de contabilitate și a celorlalte documente financiar-contabile se face pe hârtie sau pe suport electronic.

În cazul păstrării pe suport electronic a documentelor financiar-contabile, inclusiv a celor care au fost convertite din format hârtie în format electronic, nu este obligatorie aplicarea prevederilor Legii nr. 135/2007 privind arhivarea documentelor în formă electronică, cu modificările și completările ulterioare.

În cazul în care evidența contabilă este ținută cu ajutorul programelor informatice, documentele financiar-contabile se pot păstra pe suporturi tehnice, pe durata termenelor prevăzute de legislația în vigoare, cu condiția să poată fi listate în orice moment, în funcție de necesitățile entității sau la cererea organelor de control.

Arhivarea documentelor financiar-contabile în format hârtie se face în conformitate cu prevederile legale și cu respectarea următoarelor reguli generale:

- documentele se grupează în dosare, numerotate și șnuruite;
- gruparea documentelor în dosare se face cronologic și sistematic, în cadrul fiecărui exercițiu financiar la care se referă acestea. Dosarele astfel arhivate se păstrează în spații amenajate în acest scop, asigurate împotriva degradării, distrugerii sau sustragerii, dotate cu mijloace de prevenire a incendiilor.

Evidența documentelor în arhivă se ține cu ajutorul Registrului de evidență, potrivit Legii Arhivelor Naționale nr. 16/1996, cu modificările și completările ulterioare, în care sunt consemnate dosarele și documentele intrate în arhivă, precum și mișcarea acestora în decursul timpului.

Eliminarea din arhiva entității a documentelor financiar-contabile, al căror termen de păstrare a expirat, se face de către o comisie constituită potrivit procedurilor proprii ale entității. În această situație se întocmește un proces-verbal și se consemnează scăderea documentelor eliminate din Registrul de evidență al arhivei.

- **Scoaterea temporară a documentelor din arhivă**

Scoaterea temporară a documentelor din arhiva organizației se face numai cu aprobarea conducătorului acesteia, la solicitarea scrisă a șefului compartimentului creator al documentului, din care să rezulte scopul solicitării, justificarea că se impune eliberarea documentului din arhivă cât și termenul limită de returnare. În funcție de informațiile de care are nevoie, solicitantul este îndrumat să completeze o cerere pentru accesul la arhivă sau la cutiile/documentele din depozit.

În cazul unor documente de importanță majoră pentru organizație se vor elibera copii legalizate, prin grija responsabilului de arhivă.

După expirarea termenului limită specificat în cerere, solicitantul este obligat să returneze documentul/dosarul în aceeași stare în care a fost ridicat. La returnare, responsabilul de arhivă verifică integritatea și starea documentului și consemnează returnarea și starea acestuia în Registrul de depozit – **ANEXA 6**.

Documentele pot fi scoase din arhivă în scopul consultării, pe perioade limitate de timp, respectiv maximum 10 zile lucrătoare, în cazuri speciale termenul putându-se prelungi.

Creatorii și deținătorii de documente sunt obligați să elibereze, potrivit legii, la cererea persoanelor fizice sau juridice, certificate, copii și extrase după documentele pe care le creează și le dețin, chiar dacă nu au îndeplinit termenul de 30 de ani, dacă acestea se referă la drepturi care îl privesc pe solicitant, cum sunt: vechimea în muncă, studii, drepturi patrimoniale.

- **Scoaterea definitivă a documentelor din arhivă**

Scoaterea dosarelor din evidența arhivei se face cu aprobarea conducerii creatorilor sau deținătorilor de documente și cu confirmarea Arhivelor Naționale, în urma selecționării, transferului către altă unitate deținătoare sau ca urmare a distrugerii provocate de evenimente neprevăzute;

Dosarele sunt scoase din evidența arhivei pe baza unuia din următoarele acte, după caz:

- proces-verbal de selecționare;
- proces-verbal de predare-preluare – **ANEXA 7**;
- proces-verbal de constatare a deteriorării complete a documentelor sau a lipsei acestora.

Documentele deteriorate vor fi scoase din evidență în urma propunerii comisiei de selecționare, aprobată de conducerea organizației creatoare sau deținătoare și confirmată de Arhivele Naționale.

Când termenul de păstrare a documentelor în arhiva organizației a expirat, conform Nomenclatorului arhivistic sau în cazul deteriorării acestora, Comisia de Selecționare propune eliminarea lor. Aprobarea eliminării dosarelor/documentelor se face de către conducătorul organizației.

- **Selecționarea documentelor**

În cadrul organizației trebuie să funcționeze Comisia de selecționare, numită prin decizia scrisă a conducătorului organizației. Comisia de selecționare este compusă din președinte, secretar și un număr impar de membri, numiți din rândul specialiștilor proprii, reprezentând principalele compartimente creatoare de arhivă. Șeful compartimentului de arhivă (acolo unde există) sau altă persoană desemnată este de drept secretarul comisiei de selecționare.

Anual sau ori de câte ori este nevoie, la sesizarea secretarului comisiei de selecționare a documentelor, președintele convoacă comisia de selecționare. Secretarul prezintă comisiei inventarele dosarelor cu termene de păstrare expirate. În aprecierea importanței documentelor, comisia de selecționare are în vedere respectarea termenelor de păstrare a documentelor, prevăzute în Nomenclatorului arhivistic.

Când comisia de selecționare constată greșeli de încadrare a documentelor la termenele de păstrare sau stabilește ca unele dintre acestea să fie păstrate permanent, ele se menționează în inventarele corespunzătoare termenului lor de păstrare, la anul și compartimentul creator.

La încheierea lucrărilor, Comisia de selecționare întocmește procesul-verbal, care se înaintează spre aprobare conducerii organizației – **ANEXA 5**. Inventarele dosarelor propuse de Comisia de selecționare, pentru eliminarea din arhivă, însoțite de procesul-verbal aprobat de conducătorul organizației și de inventarul documentelor permanente create în perioada pentru care se efectuează selecționarea (câte un exemplar) se înaintează, cu adresă înregistrată, pentru confirmare, la Arhivele Naționale. Arhivele Naționale pot hotărî păstrarea permanentă a unor dosare, chiar dacă, potrivit nomenclatorului arhivistic, acestea au termene de păstrare temporară.

- **Folosirea documentelor arhivate**

Documentele arhivate în cadrul organizației pot fi folosite în următoarele situații: cercetare științifică, rezolvarea unor lucrări administrative, informări și eliberarea de copii, extrase și certificate. De asemenea, documentele pot fi consultate, la cerere, de către cetățeni români și străini, după 30 de ani de la crearea lor. Pentru documentele la care nu s-a împlinit acest termen, cercetarea se poate face numai cu aprobarea conducerii organizației creatoare sau deținătoare.

Documentele a căror cercetare poate afecta interesele naționale, drepturile și libertățile cetățenilor, prin datele și informațiile pe care le conțin, sau cele a căror integritate fizică este în pericol nu se dau în cercetare.

Fac parte din această categorie documentele care:

- privesc siguranța, integritatea teritorială și independența statului român, potrivit prevederilor constituționale și ale legislației în vigoare;
- pot leza drepturile și libertățile individuale ale cetățeanului;
- sunt într-o stare necorespunzătoare de conservare, situație stabilită de comisia de specialitate și consemnată într-un proces-verbal;
- nu sunt prelucrate arhivistic.

Stabilirea documentelor respective se face de către deținătorul legal al acestora, în conformitate cu Lista termenelor după care pot fi date în cercetare documentele privind interesele naționale, drepturile și libertățile cetățenilor.

6. Responsabilități

- **Conducătorul organizației**

- ✓ asigură condițiile necesare cunoașterii și respectării de către angajați a reglementărilor legale privind accesul la documentele arhivate și modul de gestionare a acestora;
- ✓ numește prin decizie componența Comisiei de selecționare la nivelul organizației, precum și persoana responsabilă cu arhivarea documentelor la nivelul organizației;
- ✓ în cazul în care se solicită acest lucru, aprobă scoaterea temporară sau permanentă a documentelor din evidența arhivei, în vederea cercetării lor.

- **Șefii de compartimente**

- ✓ asigură păstrarea și depunerea la arhivă a documentelor;
- ✓ coordonează îndosarierea documentelor pe unități arhivistice la nivelul entității;
- ✓ fac propuneri pentru întocmirea, modificarea și completarea nomenclatorului arhivistic al organizației, pentru documentele create/păstrate de către compartimentul pe care-l conduc.

- **Persoana responsabilă cu arhivarea**

- ✓ preia documentele grupate în unități arhivistice de la compartimente pentru păstrarea în arhivă;
- ✓ asigură documentele deținute în arhivă în condiții corespunzătoare;
- ✓ ține evidența intrărilor-ieșirilor unităților arhivistice din arhivă;
- ✓ verifică modul de păstrare în timp a documentelor;
- ✓ ține evidența documentelor împrumutate entităților creatoare, pe baza registrului de evidență a intrărilor-ieșirilor unităților arhivistice, iar la restituirea documentelor verifică integritatea documentelor împrumutate;
- ✓ convoacă comisia de selecționare în vederea analizării dosarelor cu termenele de păstrare expirate, care sunt propuse pentru distrugere;
- ✓ asigură difuzarea nomenclatorului arhivistic tuturor compartimentelor organizatorice din cadrul organizației.

7. Dispoziții finale

Reglementările prezentei proceduri sunt obligatorii și intră în vigoare pentru toți angajații instituției (conform formularului de distribuire a procedurii) de la data aprobării, aceștia fiind obligați să le respecte începând cu data comunicării și instruirii conținutului.

Nerespectarea de către angajați a dispozițiilor prezentei proceduri constituie abatere disciplinară, iar sancțiunea se aplică în conformitate cu prevederile din Regulamentul Intern aplicabil.

8. Formular de analiză procedură

Nr .crt	*Compartiment*	*Conducător compartiment*	*Aviz favorabil*		*Aviz nefavorabil*		
			Semnătura	*Data*	*Observații*	*Semnătura*	*Data*

9. FORMULAR EVIDENŢĂ MODIFICĂRI

Nr. Crt.	Ed.	Data ediției	Rev.	Data reviziei	Pag.	Descriere modificare	Semnătura conducătorului compartimentului
1	1	…….	0	-	-	Întocmită conform OSGG nr.600/2018	

10. Formular distribuire procedură

Compartiment	*Conducător compartiment Nume și*	*Data primirii*	*Semnătura*	*Data retrageri*	*Data intrării în*	*Semnătura*

	prenume			*i*	*vigoare a procedurii*	

11. Anexe

- Anexa 1 – Nomenclator arhivistic
- Anexa 2 – Inventar documente
- Anexa 3 – Proces verbal de predare-primire a documentelor
- Anexa 4 – Registru de Evidență a intrărilor și ieșirilor unităților arhivistice;
- Anexa 5 – Proces Verbal al Comisiei de selecționare;
- Anexa 6 – Registru de Depozit;
- Anexa 7 – Proces Verbal de predare-preluare unități arhivistice

ANTET **Anexa 1**

AICI SE INSEREAZĂ PROPRIUL NOMENCLATOR ARHIVISTIC APROBAT DE ARVIVELE NAȚIONALE

ANTET **ANEXA 2**

INVENTARUL PE ANUL ___
pentru documentele care se păstrează ..... ani (permanent)

Nr. crt.	Indicativul dosarului după nomenclator	Conținutul pe scurt al dosarului, registrului, etc.	Datele extreme	Numărul filelor	Obs.

Prezentul inventar format din ..... file conținute ..... dosare, registre, condici, cartoteci etc.

Dosarele de la nr. crt. ....., au fost lăsate la....., nefiind încheiate.

La preluare au lipsit dosarele de la nr. crt. .....

Astăzi, ... s-au preluat ..... dosare.

Am predat. *Am primit.*

ANTET **ANEXA 3**

PROCES-VERBAL
de predare primire a documentelor

Astăzi, ..., subsemnații ....., delegați ai compartimentului ....., și
....., arhivarul organizației ..... am procedat primul la predarea și al doilea la preluarea documentelor create în perioada ..... de către compartimentul menționat, în cantitate de ..... dosare.

Predarea - primirea s-a făcut pe baza inventarelor anexate, cuprinzând ..... pagini dactilografiate, conform dispozițiilor legale.

Am predat. *Am primit.*

ANTET **ANEXA 4**

REGISTRU DE EVIDENȚĂ
a intrărilor-ieșirilor unităților arhivistice

Intrări						Ieșiri				
Nr. Crt	Data intrării	Denumirea Compartimentului	Date extreme ale documentelor	Nr. dos. după inv.	Nr. dos. primite efectiv	Nr. dos. rămase la comp.	Data ieșirii	Unde s-au predat	Denumirea actului de predare, nr., data	Total dosare ieșite

ANTET **ANEXA 5**

..... Se aprobă (conducerea)
(denumirea creatorului)
….....
….....
(sediul)

PROCES-VERBAL Nr. ….....

Comisia de selecționare, numită prin Decizia nr. ….. din …....., selecționând în ședințele din …..... documentele din anii*) …..... avizează ca dosarele din inventarele anexate să fie înlăturate ca nefolositoare, expirându-le termenele de păstrare prevăzute în nomenclatorul organizației.

Președinte	Membri	Secretar
.....	.....	
.....		
Numele și prenumele	Numele și prenumele	Numele și prenumele
Semnătura	Semnătura	Semnătura

*) Anii extremi

ANTET **ANEXA 6**

REGISTRU DE DEPOZIT

1	2	3	4	5	6	7	8
Nr. crt.	Denumirea fondului/ compartimentului	Cota dosar	Scopul scoaterii din depozit	Numele solicitantului, funcția, compartimentul	Data scoaterii u.a., semnătura arhivarului	Data restituirii u.a. semnătura arhivarului	Obs.

ANTET **ANEXA 7**

PROCES-VERBAL

Predare - preluare din _____
(anul, luna, ziua)

Subsemnații _____ din partea _____ și _____ din partea _____ am procedat, primul la predarea și al doilea la preluarea ____ ani extremi _____ însumând _____ u.a. și _____ m.l.

Totodată s-au predat și preluat _____

În timpul verificării nu au fost găsite următoarele _____ u.a.

Prezentul proces-verbal cuprinde _____file și s-a încheiat în două exemplare.

Am predat, Am preluat,

15. ANEXA 15 -

Model atasat Excel

16. ANEXA 16 -

ANTET

ACORD

CU PRIVIRE LA PRELUCRAREA DATELOR CU CARACTER PERSONAL

Având în vedere obiectul Contractului nr...../..... încheiat între *(nume organizație)* ....., cu sediul în ....., C.I.F. ....., reprezentată legal de ....., în calitate de Operator,

și

(nume persoană împuternicită), persoană juridică română, cu sediul în .....înregistrată la Registrul Comerțului sub nr ..... C.U.I. ....., reprezentată legal de ....., în calitate de Persoană Împuternicită,

denumite în cele ce urmează în mod individual Partea și în mod colectiv Părțile.

Părțile au decis încheierea prezentului Acord în vederea completării cadrului contractual existent cu prevederile necesare conformării cu dispozițiile art. 28 din Regulamentul 679/2016 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), cu privire la acordurile dintre operatorii de date personale si persoanele împuternicite de către operatori.

1. Scopul

- ✓ Prezentul Acord are ca scop stabilirea condițiilor în care Persoana Împuternicită se obligă să efectueze, în numele Operatorului, operațiunile de procesare a datelor cu caracter personal.
- ✓ Pe toată durata desfășurării relațiilor contractuale, Părțile se obligă în mod expres să se conformeze și să respecte reglementările privind prelucrarea datelor cu caracter personal, atât cele generale prevăzute în Regulament, cât și cele speciale adoptate de autoritățile naționale sau europene.

2. Obiectul și limitele prelucrării datelor cu caracter personal

- ✓ Prin prezentul Acord, Părțile înțeleg să determine obiectul și limitele prelucrării datelor cu caracter personal de către Persoana Împuternicită în numele Operatorului.
- ✓ Astfel, Operatorul autorizează Persoana Împuternicită să proceseze datele personale după cum urmează:
  - Pentru întocmirea declarațiilor cu caracter fiscal privind impozitul pe profit (acolo unde este cazul), taxa pe valoarea adăugată,

accizele, impozitul pe salarii, contribuțiile la asigurările sociale, precum și celelalte impozite, taxe și vărsăminte la bugetul de stat, la bugetul asigurărilor sociale și la fondurile speciale:
    - nume, prenume, CNP, adresa de domiciliu, norma de lucru, evidența zile de concediu odihnă/medical, salariu, venituri realizate (bonusuri, avantaje), impozite și taxe salariale
  - Categoriile de persoane vizate sunt:
    - Angajații și colaboratorii Operatorului
    - Responsabilii legali ai operatorului
  - Natura și Scopul (scopurile) procesării este (sunt) cele de mai jos sau doar o parte din acestea:
    - elaborare calcul salarial
    - elaborare declarații fiscale și alte acte aferente calității de angajat
    - rapoarte specifice solicitate pe categorii de contribuții și costuri
  - Serviciile ce pot fi furnizate în temeiul contractului sunt cele de mai jos sau doar o parte dintre acestea:
    - Servicii de elaborare calcul salarial,
    - Servicii de reprezentare în fața autorităților
    - Servicii de depunere declarații fiscale în numele Operatorului
    - Servicii legate de legislația privind fiscalitatea
  - Destinatarii datelor personale prelucrate sunt:
    - Operatorul
    - Autoritățile statului conform prevederilor legale
    - Subiecții cărora le sunt prelucrate datele
    - Alte entități care pot avea acces la date în baza unei obligații legale

- ✓ Pentru a efectua serviciul contractat și descris în Contract și în prezentul Acord, Operatorul furnizează Persoanei Împuternicite următoarele informații necesare:
  - acte financiar-contabile ale operatorului
  - acte medicale cu privire la capacitatea de muncă (concedii medicale, certificate de handicap, etc)
  - pontajul
  - declarații pe proprie răspundere ale angajaților operatorului cu privire la persoane aflate în întreținere
  - decizii ale autorităților legale
  - venituri și rețineri, conform procedurilor interne

3. Durata

Prezentul Acord intră în vigoare la data semnării sale și este valabil pe toată perioada de derulare a relațiilor contractuale între Părți, conform contractului principal semnat între acestea.

4. Obligațiile Persoanei Împuternicite

În temeiul prezentului Acord, Persoana Împuternicită se obligă:

- ✓ să prelucreze datele personale numai în scopul ce constituie obiectul contractului și al prezentului Acord.

Este exceptată situația existenței unor dispoziții legale care instituie obligația prelucrării și a altor date cu caracter personal de către Persoana Împuternicită, caz în care aceasta este obligată să notifice Operatorul cu privire la existența acestei obligații legale anterior efectuării oricărei activități de procesare.

- ✓ să proceseze datele în conformitate cu instrucțiunile transmise de Operator.

În cazul în care Persoana Împuternicită consideră că o instrucțiune încalcă prevederile Regulamentului general privind protecția datelor sau orice alte dispoziții legale cu privire la protecția datelor, aceasta notifică imediat Operatorul cu privire la această situație.

În cazul în care Persoana Împuternicită este obligată să transfere date cu caracter personal într-o țară terță sau unei organizații internaționale, în temeiul dreptului Uniunii Europene sau al legislației statului membru căruia i se aplică prelucrarea, Persoana Împuternicită notifică Operatorul cu privire la această obligație legală anterior prelucrării.

- ✓ să garanteze confidențialitatea datelor cu caracter personal prelucrate.
- ✓ să se asigure că persoanele autorizate să prelucreze datele cu caracter personal fie s-au obligat în mod expres, fie au o obligație legală să păstreze confidențialitatea.

Persoana Împuternicită se obligă să asigure accesul exclusiv persoanelor care au obligația să prelucreze datele personale în scopul contractului și cu respectarea dispozițiilor legale.

- ✓ să se asigure că persoanele autorizate să proceseze datele cu caracter personal au primit o instruire adecvată privind protecția acestor date.
- ✓ să ia în considerare, în ceea ce privește instrumentele, produsele, aplicațiile sau serviciile sale, principiile protecției datelor încă din faza de proiect, precum și aplicarea lor implicit.
- ✓ Subcontractare
    - Persoana Împuternicită nu poate angaja o altă persoană împuternicită ("subîmputernicit") pentru a desfășura activități specifice de prelucrare
- ✓ Dreptul la informare al persoanelor vizate de prelucrare

La momentul colectării datelor, este responsabilitatea Operatorului de a aduce la cunoștința persoanelor vizate de operațiunile de prelucrare dreptul acestora de informare.

- ✓ Exercitarea drepturilor persoanelor vizate
    - Având în vedere natura prelucrării, Persoana Împuternicită va asista Operatorul în implementarea de măsuri tehnice și organizaționale eficiente și rezonabile pentru a asigura o protecție adecvată drepturilor subiecților, conform legislației privind protecția datelor personale, sub rezerva recuperării costurilor acestor operațiuni.
    - Persoana Împuternicită îi acordă asistență Operatorului, în măsura în care acest lucru este posibil, pentru îndeplinirea obligației Operatorului de a răspunde cererilor relative la exercitarea drepturilor persoanelor vizate: dreptul de acces, rectificare,

ștergere și obiecție la prelucrare, dreptul la restricționarea procesării, dreptul la portabilitatea datelor, dreptul de a nu fi supus unei decizii individuale automate (inclusiv profilarea).
    - Persoana Împuternicită va notifica de îndată Operatorul dacă el însuși va primi orice solicitare în temeiul unei dispoziții legale în materia prelucrării datelor cu caracter personal de la orice subiect vizat de prelucrarea datelor sale personale controlate de Operator.
    - În toate cazurile de mai sus în care persoanele vizate transmit solicitări pentru a-și exercita drepturile conferite de Regulament, Persoana Împuternicită trebuie să înainteze aceste cereri de îndată ce sunt primite prin e-mail către [……..] (a se indica o persoană de contact din cadrul Operatorului).
- ✓ Notificarea încălcării securității datelor cu caracter personal
    - Persoana Împuternicită notifică Operatorul cu privire la orice încălcare a datelor cu caracter personal în cel mult 48 ore după ce a luat cunoștință de acesta, prin email și/sau fax.
    - Notificarea respectivă trebuie transmisă împreună cu toate documentele necesare pentru a permite Operatorului, dacă este cazul, să notifice această încălcare autorității de supraveghere competente, precum și, după caz, persoanelor vizate.
    - Ulterior notificării Operatorului și în cazul în care încălcarea este obligatoriu să fie notificată, la solicitarea expresă și în numele Operatorului, Persoana Împuternicită notifică fără întârziere autoritatea de supraveghere competentă, despre încălcările cu privire la datele cu caracter personal, dar nu mai târziu de 72 de ore de la momentul luării la cunoștință.
    - Notificarea trebuie să conțină cel puțin următoarele informații:
        - să descrie natura încălcării datelor cu caracter personal, inclusiv, dacă este posibil, categoriile și numărul aproximativ al persoanelor vizate în cauză, precum și categoriile și numărul aproximativ de înregistrări de date cu caracter personal în cauză;
        - să comunice numele și datele de contact ale responsabilului cu protecția datelor sau ale altei persoane de contact de la care pot fi obținute mai multe informații;
        - să descrie consecințele probabile ale încălcării securității datelor cu caracter personal;
        - să descrie măsurile luate sau propuse spre a fi luate de către Operator pentru a remedia încălcarea datelor cu caracter personal,
        - să descrie măsurile de atenuare a eventualelor prejudicii/ efecte negative.
    - În măsura în care în mod obiectiv și justificat nu este posibilă furnizarea informațiilor în termenul de 72 de ore, informațiile pot fi furnizate și în etape, pe măsură ce detaliile privind încălcarea cu privire la datele personale devin disponibile.
    - În cazul în care încălcarea prezintă un risc ridicat pentru drepturile și libertățile persoanei vizate de prelucrare, la solicitarea si în numele Operatorului, Persoana Împuternicită comunică fără

întârziere încălcarea datelor cu caracter personal respectivei persoane vizate.
    - Notificarea trebuie să descrie într-un limbaj clar și simplu natura încălcării și, în măsura în care este posibil, să includă detalii cu privire la încălcarea datelor cu caracter personal, respectiv:
        - categoriile și numărul aproximativ al persoanelor vizate de încălcare;
        - categoriile și numărul aproximativ de înregistrări de date cu caracter personal în cauză;
        - numele și datele de contact ale responsabilului cu protecția datelor sau ale altei persoane de contact de la care pot fi obținute mai multe informații;
        - consecințele probabile ale încălcării securității datelor cu caracter personal;
        - măsurile luate sau propuse spre a fi luate de către operator pentru a remedia încălcarea datelor cu caracter personal,
        - măsuri de atenuare a posibilelor efecte negative/ eventualelor prejudicii.
- ✓ Asistența acordată de către Persoana Împuternicită Operatorului privind respectarea obligațiilor sale
    - Persoana Împuternicită sprijină Operatorul în efectuarea de evaluări de impact privind protecția datelor, în temeiul art. 35 sau art. 36 din Regulamentul general privind protecția datelor.
    - Persoana Împuternicită asistă Operatorul în ceea ce privește consultarea prealabilă a autorității de supraveghere.
- ✓ Măsuri de securitate
    - Luând în considerare stadiul actual al tehnicii, costurile implementării și natura, contextul și scopurile prelucrării, precum și riscul variabilității și gravității diferitelor drepturi și libertăți ale persoanelor fizice, Persoana Împuternicită va prelucra datele personale ale Operatorului și va pune în aplicare măsuri tehnice și organizatorice adecvate pentru a asigura un nivel de securitate corespunzător acestui risc, inclusiv, după caz, măsurile menționate de art. 32 alin. (1) din R.G.P.D.
    - La evaluarea nivelului adecvat de securitate, Persoana Împuternicită trebuie să ia în considerare riscurile prezentate de activitatea de prelucrare, în special în cazul unei breșe în siguranța datelor cu caracter personal.
    - Pentru a asigura un nivel de securitate adecvat, Persoana Împuternicită se obligă să pună în aplicare măsuri stricte de securitate, cum ar fi, dar fără a se limita la:
        - capacitatea de a asigura confidențialitatea, integritatea, disponibilitatea și reziliența în curs a sistemelor și activităților de prelucrare;
        - capacitatea de a restabili în timp util disponibilitatea și accesul la date cu caracter personal în cazul unui incident fizic sau tehnic;

- un proces de testare și evaluare periodică a eficienței măsurilor tehnice și organizatorice pentru asigurarea securității prelucrării.

✓ Durata prelucrării datelor personale

- În termen de 30 de zile de la data încetării contractului având ca obiect prelucrarea datelor personale ale Operatorului, Persoana Împuternicită are obligația de a șterge toate copiile conținând date personale prelucrate în temeiul contractului cu Operatorul.
- În același termen, Operatorul este îndreptățit să solicite în scris Persoanei Împuternicite:
  - să îi returneze prin transfer de fișiere securizat, într-un format rezonabil, o situație completă a tuturor datelor personale prelucrate;
  - să șteargă datele personale prelucrate de către Persoana Împuternicită.

  Persoana Împuternicită este obligată să se conformeze acestor obligații în termen de 30 de zile de la data încetării contractului.
- Persoana Împuternicită trebuie să se asigure că aceste date cu caracter personal ale Operatorului sunt prelucrate numai în scopul specificat în legile aplicabile care necesită depozitarea lor și nu pentru alt scop.
- Persoana Împuternicită va furniza Operatorului o confirmare scrisă a faptului că a șters datele personale ale Operatorului sau după caz a păstrat spre depozitare date conform prevederilor legale, în termen de 45 de zile de la data încetării contractului.

✓ Responsabilul cu protecția datelor

Persoana Împuternicită comunică Operatorului numele și datele de contact ale responsabilului său cu protecția datelor, dacă a desemnat unul în conformitate cu art. 37 din Regulamentul general privind protecția datelor.

✓ Registrele de evidență a categoriilor de activități de prelucrare

Persoana Împuternicită se obligă să păstreze o evidență scrisă a tuturor categoriilor de activități de prelucrare efectuate în numele Operatorului, care va conține:

- numele și datele de contact ale Operatorului în numele căruia Persoana Împuternicită acționează, al oricărui alt subîmputernicit și, după caz, al responsabilului cu protecția datelor cu caracter personal;
- categoriile de prelucrări de date efectuate în numele Operatorului;
- transferurile de date cu caracter personal către o țară terță sau o organizație internațională, inclusiv identificarea respectivei țări terțe sau a organizației internaționale și, în cazul transferurilor menționate la art. 49 alin. (1) par. 2 din R.G.P.D., documentarea garanțiilor adecvate;
- dacă este posibil, o descriere generală a măsurilor de securitate tehnice și organizatorice, incluzând, printre altele:

✓ Auditare

- Persoana Împuternicită pune la dispoziția Operatorului, la cerere, toate informațiile necesare pentru a demonstra conformitatea cu obligațiile stabilite prin prezentul Acord, permite și contribuie la servicii de audit. inclusiv inspecții ale Operatorului sau a unui auditor mandatat de Operator cu privire la prelucrarea datelor personale de către subîmputerniciți contractați.
- Drepturile la informare și de audit ale Operatorului pot fi exercitate fie în temei contractual, fie în temei legal (art. 28 alin. (3) lit. h) din Regulamentul general privind protecția datelor).
- Operatorul poate mandata un auditor.
- Operatorul trebuie să notifice Persoana Împuternicită cu privire la orice audit sau inspecție ce urmează a fi efectuată, depunând eforturi rezonabile atât Operatorul, cât și auditorii mandatați pentru a evita sau, după caz, a reduce la minimum orice fel de daune sau întreruperi de activitate în locațiile sau asupra echipamentelor. personalului și afacerilor subîmputerniciților contractați.
- Persoana împuternicită contractată trebuie să acorde acces la spațiile sale în scopul unui astfel de audit sau inspecție dacă:
  - persoana furnizează dovezi rezonabile privind identitatea și autoritatea, fiind notificat în prealabil în acest sens;
  - în afara programului de muncă, atunci când auditul sau inspecția trebuie efectuate în regim de urgență, Operatorul sau auditorul notificând Persoana Împuternicită.
- Inspecțiile sau serviciile de audit urmează a fi efectuate atunci când:
  - Operatorul consideră în mod rezonabil că acestea sunt necesare, din cauza unor preocupări reale legate de respectarea prevederilor prezentului Acord de către Persoana Împuternicită;
  - autoritatea de supraveghere sau orice altă autoritate solicită Operatorului efectuarea acestora, în scopul respectării legislației cu privire la protecția datelor cu caracter personal în orice țară sau teritoriu.

✓ Transferuri de date

Persoana Împuternicită nu va efectua transferuri de date personale în afara Spațiului Economic European care pot intra sub incidența prevederilor transferurilor interzise si care nu se încadrează printre derogările prevăzute de Regulament. Orice transfer va fi notificat Operatorului, cu precizarea tuturor condițiilor necesare transferului in condiții de securitate a prelucrării datelor, conform prevederilor Regulamentului.

5. Obligațiile Operatorului

Operatorul se obligă:

- să furnizeze Persoanei Împuternicite datele menționate mai jos;
- să furnizeze în scris, orice instrucțiune privind prelucrarea datelor de către persoana împuternicită;

- să asigure, înainte și de-a lungul procesului de prelucrare, respectarea obligațiilor stabilite prin R.G.P.D. de către Operator;
- să supravegheze prelucrarea, inclusiv prin efectuarea de servicii de audit și inspecții la locațiile Persoanei Împuternicite

Operator

Persoană împuternicită

NUME ORGANIZAȚIE

MĂSURI DE SECURITATE APLICABILE PERSOANELOR ÎMPUTERNICITE

Persoana Împuternicită va implementa următoarele măsuri de securitate:

1. **Măsuri organizatorice**

Persoana împuternicită garantează că:

- ✓ accesul la date va fi atribuit pe baza principiului "necesității de a cunoaște";
- ✓ va limita numărul de persoane autorizate care desfășoară activități legate de prelucrarea datelor;
- ✓ a implementat și menține actualizate toate procedurile și politicile aplicabile protecției datelor în general și a celor cu caracter personal în mod special;
- ✓ va bugeta și apela la consultanță de specialitate atunci când nu deține expertiză suficientă în materie de securitate a datelor;
- ✓ va instrui persoanele autorizate cu privire la reglementările privind protecția datelor, măsurile de securitate luate de persoana împuternicita și politicile de securitate implementate cu atenție specială pentru cele aplicabile în situații de urgență în materie de securitate;
- ✓ persoanele autorizate utilizează un sistem de prelucrare a datelor și au acces numai la datele la care au drept de acces; datele nu pot fi citite, copiate, modificate, eliminate sau utilizate fără autorizație în timpul procesării și ulterior în timpul stocării;
- ✓ va păstra o listă actualizată de persoane autorizate să aibă acces la date și va prezenta o astfel de lista la dispoziția Operatorului la cererea motivată a acestuia;
- ✓ va furniza o copie de rezervă actualizată a datelor prelucrate de persoana împuternicită la cererea scrisă a acestuia;
- ✓ se va asigura că angajații săi au semnat un acord corespunzător de confidențialitate atât cu privire la datele proprii ale Persoanei Împuternicite cât și la cele aparținând clienților acestuia;
- ✓ se va asigura că administratorii sistemelor IT au o experiență adecvată și că acționează întotdeauna în mod responsabil și profesionist în activităților lor cu atenție specială pentru confidențialitatea datelor;

2. **Măsuri de securitate fizică**

Persoana împuternicită:

- ✓ va folosi spații adecvate care găzduiesc infrastructura IT utilizată pentru procesarea și transferul datelor;
- ✓ va limita numărul de persoane autorizate să acceseze datele strict la lista celor care au nevoie să facă acest lucru în baza prevederii contractului cu Operatorul și strict la setul de date necesar;
- ✓ va limita accesul persoanelor strict la cele autorizate să aibă acces la infrastructura IT utilizată pentru procesarea și transferul datelor;
- ✓ să se asigure că spațiile care găzduiesc infrastructura IT sunt protejate corespunzător de acțiunea unor factori fizici distructivi care pot afecta aceste sisteme informatice: protecție adecvată la incendiu, protecție la inundații;
- ✓ va asigura condiții ambientale corespunzătoare cu privire la temperatură, umiditate și procentul de particule de praf existente în compoziția aerului;
- ✓ asigură furnizarea continuă de energie a infrastructurii IT utilizate pentru procesarea datelor, în special prin furnizarea de sisteme de energie de urgență de tip UPS;
- ✓ va păstra toate documentele în forma fizică care pot conține date personale ale Operatorului în dulapuri sub cheie și se va asigura că pe perioada consultării lor acestea nu rămân nesupravegheate;

3. Măsuri de securitate informatică

Persoana Împuternicită va garanta:

- ✓ va implementa un plan adecvat de măsuri tehnice adecvate și monitorizate periodic care să protejeze datele de indisponibilitate, distrugere, alterare, pierdere accidentală;
- ✓ va depune eforturi să eticheteze și să proceseze în mod corespunzător datele în conformitate cu gradul lor de confidențialitate;
- ✓ va asigura accesul la date doar în baza unor conturi de utilizator care sunt atribuite unic fiecărei persoane autorizate;
- ✓ conturile de utilizator trebuie să respecte următoarele condiții:
    - o vor fi menținute active doar atât timp cât sunt folosite de persoana pentru care au fost create;
    - o vor fi dezactivate imediat ce s-a decis că persoana pentru care au fost create nu trebuie să mai aibă acces la sistemele informatice;
    - o folosirea lor trebuie monitorizată și datele de audit stocate pentru perioade rezonabile de timp;
    - o conturile nefolosite pentru o perioadă mai mare de 6 luni vor fi dezactivate;
    - o parolele de acces trebuie cunoscute doar de către utilizatorii respectivi; acordarea accesului la anumite date făcându-se prin mecanisme de autorizare acceptabile și nu prin dezvăluirea datelor de acces;
    - o parolele de acces trebuie sa fie suficient de complexe (minim 8 caractere conținând litere, cifre și caractere speciale) și schimbate la intervale adecvate de timp dar nu mai mari de 3 luni;

- utilizatorii își pot schimba singuri parolele în sistemele informatice folosite;

- ✓ se va asigura că implementează măsuri tehnice automate care să asigure utilizatorilor drepturi minime pe sistemele informatice dar suficiente pentru a-și putea îndeplini sarcinile;
- ✓ va impune măsuri tehnice care să limiteze accesul neautorizat la date prin protejarea terminalelor de acces între sesiunile de lucru (terminalele pornite vor fi blocate în absența utilizatorilor autorizați);
- ✓ să implementeze un sistem de autorizare care să:
  - permită crearea de profiluri de acces bazate pe rolurile existente în organizație;
  - permită în mod excepțional acordarea de drepturi ad-hoc;
- ✓ sa implementeze soluții efective de securitate acceptate, cunoscute și cu o reputație acceptabilă în piață care să protejeze datele de aplicații de tip malware, virus, de acces neautorizat de la distanță. Acestea respectă următoarele condiții :
  - aplicațiile de tip antimalware și antivirus trebuie actualizate cel puțin zilnic;
  - patchurile de securitate pentru sistemele de operare și aplicațiile informatice sunt aplicate în cel mai scurt timp de la publicarea de către producător;
  - orice fel de patchuri de securitate sau schimbare de aplicații informatice pe sistemele care procesează datele Operatorului vor fi testate în prealabil pentru a afecta cât mai puțin disponibilitatea datelor;
  - toate măsurile de securitate vor fi periodic inspectate pentru a se confirma buna lor funcționare și eficiența protecției pe care o oferă;
- ✓ se vor implementa măsuri de securitate la nivel de infrastructura IT pentru toate sistemele care pot comunica cu sistemele ce procesează datele : echipamente wi-fi, echipamente IoT, echipamente de comunicații active – switchuri, routere etc; se vor dezactiva protocoalele de administrare nesecurizate și se vor verifica și actualiza în mod periodic firmware-ul;
- ✓ va efectua copii de siguranță a datelor cel puțin zilnic; salvările se păstrează pentru o perioada de minim un an; copiile de siguranță vor fi criptate și stocate în spații securizate;
- ✓ va lua măsuri rezonabile care să asigure restaurarea datelor în caz de incident informatic în cel mai scurt timp posibil astfel încât aceste incidente să nu afecteze disponibilitatea și integritatea datelor;
- ✓ datele utilizate pentru autentificare trebuie să fie protejate prin măsuri de securitate criptografice eficiente;
- ✓ se va asigura că accesul la date este în permanență monitorizat și că poate verifica cine, când și ce a modificat, șters sau autorizat la o perioada de timp rezonabilă după ce acest fapt s-a realizat; log-urile trebuie salvate pentru o perioadă de un an;
- ✓ accesul administrativ pe toate echipamentele IT se va stoca pentru o perioadă de 1 an, pe cât posibil într-un sistem centralizat de management al log-urilor;

- ✓ datele vor fi șterse ireversibil în cazul înlocuirii hardware sau reutilizării hardware;
- ✓ în cazul în care se constată o încălcare a datelor sau o vulnerabilitate de securitate în procesul de prelucrare a datelor sau în orice sistem utilizat pentru furnizarea serviciilor, compania este informată imediat despre incident și despre toate măsurile corective implementate.

17. ANEXA 17 -

ANTET

CHESTIONAR
PRIVIND CONFORMITATEA IN MATERIE DE PROTECTIE A DATELOR

I. SCOP

Acest document (“Chestionar”) **are drept scop evaluarea**, de către XXXX, a **nivelului de conformitate al organizației dumneavoastră în ceea ce privește responsabilitățile privind protecția și confidențialitatea datelor sau, după caz, capacitatea organizației dumneavoastră de a asista** XXXX **în conformarea cu propriile obligații în materie de protecție și confidențialitate a datelor**.

Dacă o întrebare nu vă este aplicabilă, vă rugăm să completați cu "N/A" căsuța corespunzătoare întrebării respective.

Răspunsurile dumneavoastră și informațiile solicitate sunt necesare pentru a ne convinge asupra nivelului conformității organizației dumneavoastră cu normele de protecție a datelor, precum și asupra măsurilor care trebuie implementate pentru a atinge un nivel satisfăcător de conformitatea cu cerințele GDPR.

Vă atenționăm asupra seriozității de completare a chestionarului și **vă informăm că forma completată și semnată reprezintă Declarația pe proprie răspundere cu privire la îndeplinirea de către organizația dumneavoastră a conformității cu prevederile GDPR** și se constituie Anexă la Contractul nr. ..... din .....

II. DEFINIȚII

„GDPR" înseamnă Regulamentul (UE) 2016/679 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date ("Regulamentul General de Protecție a Datelor")

„Date cu Caracter Personal" înseamnă orice informații referitoare la o persoană fizică identificată sau identificabilă („persoană vizată"); o persoană fizică identificabilă este acea persoană care poate fi identificată, direct sau indirect, în special prin referire la un număr de identificare, cum ar fi un nume, număr de identificare, date de localizare, un identificator online, sau la unul sau la mai multe elemente specifice, proprii identității sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale;

„(a) Prelucra" "Prelucrare" sau "Prelucrat" 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;

„Persoana vizată" persoana fizică ale cărei date personale sunt prelucrate și stocate în bazele de date/ sistemele de evidență manuale/automate.

III. ÎNTREBĂRI

Vă rugăm să ne oferiți următoarele informații pentru a sprijini XXXX în evaluarea nivelului potențial de risc pe care îl implică Prelucrarea (actuală sau viitoare) a Datelor cu Caracter Personal:

Vă rugăm să menționați fiecare scop pentru care Datele cu Caracter Personal vor fi prelucrate	**Vă rugăm să enumerați toate categoriile de Date cu Caracter Personal ce urmează să fie prelucrate**	**Vă rugăm să furnizați o estimare, pe categorii, a volumului de Date cu Caracter Personal ce urmează să fie prelucrate**

CERINȚE DE CONFIDENȚIALITATE ȘI DE PROTECȚIE A DATELOR CU CARACTER PERSONAL	**DA/NU**	**Comentarii/informații solicitate**
Informații generale privind prelucrarea si entitățile implicate		
Angajații dumneavoastră au acces la Datele cu Caracter Personal ale XXXX? *Dacă da, vă rugăm să indicați pe scurt în coloana "Comentarii" numărul angajaților implicați în Prelucrarea Datelor cu Caracter Personal ale XXXX și atribuțiile lor în ceea ce privește respectiva Prelucrare.*		
Organizația dumneavoastră are o Politică de Prelucrare a Datelor?		
Folosiți subcontractori pentru a prelucra Datele cu Caracter Personal ale XXXX? *Dacă da, vă rugăm să indicați, într-o scurtă listă, astfel de subcontractori folosiți în prezent.*		
Dacă răspunsul este afirmativ, există prevederi contractuale ce guvernează prelucrarea Datelor cu Caracter Personal ale XXXX de către subcontractorii folosiți în prezent?		
A fost XXXX consultat, î**n trecut**, în ceea ce privește subcontractorii care au acces la Datele Personale ale XXXX?		
POLITICA ȘI GUVERNANȚA		
Ați numit un reprezentant în materie de protecție a datelor sau un responsabil de protecție a datelor? *Vă rugăm să menționați datele sale de contact*		
Ați stabilit și implementat politici și proceduri pentru guvernanța Datelor cu Caracter Personal? Aceste politici și proceduri includ instrumente de securitate care au fost implementate pentru		

protecția Datelor cu Caracter Personal?		
Când au loc modificări ale acestei politici de protecție a datelor, sunt ele comunicate angajaților dumneavoastră?		
Este reglementată în politicile și procedurile dumneavoastră modalitatea de alocare a rolurilor și responsabilităților în ceea ce privește protecția datelor și confidențialitatea?		
În politicile și procedurile dumneavoastră privind guvernanța Datelor cu Caracter Personal sunt stabilite sancțiuni disciplinare în cazul încălcării acestor politici & proceduri, inclusiv escaladarea ierarhică în interiorul organizației dumneavoastră?		
Sunt politicile și procedurile dumneavoastră de protecție / confidențialitate a datelor comunicate angajaților dumneavoastră în mod constant, de ex. cel puțin anual?		
Păstrați dovezi (trasabilitatea) acestor comunicări?		
Ați implementat politici și proceduri conform cărora faceți eforturi rezonabile în scopul prelucrării în mod valid și a actualizării Datelor cu Caracter Personal ale XXXX?		
PRELUCRAREA DATELOR CU CARACTER PERSONAL		
Ați prevăzut vreo procedură pentru a evalua dacă o solicitare sau instrucțiune din partea XXXX privind prelucrarea Datelor cu Caracter Personal ale XXXX este legitimă?		
Dacă apreciați drept nelegitimă o instrucțiune primită din partea XXXX privind prelucrarea Datelor cu Caracter Personal, cum veți acționa în legătură cu aceasta?		
Ați implementat vreun proces pentru a vă asigura că orice modificări ale modului în		

care sunt prelucrate Datele cu Caracter Personal ale XXXX sunt comunicate către XXXX și este obținută aprobarea prealabilă a acesteia, dacă este cazul?		
Ați fi pregătiți (ați avea resursele necesare) pentru a asista XXXX în procedura de efectuare a unei evaluări a impactului asupra protecției datelor, în cazul în care XXXX a stabilit că prelucrarea Datelor cu Caracter Personal prezintă un risc ridicat, conform GDPR?		
Veți permite XXXX să realizeze audituri pentru a verifica conformitatea dumneavoastră cu cerințele GDPR, inclusiv politicile și procesele de protecție și confidențialitate a datelor, sistemele folosite pentru a prelucra Datele cu Caracter Personal ale XXXX și locațiile în care Datele cu Caracter Personal ale XXXX sunt prelucrate?		
Aveți stabilit un proces pentru documentarea prelucrărilor de date cu caracter personal pe care le realizați în numele XXXX?		
Ați definit procese pentru ștergerea Datelor cu Caracter Personal ale XXXX în conformitate cu politicile și regulile de păstrare a acestora, în cazul în care acestea sunt comunicate de către XXXX?		
În absența oricărei reguli transmise de XXXX pentru păstrarea datelor, aveți politici standard de păstrare sau reguli de ștergere pentru prelucrările pe care le veți face sau pe care le faceți în prezent pentru XXXX?		
Ați definit procese pentru a vă asigura că, odată ce relația contractuală cu XXXX se va fi terminat, toate Datele cu Caracter Personal ale XXXX vor fi (a) fie extrase din toate sistemele și înregistrările dumneavoastră și restituite XXXX, (b) fie purjate/ șterse din toate sistemele și înregistrările dumneavoastră?		
CONȘTIENTIZAREA PROTECȚIEI ȘI CONFIDENȚIALITĂȚII DATELOR ȘI FORMĂRI PENTRU		

PERSONAL		
Semnați acorduri de confidențialitate cu angajații dumneavoastră prin care aceștia se angajează să respecte confidențialitatea sau au o obligație statutară de păstrare a confidențialității?		
Contractele semnate de angajații dumneavoastră prevăd că responsabilitățile privind Protecția Datelor cu Caracter Personal se extind și în afara orelor de muncă normale, cât și ulterior încetării contractului de muncă?		
Contractele semnate de angajații dumneavoastră prevăd măsuri disciplinare pentru încălcarea responsabilităților în ceea ce privește Datele cu Caracter Personal?		
Ați comunicat (printr-un mijloc potrivit) angajaților dumneavoastră ce sunt implicați în gestionarea sistemelor de prelucrare a Datelor cu Caracter Personal politicile și procedurile de protecție a datelor sau privind confidențialitatea?		
Este politica de protecție a datelor cu caracter personal comunicată și acceptată de către toți angajații noi și de angajații existenți atunci când aceștia își schimbă poziția (iar această schimbare de poziție implică preluarea de noi responsabilități în ceea ce privește prelucrarea Datelor cu Caracter Personal)?		
Ați inserat în cadrul politicii de protecție a datelor reguli specifice pentru accesarea Datelor cu Caracter Personal ale XXXX doar de către persoane desemnate/departamente/grupuri de persoane desemnate în acest sens? Cum este asigurat accesul la Datele cu Caracter Personal ale XXXX separat față de rolurile și responsabilitățile celorlalți membri ai personalului?		
Ați definit și implementat formări profesionale și ați realizat acțiuni de		

sensibilizarea ale personalului dvs. implicat în Prelucrarea Datelor cu Caracter Personal ale XXXX cu privire la protecția și confidențialitatea acestora?		
Sunt aceste acțiuni de formare/ sensibilizare destinate tuturor noilor veniți și personalului existent în cazul schimbării de funcție? Puteți dovedi că aceste acțiuni de formare/ sensibilizare au fost realizate?		
Acțiunile de formare și programul de sensibilizare sunt realizate în mod periodic, de ex. anual?		
DREPTURILE PERSOANELOR VIZATE		
Ați implementat un proces pentru oferirea de asistență XXXX, la solicitarea acesteia, în vederea răspunderii cererilor privind exercitarea de către persoanele vizate a drepturilor prevăzute de GDPR în legătură cu Datele cu Caracter Personal prelucrate în numele XXXX *sau* ați implementat un proces pentru gestionarea în mod direct a acestor cereri?		
Ați definit un proces pentru a sprijini XXXX în corectarea Datelor cu Caracter Personal prelucrate în cadrul unor sisteme pentru care sunteți responsabili?		
Ați implementat un proces pentru ca, la solicitarea XXXX, să răspundeți direct cererilor adresate direct dumneavoastră în legătură cu Datele cu Caracter Personal ale XXXX?		
Ați implementat vreo procedură în scopul de a colecta și gestiona cererile XXXX sau ale Persoanelor Vizate în legătură cu Datele lor cu Caracter Personal?		
Aveți implementat un proces clar care să permită XXXX să extragă Datele cu Caracter Personal ale XXXX din sisteme pentru care sunteți responsabili, astfel încât XXXX să respecte obligațiile sale în materie de portabilitate a datelor, dacă		

este cazul?		
Aveți un proces clar care să permită XXXX să blocheze accesul la Datele cu Caracter Personal ale unei anumite Persoane Vizate?		
Ați putea să blocați temporar accesul la Datele cu Caracter Personal ale unei Persoane Vizate?		
Ați putea să sprijiniți, la solicitarea XXXX, orice cerere a XXXX privind pseudonimizarea sau anonimizarea Datelor cu Caracter Personal?		
Toate categoriile de date personale pot fi pseudonimizate sau anonimizate la solicitarea XXXX?		
ÎNCĂLCĂRI ALE SECURITĂȚII ȘI PROTECȚIEI DATELOR CU CARACTER PERSONAL		
Ați implementat un program de securitate a informațiilor ce include politici și proceduri pentru a proteja și a păstra în siguranță Datele cu Caracter Personal ale XXXX conform bunelor practici din industrie și în conformitate cu prevederile legale aplicabile?		
Monitorizați împotriva intruziunilor și a altor activități neautorizate sistemele informatice în funcțiune în cadrul rețelei companiei dumneavoastră, în care Datele cu Caracter Personal sunt prelucrate?		
Ați implementat procese de planificare a backupului pentru a proteja Datele cu Caracter Personal ale XXXX împotriva utilizării, accesului, dezvăluirii, alterării sau distrugerii neautorizate?		
Faceți o evaluare anuală a securității rețelei informatice?		
Ați implementat o politică privind dispozitivele mobile care să limiteze și să protejeze suplimentar utilizarea Datelor cu Caracter Personal accesate sau utilizate pe un dispozitiv mobil?		

Ați prevăzut instrumente menite să raporteze către XXXX incidente/încălcări ale securității ce implică Datele cu Caracter Personal ale XXXX?		
Sunt procesele dumneavoastră pentru înregistrarea (trasabilitatea) și raportarea către XXXX a incidentelor/încălcărilor securității privind Datele cu Caracter Personal comunicate în interiorul organizației dumneavoastră?		
Există o persoană din cadrul organizației dumneavoastră care este răspunzătoare pentru gestionarea incidentelor și pentru raportarea acestora către XXXX?		
Procedurile dumneavoastră includ cerința ca notificarea XXXX (dacă Datele cu Caracter Personal ale XXXX sunt impactate) să fie realizată în termen de 24 de ore, astfel încât să permită XXXX să investigheze și să facă notificările relevante către autoritate/autorități în termenul de 72 de ore prevăzut de GDPR?		
Dacă vreun incident de securitate care afectează Datele cu Caracter Personal ale XXXX s-a petrecut în ultimele 12 luni, ați notificat acest lucru către XXXX?		
SUBCONTRACTARE		
Aveți un proces de verificare a antecedentelor documentat pentru selectarea subcontractorilor, care cuprinde o revizuire și confirmarea controlului administrativ, fizic și tehnic în ceea ce privește protecția datelor cu caracter personal și / sau confidențialitatea acestora?		
Vă asigurați că ați semnat acorduri/contracte scrise cu subcontractorii dumneavoastră care prevăd în sarcina acestora aceleași obligații sau obligații echivalente în legătură cu prelucrarea Datelor cu Caracter Personal ale XXXX ca și cele pe care dumneavoastră le-ați asumat		

contractual în relație cu XXXX ?		
În cazul unui răspuns afirmativ, aceste acorduri stabilesc obligația subcontractorilor de a prelucra Datele cu Caracter Personal ale XXXX doar în legătură cu scopul convenit (de XXXX)?		
În cazul unui răspuns afirmativ, aceste acorduri stabilesc obligația subcontractorului de a distruge/restitui către dumneavoastră toate Datele cu Caracter Personal ale XXXX după terminarea contractului semnat cu subcontractorul?		
Monitorizați în mod constant conformitatea subcontractorului cu sarcinile sale în materie de protecție a datelor?		
Aveți un proces pentru notificarea XXXX sau, acolo unde este cazul, pentru a solicita aprobarea XXXX atunci când apare o modificare a subcontractorilor folosiți pentru a prelucra Datele cu Caracter Personal ale XXXX?		
Ați implementat o politică sau procedură pentru a notifica XXXX despre desemnarea unui nou subcontractor și, dacă este cazul, pentru a gestiona obiecțiile XXXX față de această desemnare?		
Ați implementat o procedură pentru a notifica XXXX în termen de 24 de ore în legătură cu orice încălcare produsă de sau în legătură cu un subcontractor?		
POLITICA DE PĂSTRARE (RETENȚIE A DATELOR)		
Vă asigurați că Datele cu Caracter Personal ale XXXX sunt păstrate doar pe durata necesară prestării serviciilor solicitate de XXXX, singura excepție în care Datele cu Caracter Personal ale XXXX sunt păstrate ulterior acestei date fiind o cerință prevăzută de lege?		
Puteți/veți putea să ștergeți/ distrugeți complet Datele cu Caracter Personal ale		

XXXX la solicitarea XXXX?		
Veți putea să oferiți un certificat scris care să confirme completa ștergere/distrugere a Datelor cu Caracter Personal ale XXXX?		
LOCUL PRELUCRĂRII DATELOR CU CARACTER PERSONAL		
Veți prelucra Date cu Caracter Personal în: ☐ Spațiul Economic European (SEE) ☐ În afara SEE ☐ Ambele		
Va prelucra vreunul dintre subcontractorii dumneavoastră Date cu Caracter Personal ale XXXX în: ☐ Spațiul Economic European (SEE) ☐ Exteriorul SEE ☐ Amândouă *Vă rugăm să indicați explicit în rubrica "Comentarii" dacă vreunul dintre subcontractorii dumneavoastră este stabilit în afara SEE și să ne oferiți o listă a subcontractorilor aflați în această situație, prin menționarea inclusiv a statului în care aceștia sunt stabiliți.*		
Veți prelucra Date cu Caracter Personal ale XXXX: ☐ În centrele proprii situate în interiorul SEE? ☐ În unul din centrele proprii situate în afara SEE? ☐ Într-un centru de date al unui terț, situat în SEE? ☐ Într-un centru de date al unui terț, situat în afara SEE? ☐ Într-un serviciu de cloud public?		

Vă asigurați că standardele și procedurile aplicabile în locațiile/jurisdicțiile în care dumneavoastră și subcontractorii dumneavoastră vă derulați activitatea sunt potrivite și, în orice caz, sunt cel puțin echivalente standardelor și procedurilor pe care le-ați convenit cu XXXX?		
Transferați Date cu Caracter Personal ale XXXX către o țară din afara SEE?		
Vreunul dintre subcontractorii dumneavoastră transferă Date cu Caracter Personal ale XXXX în afara SEE?		
Dacă transferați Date cu Caracter Personal ale XXXX într-o locație: • Ce este situată ÎN AFARA SEE; sau • Ce nu este una dintre "Țările Recunoscute ca fiind Sigure" (nivel adecvat de protecție), astfel cum sunt acestea stabilite de Comisia Europeană, veți semna cu XXXX un acord de transfer de date bazat pe Clauzele Model ale UE (clauze contractuale standard) pentru transferul de date de la exportatori la importatori ?		
DEZVALUIREA CATRE TERTE PARTI		
Aveți o politică (proces documentat) privind evaluarea legalității cererilor de dezvăluire a Datelor cu Caracter Personal către terți, inclusiv către instanțele judecătorești și alte organe judiciare?		
Personalul dumneavoastră însărcinat cu primirea unor asemenea solicitări cunoaște respectiva politică / respectivul proces?		
Respectiva politică / respectivul proces impune ca toate cererile și analizele să fie înregistrate (trasabilitate, log-uri)?		
Politica/procesul dumneavoastră impune efectuarea unei evaluări a cererii primite din partea terților, în sensul verificării temeiniciei respectivelor cereri, spre a vă		

asigura că dezvăluiți asemenea Date cu Caracter Personal către terți care sunt îndreptățiți în mod legal să aibă acces la Datele Personale?		
Politica/procesul dumneavoastră impune efectuarea unei analize asupra dreptului / legitimității notificării XXXX în legătură cu asemenea cereri ale terților ce presupun accesul la sau dezvăluirea Datelor cu Caracter Personal ale XXXX?		
Ați reglementat o procedură pentru a solicita acordul XXXX (dacă nu există o obligație legală de a dezvălui respectivele date) în cazul unei cereri de acces/ dezvăluire a Datelor cu Caracter Personal ale XXXX?		

Vă rugăm să menționați:
- numele și funcția persoanei care a completat Chestionarul de mai sus;

- adresa de email a persoanei

- numele și datele de contact ale persoanei responsabile cu protecția datelor

Vă rugăm să menționați data completării Chestionarului:

Vă rugăm să semnați acest Chestionar: