

PLATFORMA NET-DD

NORME INTERNE DE IMPLEMENTARE A REGULAMENTULUI GENERAL PENTRU PROTECTIA DATELOR¹ (GDPR)

**APLICABIL PENTRU TOȚI OPERATORII PLATFORMEI NET-DD
ȘI A SERVICIILOR NET-DD INTEGRATE PE ACEASTA:**

- **NET-DD PLATFORM CORE**
 - ACCESS
 - NET
 - CARD
- **NET-DD ORG**
- **NET-DD PROFESSIONAL**
 - NET-DD SPORT
- **NET-DD SCIENCE**
 - NET-DD PUBLISH
 - NET-DD TRAINING
 - NET-DD LEARNING
- **NET-DD PROJECT**
- **NET-DD MEDICAL**

¹ VERSIUNEA NR.1 emisă de către administratorul Platformei NET-DD (NET-DD ADMIN) la data de 25 Mai 2018

PREAMBUL.....	4
1. Proceduri specifice interne de implementare a GDPR la nivelul organizației - operator de date personale.....	6
1.1. Funcția de RESPONSABIL CU PROTECȚIA DATELOR în cadrul organizației.....	7
Procedura de notificare a Autorității Naționale de Supraveghere a Prelucrării Datelor Personale.....	8
Notificarea ANSPDP se realizează în următoarele situații:	8
Notificarea riscului de compromitere a securității datelor personale	8
Identificarea situației de risc sau de compromitere efectivă a securității datelor personale	9
1.2. Procedura Nr. 1: Reglementarea internă a managementului computerizat al datelor personale.....	9
1.2.1. Proceduri aplicate de către managementul organizației - operator	9
1.2.1.a. Proceduri preliminare.....	10
1.2.1.1. Determinarea scopurilor pentru care sunt operate date personale de către organizație	10
1.2.1.2. Determinarea / Inventarierea datelor personale care sunt prelucrate de către organizația - operator	10
1.2.1.2.a. Date prelucrate pentru managementul general al organizației	13
1.2.1.2.b. Date prelucrate pentru managementul activităților specifice ale organizației.....	14
1.2.1.3. Managementul evidențelor privind prelucrările datelor personale la nivelul organizației	14
1.2.1.4. Determinarea termenului pentru care sunt prelucrate datele cu caracter personal	15
1.2.1.5. Managementul asigurării respectării drepturilor persoanelor privitor la prelucrarea datelor personale ale acestora de către organizația operator.....	15
1.2.1.5.a. Respectarea temeiului legal pentru prelucrarea datelor personale ..	16
1.2.1.5.b. Consimțământul persoanei pentru prelucrarea datelor cu caracter personal.....	16
1.2.1.5.c. Managementul securității prelucrării datelor personale	16
Anonimizarea datelor personale.....	17
1.2.1.6. Evaluarea impactului prelucrării de către organizația - operator asupra protecției datelor cu caracter personal.....	18
1.2.1.6.a. Evaluarea riscurilor prelucrării incorecte a datelor personale.....	18
1.2.1.6.b. Evaluarea riscurilor de compromitere a securității datelor personale	19

1.2.1.6.c. Măsurile pentru minimizarea riscurilor legate de prelucrarea datelor personale	19
1.3. Procedura nr. 2: Instruirea operatorilor IT autorizați pentru asigurarea protecției datelor personale și a securității informatice	20
1.3.1. Asigurarea securității accesului la datele personale	20
1.3.1.1. Prelucrarea datelor în format analogic	20
1.3.1.2. Prelucrarea computerizată a datelor	21
Proceduri specifice:.....	21
1.3.2. Asigurarea securității prelucrării efective a datelor personale	22
1.3.3. Reglementarea accesului la datele personale	24
1.4. Procedura nr. 3: Informarea persoanelor asupra condițiilor de prelucrare a datelor și a drepturilor acestora	25
2. Specificații tehnice și de operare ale aplicațiilor IT&C utilizate pentru prelucrarea computerizată a datelor personale.....	27
2.1. Asigurarea securității informatice a aplicațiilor IT&C.....	28
2.1.1. Securitatea informatică.....	29
2.1.1.1. Tehnologia securității informatice	30
2.1.1.1.a. Funcționarea sistemelor informatice.....	31
2.1.1.1.b. Securitatea datelor.....	33
2.1.1.1.c. Securitatea accesului la date	33
2.1.1.1.c.1. Securitatea fizică a accesului la date	34
2.1.1.1.c.2. Securitatea fluxurilor informaționale	34
2.2. Mecanisme de auditare automatizate a operării aplicațiilor IT&C	36
2.2.1. Auditarea generală a operării de date personale	37
2.2.2. Auditarea generală a securității informatice a organizației - operator	38
2.2.3. Auditarea respectării prevederilor GDPR.....	39
2.3. Mecanismul automatizat pentru asigurarea respectării drepturilor persoanei privind prelucrarea datelor personale.....	39
3. LEGISLAȚIE PRIVIND PRELUCRAREA COMPUTERIZATĂ A DATELOR CU CARACTER PERSONAL.....	41
3.1. Prevederi contractuale exprese pentru respectarea GDPR.....	41
3.2. Reglementări legislative române	45
3.3. Reglementări legislative europene.....	46
4. LEGISLAȚIA PRIVIND CARDUL ELECTRONIC PERSONAL MULTIFUNCȚIONAL e-ID PERSONAL CARD - CARDUL PROFESIONAL EUROPEAN.....	48
4.1. Reglementări ale instituțiilor Uniunii Europene.....	48

4.2. Reglementări legislative române	48
5. Deficiențele prevederilor GDPR	49

PREAMBUL

Regulamentul General pentru Protecția Datelor (GDPR) este emis de către Parlamentul European și are caracter imediat obligatoriu la nivelul statelor membre. Scopul regulamentului este asigurarea unui cadru unitar legal care să garanteze respectarea drepturilor persoanelor de către toți operatorii acestor date, fie că se realizează o prelucrare analogică sau computerizată.

GDPR modifică și completează reglementarea curentă a prelucrărilor de date personale prin Directiva Comisiei Europene EC/95/46, directivă transpusă în legislația românească prin legea 677/2001.

GDPR încurajează prelucrarea computerizată a datelor personale în vederea creșterii eficienței administrative și a mobilității acestora între statele membre, cu condiția implementării unui set de proceduri precise a prevederilor acestuia, la nivelul:

- operatorilor de date personale;
- împuterniciților operatorilor de date personale;
- autorităților naționale responsabile de protecția datelor personale.

În înțelesul GDPR, toate categoriile de procesatori de date personale enumerate mai sus sunt PERSOANE JURIDICE, de aceea se impune o precizare:

- în toate documentele tehnice și de prezentare ale Platformei NET-DD și serviciilor NET-DD, termenul de **OPERATOR** definește angajatul unei organizații care utilizează aceste sisteme informatice, având pentru aceasta autorizarea expresă a organizației (operator autorizat).

Pentru evitarea oricărei confuzii, în prezentul document:

- organizația care prelucrează date personale se va denumi "**organizație operator de date personale**";
- angajații acesteia, care lucrează efectiv cu date personale, utilizând aplicații IT&C se vor denumi "**operatori IT**" sau "**operatori IT autorizați**".

NET-DD ADMIN, în calitatea sa de administrator al Platformei NET-DD și a serviciilor NET-DD integrate pe aceasta, dar și în calitate de operator de date cu caracter personal în cadrul activităților sale proprii, își asumă responsabilitatea de a pune la dispoziția tuturor operatorilor cu care are relații contractuale a unei proceduri unitare pentru implementarea GDPR și pentru instruirea permanentă, proactivă, a acestora.

Procedura elaborată de către NET-DD ADMIN prevede toate mecanismele necesare **informării persoanelor ale căror date personale sunt prelucrate** prin operatorii Platformei NET-DD și a serviciilor NET-DD asupra:

- drepturilor garantate prin GDPR;
- metodelor de protejare a datelor personale;
- utilizării sistemelor NET-DD care maximizează eficiența sistemelor de prelucrare computerizată a datelor personale prin Platforma NET-DD și prin serviciile NET-DD.

În înțelesul GDPR, datele personale pot fi prelucrate computerizat (*Platforma NET-DD și serviciile NET-DD prelucrează date personale EXCLUSIV computerizat*), prin aplicații de tipuri foarte variate:

- la cererea persoanei-posesor al datelor în cauză;
- de către un operator de date cu care o persoană are stabilite relații reglementate de diferite naturi:
 - administrative;
 - contractuale;
 - altele.

Operatorul de date NU poate prelucra datele unei persoane altfel decât:

- în conformitate cu relațiile reglementate pe care le are cu respectiva persoană;
- informând corect și complet asupra modului de utilizare a datelor prelucrate;
- cu acordul expres al persoanei (cu excepția situațiilor când legea prevede altfel), consemnat ca atare.

Datele personale pot fi folosite fără acordul expres al posesorului acestora:

- în cadrul unui contract la care acesta este parte semnatară;
- în condițiile în care există o prevedere legală expresă care să autorizeze operatorul de date în acest sens.

În toate situațiile, utilizarea de către un operator al datelor personale este **INCORECTĂ**:

- fără declararea scopului exact pentru care se face prelucrarea acestora;
- în afara **NECESITĂȚII OBIECTIVE** a prelucrării acestora pentru atingerea scopului declarat;
- excedând, în orice fel, scopul declarat -cu excepția situației când:
 - există o necesitate obiectivă și imediată pentru extinderea scopului declarat al prelucrării de date;
 - se comunică posesorului de date extinderea scopului prelucrării;
 - se obține acordul posesorului de date, dacă este necesar.

Procedura de implementare a GDPR la nivelul operatorilor de date care utilizează Platforme NET-DD presupune:

- elaborarea unui set de proceduri specifice interne;
- respectarea unui set de specificații tehnice și de operare a aplicațiilor IT&C prin care se realizează prelucrarea computerizată a datelor personale.

1. Proceduri specifice interne de implementare a GDPR la nivelul organizației - operator de date personale

Procedurile interne specifice de implementare GDPR la nivelul organizației - operator de date personale implică asigurarea, în structura organizatorică proprie, a **FUNȚIEI DE RESPONSABIL CU PROTECȚIA DATELOR**.

*În situația organizațiilor mici și medii NET-DD ADMIN recomandă crearea în organigramă a funcției de **responsabil cu protecția datelor**, cu normă de lucru zilnică de maximum 2 (două) ore, inclusiv în zilele libere.*

Contractarea unui serviciu în acest sens (externalizarea activității) este nerecomandabilă, date fiind:

- costul excesiv al serviciului;
- **acordarea accesului la sistemele informatice proprii și la datele procesate prin acestea a unui terț, ceea ce crește riscurile de încălcare a confidențialității;**
- dificultatea asigurării permanenței serviciului de protecție a datelor, conform GDPR.

Îndeplinirea prevederilor funcției de responsabil de protecția datelor de către oricare angajat al organizației **NU** presupune, conform GDPR:

- **instruirea** acestuia, altfel decât prin instruirea asupra pachetului de proceduri puse la dispoziție de către NET-DD ADMIN, prin prezenta documentație;
- **certificarea** acestuia de vreo instituție a statului sau de vreo organizație de certificare, publică sau privată.

Pentru maximum de formalism legal, NET-DD ADMIN asigură un **SISTEM DE CERTIFICARE INTERNĂ A INSTRUIRII ADECVATE A RESPONSABILULUI DE PROTECȚIA DATELOR**, pentru toate organizațiile partenere, utilizatoare ale sistemelor informatice, ale Platformei NET-DD sau altele.

1.1. Funcția de RESPONSABIL CU PROTECȚIA DATELOR în cadrul organizației

Responsabilul de protecția datelor (RPD) din cadrul organizației trebuie să cunoască prevederile Regulamentului General de Protecție a Datelor (**GDPR**) al Uniunii Europene și să asigure punerea în aplicare, la nivelul organizației, a acestora, **ÎN COLABORARE PERMANENTĂ CU MANAGEMENTUL ORGANIZAȚIEI - OPERATOR**, prin:

- implementarea și asigurarea respectării procedurilor GDPR descrise în prezenta documentație:
 - instruirea periodică a angajaților care asigură prelucrarea datelor personale:
 - ale angajaților și colaboratorilor organizației;
 - ale beneficiarilor activității organizației;
 - informarea persoanelor ale căror date sunt prelucrate de către organizație;
 - informarea managementului organizației asupra procedurilor de implementare a GDPR;
- instruirea periodică asupra documentației oficiale privind implementarea GDPR, prin sistemul periodic de instruire al Platformei NET-DD (**NET-DD GDPR**).

O responsabilitate expresă a RPD este colaborarea permanentă și eficientă cu:

- furnizorii de servicii pentru prelucrarea datelor cu caracter personal - **ÎMPUTERNICIȚII** organizației - operator;
- Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal.

Toate **sistemele computerizate** utilizate pentru prelucrarea datelor personale **TREBUIE să fie prevăzute**, pe lângă sistemele de auditare a prelucrărilor de date personale (*capitolul 2.2.*), **cu sisteme de alertare în timp real** pentru:

- riscul de compromitere a datelor personale;
- riscul de compromitere a securității datelor personale;
- încălcarea procedurilor de prelucrare a datelor personale;
- compromiterea securității datelor personale;
- compromiterea securității și confidențialității datelor personale.

RPD TREBUIE să poată fi notificat în timp real prin toate aceste sisteme de alertă, astfel ca să poată lua măsuri imediate, sau în termen maxim de 72 de ore.

Procedura de notificare a Autorității Naționale de Supraveghere a Prelucrării Datelor Personale

Notificarea Autorității Naționale de Supraveghere a Prelucrării Datelor Personale, se realizează prin:

- procedura directă:
 - on-line, prin adresa web a autorității;
 - prin adresarea telefonică a autorității;
- procedura automatizată - notificarea Autorității prin Platforme NET-DD de către NET-DD ADMIN.

Notificarea ANSPDP se realizează în următoarele situații:

1. demararea oricărei noi prelucrări de date personale de către organizația operator -prin procedura directă on-line;
2. solicitarea autorizării exprese pentru prelucrare de date cu caracter personal speciale (sensibile), în condițiile legislației naționale în vigoare - procedura directă on-line;
3. identificarea unui risc imediat de compromitere a securității datelor personale prelucrate de către organizația - operator:
 - 4.1. la nivelul organizației;
 - 4.2. la nivelul împuterniciților organizației - operator, furnizori de servicii de prelucrare a datelor personale:
 - a. procedura automatizată - în cazul serviciilor operate prin Platforma NET-DD;
 - b. procedura directă.

Notificarea riscului de compromitere a securității datelor personale

Pe lângă notificarea ANSPDP, riscul de compromitere sau compromiterea efectivă a securității datelor personale la nivelul unei organizații - operator se notifică imediat (sau în maximum 72 de ore) **TUTUROR POSESORILOR DE DATE AFECTAȚI.**

Notificarea posesorilor de date trebuie să conțină:

- tipul datelor afectate;
- durata pentru care au fost compromise;
- dacă defectul care a produs compromiterea datelor este remediat;
- recomandări pentru a evita efectele compromiterii temporare a datelor.

Același set de informații trebuie comunicate ANSPDP.

Utilizatorii Platformei NET-DD pot utiliza procedura automatizată pentru ambele tipuri de notificări pentru serviciile acestora aflate în operare, prin:

- PORTALUL NET-DD și sistemul de card personal multifuncțional NET-DD CARD;
- prin lansarea în bloc a unui mesaj de notificare către adresele de e-mail ale tuturor posesorilor de date afectați.

Pentru orice alt tip de servicii, procedura de notificare directă este imperativă.

Identificarea situației de risc sau de compromitere efectivă a securității datelor personale

Această procedură specifică RPD este asigurată prin:

- procedurile interne ale organizației operator (*Capitolul 1.2., 1.3.*);
- sistemele de auditare automatizată a prelucrărilor computerizate (*Capitolul 2*).

1.2. Procedura Nr. 1: Reglementarea internă a managementului computerizat al datelor personale

În conformitate cu prevederile GDPR și a legislației naționale în domeniu, oricare organizație - operator de date personale trebuie să reglementeze intern următoarele aspecte procedurale:

- proceduri pentru managementul organizației;
- proceduri pentru operatorii de date personale:
 - angajați ai organizației;
 - colaboratori externi (*se vor utiliza contracte de colaborare care să conțină prevederile contractuale specifice GDPR precizate în Capitolul 2./2.3*);
- proceduri pentru achiziția de sisteme informatice pentru prelucrarea computerizată a datelor personale (*vezi Capitolul 2*).

Procedurile cuprinse în prezentul document nu sunt aplicabile exclusiv prelucrărilor computerizate de date personale, ci și prelucrărilor utilizând formate analogice.

1.2.1. Proceduri aplicate de către managementul organizației - operator

Procedurile pentru implementarea GDPR de către managementul organizației - operator sunt detaliate în anexele standardizate corespunzătoare fiecărui punct al acestui capitol. Anexele sunt identificate cu numărul subcapitolului căruia acestea corespund.

1.2.1.a. Proceduri preliminare

Managementul organizației - operator trebuie să demareze implementarea GDPR prin următoarele proceduri preliminare:

1. **De desemnarea și instruirea, utilizând prezenta documentație, a RESPONSABILULUI CU PROTECȚIA DATELOR (capitolul 1.1).**
2. **Implementarea măsurilor de securitate fizică a datelor personale prelucrate de către organizația - operator:**
 - a. **prin asigurarea securității fizice a depozitelor datelor personale (analogice și digitale);**
 - b. **managementul riguros al drepturilor de acces și de operare a datelor personale de către fiecare membru autorizat al organizației - operator de date personale, sub controlul RPD.**

Măsurile de securitate informatică a datelor personale sunt realizate prin implementarea procedurilor prezentate în capitolul 2.1.

1.2.1.1. Determinarea scopurilor pentru care sunt operate date personale de către organizație

Conform legislației în vigoare privind prelucrarea datelor personale, declararea exactă a scopurilor pentru care aceste date sunt colectate și prelucrate de către fiecare operator de date este, deja, obligatorie.

GDPR întărește această obligativitate, în sensul:

- corelării precise a fiecărui scop pentru care se prelucrează date personale cu determinarea strictă a NECESITĂȚII colectării fiecărei date personale în parte spre prelucrare;
- explicitarea motivelor pentru care necesită prelucrarea fiecărei date în parte ;
- asigurării comunicării scopului și necesității prelucrării fiecărei date în parte către posesorul datelor personale în cauză.

Scopul prelucrării datelor personale și necesitatea colectării fiecărei date personale în parte pentru realizarea scopului enunțat determină inventarierea datelor personale prelucrate (capitolul 1.2.1.2).

1.2.1.2. Determinarea / Inventarierea datelor personale care sunt prelucrate de către organizația - operator

Datele personale prelucrate de către organizația-operator, în vederea implementării eficiente și riguroase a GDPR, se clasifică:

- în funcție de sensibilitatea datelor (care determină nivelul de securitate al prelucrării acestora):
 - date publicabile;
 - date confidențiale;
 - date sensibile;
 - date protejate;
- în funcție de posibilitățile de utilizare de către organizația - operator:
 - date de uz strict intern - date blocate;
 - date utilizabile între organizațiile relaționate:
 - subordonate;
 - supraordonate;
 - terțe organizații contractate.

Datele utilizabile între organizații sunt:

- date partajabile;
- date transmisibile;
- date publicabile.
- în funcție de natura datelor:
 - date de identificare personală:
 - date subiective:
 - prenume;
 - porecla personală;
 - date obiective:
 - nume;
 - inițialele părinților;
 - porecla familiei;
 - fotografie;
 - gen;
 - data nașterii;
 - locul nașterii:
 - continent;
 - țară;
 - unitate administrativ-teritorială;
 - localitate;
 - adresă:
 - locuință;
 - maternitate;
 - cod numeric personal;
 - date personale biologice:
 - date antropologice:
 - tip antropologic;
 - rasă;
 - date antropometrice;
 - date biometrice;
 - date genetice de identificare;

- date medicale:
 - date clinice;
 - date paraclinice;
 - date farmaceutice;
- date personale sociale:
 - cetățenie;
 - rezidență;
 - etnie;
 - apartenență religioasă;
 - adrese:
 - domiciliu;
 - rezidență;
 - altele;
 - date educaționale;
 - date profesionale;
 - date patrimoniale;
 - date financiare:
 - conturi bancare;
 - date fiscale;
 - date de salarizare;
 - date privind alte venituri;
 - date de asigurare:
 - asigurare medicală;
 - asigurare de malpraxis;
 - asigurare generală;
 - alte asigurări;

Fiecărei date personale prelucrate conform procedurilor descrise în prezentul document trebuie să îi fie asociată, în anexele sale:

- scopul prelucrării;
- clasa din care face parte.

De exemplu: date de identificare (antropologice, antropometrice, biologice) și sociale (de tipul etniei, religiei, mediului de trai, mediului de muncă, obiceiurilor de viață - fumat, consum de alcool, etc.) sunt de interes pentru **scopul MEDICAL** al prelucrărilor de date personale.

Aparent, religia sau etnia nu ar fi direct legate de problemele medicale ale persoanei, dar, în realitate, POT FI FOARTE RELEVANTE, anumite afecțiuni genetice și metabolice (și nu numai) fiind strâns legate de etnie, rasă sau obiceiuri determinate de religie.

Datele personale prelucrate de către organizația - operator se clasifică, în funcție de scopul general al prelucrării în:

- date prelucrate pentru managementul general al organizației;
- date prelucrate pentru managementul activităților specifice ale organizației.

Este evident că o parte a datelor privind activitățile specifice ale organizației sunt prelucrate în scop managerial:

- în format complet;
- în format anonimizat (*vezi capitolul 1.2.1.5.c.*).

1.2.1.2.a. Date prelucrate pentru managementul general al organizației

Managementul general al oricărei organizații moderne implică prelucrarea unui pachet de date personale:

- ale angajaților;
- ale beneficiarilor activităților prestate de către angajați:
 - persoane fizice;
 - reprezentanți ai persoanelor juridice;
- ale furnizorilor de bunuri și servicii ai organizației;
- ale personalului organizațiilor cu care au raporturi instituționale conform legii.

Managementul activităților specifice ale organizației presupune extinderea pachetelor de date personale altele decât cele ale angajaților, detaliate în capitolul 1.2.1.2.b.

Datele personale prelucrate pentru asigurarea managementului organizației - operator de date este necesar a fi inventariate într-o anexă a prezentului subcapitol.

Acestor date personale le sunt asociate:

- date financiar - contabile;
- date patrimoniale ale organizației;
- date privind activitățile specifice executate de către fiecare angajat al organizației (*capitolul 1.2.1.2.b.*).

Scopul principal al prelucrării acestor date sunt:

- analiza și decizia managerială;
- raportarea financiar - contabilă conform legii;
- elaborarea de documente comerciale relevante;
- susținerea activităților de promovare, marketing și comerciale;
- orice altă activitate care este necesară derulării optime a activității organizației-operator.

1.2.1.2.b. Date prelucrate pentru managementul activităților specifice ale organizației

Datele personale prelucrate în cadrul activităților specifice ale organizației - operator sunt relaționate:

- datelor personale ale angajaților care asigură derularea respectivelor activități asupra beneficiarilor acestora;
- datelor financiar - contabile asociate resurselor organizației - operator:
 - alocate derulării activităților;
 - rezultate din derularea activităților;
- asigurării datelor și informațiilor relevante STRICT NECESARE derulării optime a activităților.

În funcție de fiecare activitate specifică a organizației - operator, **pachetele de date personale** prelucrate sunt stabilite cu rigurozitate și comunicate posesorilor acestora, conform prevederilor GDPR.

NET-DD ADMIN specifică inventarul datelor personale prelucrate conform scopului fiecărui **serviciu NET-DD** de informatizare a activităților specifice organizațiilor - operator utilizatoare, pentru uzul RPD al acestora - acestea corespund interfețelor de achiziție de date personale specifice fiecărui serviciu NET-DD. Transmiterea acestor informații către posesorul datelor fiind obligația organizației - operator, prin RPD.

1.2.1.3. Managementul evidențelor privind prelucrările datelor personale la nivelul organizației

Datele personale se prelucrează conform reglementărilor din capitolele precedente.

Evidența prelucrărilor de date conforme se asigură de către RPD prin:

- metode analogice -registrul scris al prelucrărilor de date;
- registrul electronic de evidență a prelucrărilor de date – organizația - operator de date personale **TREBUIE** să solicite în mod expres furnizorilor de servicii IT contractați în scopul computerizării prelucrărilor de date, inclusiv de date personale, ca aplicațiile furnizate să fie prevăzute cu sisteme de auditare și raportare a rezultatelor audității, cu specificații descrise în capitolul 2.2.

Evidențele prelucrărilor de date personale trebuie să poată fi puse la dispoziția posesorilor respectivelor date:

- în format analogic - generat și livrat pe bază de semnătură de primire, de către RPD;
- în format digital - prin mecanismul automatizat pentru asigurarea respectării drepturilor persoanei privind prelucrarea datelor personale (*capitolul 2.3.*).

1.2.1.4. Determinarea termenului pentru care sunt prelucrate datele cu caracter personal

În funcție de scopurile pentru care sunt prelucrate, datele personale pot fi utilizate:

- pentru o singură dată - fiind uitate imediat ce scopul prelucrării este realizat - exemplu: emiterea unei chitanțe pentru o încasare în numerar, uitarea intervenind la data expirării obligativității legale de păstrare a documentelor contabile (5 ani în prezent);
- pentru o durată limitată - exemplu: pe durata unui contract de muncă, uitarea intervenind în același termen ca mai sus;
- pe durată nelimitată - exemplu:
 - istoricul fiscal sau medical al unei persoane;
 - datele de evidență a populației.

ESTE OBLIGATORIE MENȚIONAREA DURATEI DE PRELUCRARE A DATELOR ÎN TEXTUL DE INFORMARE ÎN VEDEREA OBTINERII CONSIMȚĂMÂNTULUI PERSOANEI PENTRU PRELUCRAREA DATELOR PERSONALE (*capitolul 1.2.1.5.*)

1.2.1.5. Managementul asigurării respectării drepturilor persoanelor privitor la prelucrarea datelor personale ale acestora de către organizația operator

Principalul drept al posesorului de date personale (respectiv persoana însăși) este **ASIGURAREA CONFIDENȚIALITĂȚII** tuturor prelucrărilor efectuate asupra lor, în condițiile legii. Altfel spus, doar o reglementare legală specială poate să anuleze dreptul la garantarea confidențialității prelucrărilor de date personale.

Prin GDPR se adaugă dreptul la confidențialitate, următoarele drepturi suplimentare ale persoanei:

- dreptul de informare și acces la date cu caracter personal,
- dreptul la rectificare,
- dreptul la ștergerea datelor („dreptul de a fi uitat”),
- dreptul la restricționarea prelucrării,
- dreptul la portabilitatea datelor,
- dreptul la opoziție,
- dreptul la decizie individuală automatizată.

1.2.1.5.a. Respectarea temeiului legal pentru prelucrarea datelor personale

În conformitate cu legislația națională și europeană (*Capitolul 3*), situațiile generale reglementate pentru care pot fi prelucrate datele cu caracter personal sunt:

- persoana vizată și-a dat consimțământul;
- datele sunt necesare pentru executarea unui contract la care persoana vizată este parte;
- îndeplinirea unei obligații legale a societății,
- prelucrarea este necesară în scopul intereselor legitime ale societății.

Pe lângă aceste situații, organizația - operator poate prelucra date personale în condițiile legilor speciale, în acest caz, managementul organizației conformându-se prevederilor în cauză.

1.2.1.5.b. Consimțământul persoanei pentru prelucrarea datelor cu caracter personal

Managementul organizației - operator de date personale trebuie să implementeze, în acord cu cele de mai sus, procedura pentru informarea și obținerea consimțământului posesorului de date personale pentru prelucrarea acestora, conform Procedurii de la Capitolul 1.3.

Redactarea conținutului informativ al formatului pentru obținerea consimțământului trebuie să asigure prezentarea explicită a tuturor procedurilor din Capitolul 1.2.

1.2.1.5.c. Managementul securității prelucrării datelor personale

Organizația - operator de date cu caracter personal asigură managementul securității datelor personale prin:

- implementarea procedurilor pentru instruirea operatorilor autorizați să prelucreze date personale (*Capitolul 1.3.*);
- asigurarea conformității sistemelor de prelucrare a datelor personale utilizate (*Capitolul 2.*):
 - existente - revizuirea contractelor de prestări servicii (computerizate sau analogice) cu împuterniciții;
 - nou achiziționate.

Anonimizarea datelor personale

Anonimizarea datelor personale este un mecanism esențial în maximizarea protecției acestora: în procesele de prelucrare computerizată; în cadrul transferurilor de date necesare asigurării fluxurilor informaționale; în condițiile stocării și arhivării pe termen lung a datelor.

NET-DD ADMIN a dezvoltat sisteme de prelucrare a datelor personale care asigură completa anonimizare a acestora, inclusiv în raport cu operatorii care asigură prelucrările de date. Aceste sisteme, însă, sunt complicate de utilizat în condițiile în care responsabilitatea persoanei - posesor al datelor personale este foarte dificilă (din motive de pregătire IT, de conștiință civică, de vârstă, motive de ordin social și educațional, etc).

Totuși, este important de înțeles de către operatorii de date personale că sistemele moderne de prelucrare computerizată permit grade progresive de anonimizare a datelor: față de operatorii autorizați de date personale, raportate: necesității de personalizare a datelor prelucrate; nivelului de sensibilitate al datelor prelucrate.

De exemplu:

- datele personale ale unui salariat al organizației - operator de date:
 - nu pot fi anonimizate pentru operatorul autorizat al serviciului de resurse umane;
 - pot fi anonimizate pentru operatorul serviciului de contabilitate

sau

- datele personale ale unui pacient:
 - nu pot fi anonimizate pentru medic;
 - pot fi anonimizate pentru serviciul de contabilitate al spitalului.

Capitolul 2.1. prezintă toate specificațiile tehnice și procedurile prin care se asigură securitate optimală a prelucrărilor de date personale, inclusiv mecanismele de anonimizare, dar, din perspectiva GDPR, este necesar ca **RPD**:

- **să solicite, în cunoștință de cauză, implementarea mecanismelor de anonimizare a datelor de către furnizorii de servicii IT&C;**
- **să anonimizeze datele personale în documente analogice sau digitale emise de către organizația - operator, de fiecare dată când este necesar, pentru a proteja drepturile persoanei.**

DEZANONIMIZAREA DATELOR PERSONALE este un mecanism recomandat ca **OBLIGATORIU** de către NET-DD ADMIN, tuturor operatorilor, managementul responsabil al acestui mecanism fiind atributul RPD.

1.2.1.6. Evaluarea impactului prelucrării de către organizația - operator asupra protecției datelor cu caracter personal

Activitatea oricărei organizații depinde de prelucrarea unui volum specific de date cu caracter personal, accesibile unui număr de persoane și organizații autorizate în acest sens:

- de către organizația-operator;
- prin lege.

În acest context, este necesară o evaluare eficientă a impactului pe care aceste prelucrări le poate avea asupra datelor personale și posesorilor acestora, dar și asupra societății, urmată de stabilirea unor măsuri eficiente pentru anulare tuturor potențialelor efecte negative.

1.2.1.6.a. Evaluarea riscurilor prelucrării incorecte a datelor personale

Declararea incorectă a scopurilor prelucrării datelor personale trebuie evitată cu prioritate de către managementul organizației - operator.

Pe de altă parte, în condițiile implementării procedurilor interne descrise în prezentul capitol, managementul organizației trebuie să evalueze și să ia măsuri în consecință pentru:

- Evaluarea efectelor prelucrării incorecte a datelor personale în interesul direct al operatorului de date:
 - transmiterea datelor prelucrate:
 - în interes propriu;
 - în interesul unor organizații la care operatorul este afiliat;
 - publicarea ilicită a datelor personale;
 - comercializarea datelor personale prelucrate la care operatorul are acces;
- Evaluarea efectelor prelucrării datelor personale prin sisteme inteligente utilizând volume mari de date (big data) (*evaluarea prelucrării pe scară largă a unor categorii speciale de date sau în cazul evaluării sistematice a aspectelor personale, care se bazează pe prelucrarea automată și care stă la baza unor decizii care produc efecte asupra persoanei fizice²*):
 - efecte juridice;
 - efecte sociale;
 - efecte politice;
 - efecte comerciale/financiare;
 - efecte psihologice.

² Vezi scandalul "Cambridge Analytica".

1.2.1.6.b. Evaluarea riscurilor de compromitere a securității datelor personale

Compromiterea securității datelor personale se poate realiza:

- la nivelul operatorilor autorizați ai organizației - operator de date, prin nerespectarea procedurilor de la *capitolul 1.4.*;
- la nivelul sistemelor IT&C utilizate pentru prelucrarea computerizată a datelor personale, prin nerespectarea condițiilor și specificațiilor precizate la *capitolul 2.*;
- prin nerealizarea sau nerespectarea condițiilor contractuale cu împuterniciții organizațiilor-operator de date personale, conform *capitolului 3.*

1.2.1.6.c. Măsuri pentru minimizarea riscurilor legate de prelucrarea datelor personale

Măsurile necesare a fi luate conform evaluării riscurilor de prelucrare incorectă sunt parte a procedurilor stabilite la *capitolul 1.4.*

Măsurile necesare a fi luate conform evaluării riscurilor de compromitere a securității datelor personale sunt parte a procedurilor stabilite la *capitolele 1.3. și 2.1.*

1.3. Procedura nr. 2: Instruirea operatorilor IT autorizați pentru asigurarea protecției datelor personale și a securității informatice

Instruirea operatorilor IT autorizați de către organizația - operator de date personale este responsabilitatea RPD al organizației și prevede următoarele proceduri specifice:

1.3.1. Asigurarea securității accesului la datele personale

1.3.1.1. Prelucrarea datelor în format analogic

- accesul la datele personale operate în format analogic este realizat prin accesul restricționat la depozitele / arhivele organizației:
 - cheie;
 - card de acces;
- accesul la formulare de prelucrare a datelor personale conform drepturilor de prelucrare - trebuie verificat de către un angajat cu funcție de registrator/arhivar:
 - formularele trebuie marcate cu datele/însemnele organizației;
 - identificarea persoanei care prelucrează datele trebuie să fie vizibilă și completă;
 - sistemul de arhivare/depozitare al organizației trebuie să se regăsească în formular;
- controlul prelucrărilor de date ale fiecărui operator autorizat trebuie să se realizeze sistematic:
 - de către un superior;
 - de către RPD;
- pe durata prelucrării datelor, operatorul trebuie să asigure securitatea formularelor utilizate:
 - accesul terților trebuie să se facă numai reglementat:
 - cine are drept de vizualizare a datelor în cursul prelucrării;
 - cine are drept de verificare;
 - cine are drept de suprascriere;
 - cine are dreptul să închidă procesul de prelucrare a datelor;
 - comunicarea dintre operator și persoana ale cărei date sunt prelucrate trebuie să se facă în mod confidențial:
 - participarea altor persoane din cadrul organizației trebuie reglementată³;
 - acordul persoanei:

³ Exemplu din medicină unde medicul ia în calcul:

- prelucrarea de date în prezența unei asistențe este obligatorie;
- participarea studenților la procesul de tratament al pacientului;
- consult interdisciplinar;
- altele, conform specificului activităților medicale.

- trebuie să fie explicit în acest sens;
- este implicit;
- arhivarea/depozitarea datelor prelucrate, după încheierea procesului de prelucrare:
 - se face imediat după încheierea prelucrării, în facilitățile securizate ale organizației;
 - trebuie verificată de către un angajat cu funcție de registrator/arhivar.

SECURITATEA ACCESULUI LA DATE ESTE RESPONSABILITATEA COMUNĂ A:

- OPERATORULUI AUTORIZAT:
- REGISTRATORULUI/ARHIVARULUI.

SUPRAVEGHEREA ASIGURĂRII SECURITĂȚII ACCESULUI LA DATE ESTE RESPONSABILITATEA RPD.

1.3.1.2. Prelucrarea computerizată a datelor

Dacă în cursul prelucrării computerizate a datelor se utilizează și formate analogice asociate procesului de prelucrare, se vor respecta, pentru aceasta, toate procedurile de mai sus.

Proceduri specifice:

- asigurarea securității terminalelor prin care se operează date - accesul fizic în spațiile unde funcționează terminalele trebuie:
 - restricționat, accesul fiind rezervat exclusiv operatorilor IT autorizați;
 - securizat:
 - sub cheie;
 - prin card de acces;
 - mixt;
 - terminalele de operare trebuie PAROLATE;
 - logarea operatorului IT trebuie să fie unică, personalizată prin:
 - cont de acces parolat;
 - citire de card de identificare;
 - sistemele IT utilizate trebuie să asigure delogarea automată după un interval rezonabil de inactivitate (recomandarea este nu mai lung de 30 de minute);
- asigurarea securității transferurilor de date prin securizarea tuturor punctelor de conectare dintre terminale și unitățile centrale de operare:
 - sisteme intranet;
 - sisteme internet;
 - sisteme mixte;
- asigurarea securității accesului la unitățile centrale de operare:

- accesul restricționat, rezervat exclusiv personalului cu funcție în procedurile de mentenanță⁴;
- accesul procedurat în cazul serviciilor externalizate către centre de date⁵;
- asigurarea securității împotriva riscurilor transferurilor de date prin internet:
 - toate echipamentele periferice utilizate în prelucrarea datelor personale **TREBUIE SĂ AIBĂ ACCES RESTRICȚIONAT LA INTERNET:**
 - prin utilizarea de servicii securizate de conectivitate (VPN, MPLS, VPLS);
 - prin limitarea accesului operatorilor strict la domeniile web utilizate în activitatea organizației (evitarea accesării de domenii web nesigure);
 - prin eliminarea utilizării serviciilor de poștă electronică publice (tip gmail sau yahoo);
- operatorii IT autorizați **TREBUIE** să evite orice formă de dispozitiv de memorie externă, încărcarea de documente sau alte tipuri de fișiere realizându-se exclusiv prin metode care nu prezintă riscuri de infectare a sistemelor de operare IT&C.

Recomandarea este ca toate comunicațiile digitale ale organizațiilor - operator de date personale să se realizeze exclusiv prin sistemele de telecomunicații securizate enumerate mai sus.

Serviciile de poștă electronică securizate TREBUIE monitorizate permanent de către un operator dedicat.

OPERATORII IT&C NU POT, SUB NICI UN MOTIV, SĂ TRANSFERE DATELE/CARDURILE PROPRII DE LOGARE ALTOR PERSOANE, INDIFERENT DE ROLUL ACESTORA ÎN ORGANIZAȚIE SAU ÎN AFARA ACESTEIA.

1.3.2. Asigurarea securității prelucrării efective a datelor personale

Securitatea prelucrării efective (propriu-zise) a datelor personale este responsabilitatea directă a operatorului autorizat care realizează prelucrarea în cadrul activităților specifice ale organizației-operator.

1. Confidențialitatea prelucrării datelor presupune asigurarea unui mediu de lucru cu posesorul datelor personale adecvat - schimbul de informații între persoană și operatorul autorizat trebuie să se realizeze fără a putea fi interceptat de către terți;

⁴ Procedurile de mentenanță trebuie solicitate tuturor furnizorilor de sisteme și servicii IT&C de către RPD și trebuie comunicate prin instructaj personalului organizației.

⁵ Procedurile de securitate și asigurare a accesului trebuie puse la dispoziție de către furnizorii IT&C (împuterniciți ai organizației - operator) și comunicate personalului organizației prin instructaj.

2. Mediile de achiziție și de stocare (analogice, digitale sau mixte) a datelor personale pe durata prelucrării trebuie să fie securizate de către operator pe întreaga durată a prelucrării;
3. Prelucrarea propriu - zisă a datelor poate fi realizată de către operatori multipli:
 - a. din cadrul unei singure organizații;
 - b. din organizații multiple.

În acest caz este **IMPERATIV** ca operatorul fiecărei prelucrări de date în parte să fie identificat:

- a. la începutul prelucrării realizate;
 - b. la finalul prelucrării realizate;
4. Rezultatele prelucrărilor de date trebuie securizate, accesul la acestea fiind reglementat (capitolul 1.3.3.):
 - a. pe durata prelucrării;
 - b. după finalizarea prelucrării.

Rezultatele prelucrării datelor personale sunt destinate (BENEFICIARIILOR PRELUCRĂRILOR DE DATE):

- organizației - operator;
- posesorului datelor personale;
- unor terțe părți interesate;
- publicului larg.

Operatorii autorizați trebuie să asigure securitatea datelor și a rezultatelor prelucrării acestora:

- prin asigurarea securității accesului (capitolul 1.3.1.);
- asigurarea securității comunicării (capitolul 2.1.);
- prin asigurarea accesului reglementat la date și la rezultatele prelucrării acestora (capitolul 1.3.3.).

Rezultatele prelucrării datelor personale trebuie prezentate destinatarilor acestora:

- în formatul standardizat și personalizat al organizației - operator;
- cu identificatorul operatorului/operatorilor autorizați care au realizat prelucrările de date.

Comunicarea rezultatelor prelucrării datelor trebuie să prezinte înregistrarea confirmării primirii comunicării de către destinatar.

1.3.3. Reglementarea accesului la datele personale

Reglementarea accesului la date personale este produsă de către organizația - operator, supravegheată de către RPD și pusă în practică de către operatorii autorizați ai organizației.

Reglementarea accesului la date personale are în vedere:

- accesul la date personale;
- accesul la mecanismele de prelucrare a datelor personale;
- accesul la rezultatele prelucrării datelor personale;
- accesul la depozitele și arhivele de date personale.

Reglementarea accesului la datele personale se realizează prin definirea **DREPTURILOR DE ACCES** și prin alocarea adecvată a acestora:

- operatorii autorizați;
- către beneficiarii prelucrărilor de date;
- către publicul larg - DATE PUBLICABILE.

Clasificarea generală a drepturilor de acces utilizată în Platforma NET-DD:

- drept de administrator:
 - poate accesa și prelucra date fără restricții;
 - alocă drepturile de operator autorizat;
 - alocă drepturile de acces ale operatorilor autorizați;
 - poartă întreaga răspundere a prelucrării datelor de către organizația-operator;
- drept de procesare de date:
 - complet;
 - restricționat;
- drept de vizualizare de date;
- drept de vizualizare anonimată de date;
- drept de prelucrare a datelor:
 - complet;
 - restricționat;
- drept de vizualizare a rezultatelor prelucrărilor de date;
- drept de utilizare a rezultatelor prelucrărilor de date:
 - prin comunicare;
 - prin tipărire și comunicare;
 - prin comunicare și prin transfer;
 - prin partajare;
 - prin publicare.

Un sistem computerizat pentru management informațional TREBUIE să fie prevăzut cu un mecanism eficient pentru reglementarea accesului la datele personale publicate.

Accesul la datele personale și la rezultatele prelucrării acestora al posesorului datelor (persoana) este reglementat special, conform prevederilor GDPR, fiind garantat:

- prin acces fizic;
- prin solicitarea de rapoarte în format analogic;
- prin internet - în cazul Platformei NET-DD și a serviciilor sale integrate, accesul liber securizat al persoanei la propriile date prelucrate se realizează prin PORTALUL NET-DD accesibil acesteia prin autentificare on-line.

1.4. Procedura nr. 3: Informarea persoanelor asupra condițiilor de prelucrare a datelor și a drepturilor acestora

Informarea persoanelor asupra condițiilor de prelucrare a datelor personale și a drepturilor pe care le au, în acest sens, conform GDPR este principala preocupare a acestui regulament european, scopul fiind evitarea utilizării excesive sau cu rea-credință a respectivelor date.

Operatorii autorizați pentru prelucrarea datelor personale TREBUIE să se asigure, pentru fiecare persoană ale cărei date le prelucrează, că:

- pot realiza în orice moment, informarea corectă și completă a persoanei ale cărei date începe să le prelucreze, asupra condițiilor de prelucrare și a drepturilor de care dispune în acceptarea prelucrării;
- pot certifica faptul că:
 - persoana a fost informată;
 - a dat acceptul pentru prelucrarea datelor;
- drepturile persoanei sunt respectate în totalitate prin procedurile și mecanismele de prelucrare a datelor pe care le utilizează.

Procedura de informare a persoanei este:

- adoptată de către organizația-operator;
- implementată și verificată în permanență de către RPD;
- aplicată cu rigurozitate de către operatorii autorizați.

Platforma NET-DD este prevăzută cu:

- un sistem complet de informare a persoanelor, conform tuturor prevederilor GDPR;
- un sistem standard de certificare a realizării corecte a informării persoanelor;
- un sistem optimizat dedicat managementului informațional realizat de către persoanele - posesor al datelor:
 - sistemul NET-DD CARD, denumit "**e-ID PERSONAL**";
 - PORTALUL NET-DD.

Rigoarea și eficiența sistemului **NET-DD CARD** excede prevederile GDPR, constituind o **GARANȚIE ABSOLUTĂ** asupra respectării drepturilor persoanei în prelucrarea datelor personale prin Platforma NET-DD și serviciile NET-DD integrate.

NICI O PRELUCRARE DE DATE PERSONALE DE CĂTRE VREUN OPERATOR AL PLATFORMEI NET-DD NU POATE FI REALIZATĂ ȘI FINALIZATĂ ALTFEL DECÂT:

- **ÎN PREZENȚA POSESORULUI DE DATE;**
- **DUPĂ CITIREA CARDULUI e-ID PERSONAL;**
- **DUPĂ INTRODUCEREA UNUI COD PIN ASOCIAT CARDULUI DE CĂTRE POSESORUL ACESTUIA.**

2. Specificații tehnice și de operare ale aplicațiilor IT&C utilizate pentru prelucrarea computerizată a datelor personale

Prelucrarea computerizată a datelor personale a devenit standard în funcționarea societății moderne, datorită eficienței crescute și costurilor reduse. Idealul ar fi ca, prin procesare computerizată informațională, în general și a datelor personale, în particular, să se elimine suportul de hârtie în toate activitățile umane.

Platforma NET-DD este o dovadă operațională că acest obiectiv poate fi atins în timp scurt.

Tehnologia, oricât de avansată este, presupune, pe lângă avantajele semnificative, RISCURI. Din acest motiv, prelucrarea computerizată a datelor trebuie să se realizeze utilizând sisteme informatice competente și sigure, descrise de setul de specificații tehnice și de operare prezentate în acest capitol. Aceste specificații asigură:

- SECURITATE;
- EFICIENȚĂ;
- ADAPTABILITATE.

Securitatea prelucrării datelor personale trebuie să asigure, conform GDPR:

- confidențialitatea,
- integritatea,
- disponibilitatea și rezistența continue ale sistemelor și serviciilor de prelucrare,
- un proces pentru testarea, evaluarea și aprecierea periodică ale eficacității măsurilor tehnice și organizatorice.

Aceste caracteristici generale sunt detaliate în capitolul 2.1.

Eficiența prelucrării computerizate a datelor presupune (în linii mari):

- implementare rapidă;
- cost de operare minimal;
- operare eficientă:
 - timp de lucru cât mai redus pentru fiecare operațiune de prelucrare de date;
 - costuri minime de personal dedicat;
- asigurarea CORECTITUDINII DATELOR PRELUCRATE:
 - prin operare corectă a datelor;
 - prin aplicarea de mecanisme inteligente de verificare a corectitudinii datelor;
 - prin aplicarea de mecanisme de actualizare eficientă a datelor;
- utilizarea de algoritmi de prelucrare a datelor eficienți:
 - sub aspectul resurselor utilizate;
 - sub aspectul relevanței rezultatelor prelucrării.

Adaptabilitatea sistemelor de prelucrare computerizată a datelor constă din capacitatea acestora de a fi reprogramate, de oricâte ori este necesar, pentru a asigura maximum de eficiență (societatea și tehnologia sunt dinamice, aceste sisteme trebuind să se adapteze fără discontinuități).

Din perspectiva GDPR esențiale sunt:

- asigurarea securității informatice a sistemelor IT&C utilizate în prelucrarea datelor personale;
- disponibilitatea unor mecanisme de auditare și control a respectării prevederilor GDPR;
- asigurarea accesului persoanei - posesor al datelor personale în sistemele IT&C care îi prelucrează computerizat pachete de date personale.

2.1. Asigurarea securității informatice a aplicațiilor IT&C

Asigurarea securității informatice a aplicațiilor IT&C utilizate în prelucrarea datelor personale este responsabilitatea partajată a:

- Organizației - operator de date;
- împuterniciților organizației-operator;
- furnizorului de aplicații IT&C.

În cazul Platformei NET-DD, NET-DD ADMIN are calitatea de împuternicit și furnizor de aplicații IT&C pentru toate organizațiile - operator conectate la platformă, care utilizează servicii NET-DD.

Organizația-operator, prin RPD, are obligația:

- asigurării implementării procedurilor de securitate a prelucrării datelor la nivelul operatorilor săi autorizați (capitolul 1.3.);
- asigurării condițiilor de securitate generale la nivelul organizației privind accesul la sistemele de prelucrare de date;
- verificării specificațiilor tehnice ale sistemelor și serviciilor informatice și de telecomunicații achiziționate pentru prelucrarea computerizată de date;
- asigurării sistemelor de back-up interne:
 - energetic (echipamente UPS, generatoare electrice);
 - de telecomunicații (redundanța serviciilor de telecomunicații);
 - periferice IT&C (disponibilitatea permanentă de echipamente periferice de rezervă).

Împuternicitul trebuie să asigure:

- confidențialitatea activităților sale realizate în beneficiul organizației - operator de date;
- utilizarea de sisteme informatice și de telecomunicații conforme specificațiilor din capitolele următoare:
 - informarea organizației - operator de date asupra obligațiilor sale descrise în paragraful anterior.

2.1.1. Securitatea informatică

Securitatea informatică reprezintă ansamblul caracteristicilor prin care datele și informațiile sunt prelucrate computerizat:

- continuu;
- fără riscuri de:
 - afectare a calității;
 - afectare a volumului;
 - afectare a disponibilității:
 - pentru operatori;
 - pentru beneficiarii prelucrării;
 - afectare a drepturilor patrimoniale;
 - afectare a confidențialității:
 - datelor;
 - prelucrării datelor;
 - rezultatelor prelucrării datelor.

Caracteristicile securității informatice se aplică egal tuturor prelucrărilor computerizate de date, inclusiv a celor personale, cu următoarea precizare:

- datele personale sunt proprietatea exclusivă a posesorului acestora;
- în cazul unor prelucrări de date complexe, care conțin și date personale, puse la dispoziția expresă a organizației - operator sau persoanei operator de către posesorul de date (prin consimțământ sau contract):
 - datele personale sunt și rămân proprietatea posesorului acestora;
 - ansamblul datelor prelucrate, precum și rezultatele prelucrărilor de date, sunt și rămân proprietatea organizației - operator sau persoanei - operator.

În consecință:

- beneficiarul asigurării securității informatice este:
 - direct – organizația - operator sau persoana - operator de date;
 - indirect - posesorul de date personale prelucrate;
- responsabili de asigurarea securității informatice sunt:
 - organizația - operator sau persoana - operator de date;
 - furnizorii de servicii IT&C utilizați de către aceștia;
 - împuterniciții pentru prelucrarea de date cu caracter personal;
 - posesorul datelor personale, atunci când are acces la sistemele informatice care îi prelucrează computerizat datele.

RESPONSABILITATEA PENTRU:

- **UTILIZAREA TUTUROR MECANISMELOR TEHNOLOGICE;**
- **PUNEREA LA DISPOZIȚIE A INSTRUCȚIUNILOR DE OPERARE AFERENTE ASIGURĂRII SECURITĂȚII INFORMATICE**

REVINE FURNIZORULUI DE SERVICII IT&C PENTRU PRELUCRAREA COMPUTERIZATĂ INFORMAȚIONALĂ.

2.1.1.1. Tehnologia securității informatice

Securitatea informatică se asigură, tehnologic, la nivelul tuturor componentelor unui sistem informatic operațional:

- echipamentele periferice ale sistemului;
- sistemele de transfer de date;
- unitatea centrală a sistemului.

Există, în prezent, două clase importante de sisteme informatice:

- sisteme închise;
- sisteme deschise.

Asigurarea securității informatice a sistemelor închise este mult mai costisitoare decât a celor deschise, atunci când este vorba despre management informațional, complex (volum mari de date, mulți operatori, mulți beneficiari ai prelucrărilor computerizate).

Riscurile de securitate informatică sunt egale în cazul celor două clase de sisteme, cu excepția unui singur tip de risc: **riscul de securitate a accesului la date.**

Riscul de securitate a accesului la date crește proporțional cu gradul de deschidere a unui sistem informatic:

- gradul 1 - utilizarea de rețele intranet;
- gradul 2 - conectare la internet;
- gradul 3 - operarea de sisteme în rețele virtuale:
 - Software as a Service;
 - Platform as a Service;
 - CLOUD;
- gradul 4 - operare de sisteme prin portaluri de acces internet.

În concluzie, securitatea informatică este obținută prin tehnologii care adresează:

- funcționarea permanentă a sistemelor informatice, asigurând:
 - disponibilitatea datelor;
 - operaționalitatea sistemelor de prelucrare a datelor;
- securitatea datelor;
- securitatea accesului la date;

2.1.1.1.a. Funcționarea sistemelor informatice

Securitatea informatică presupune ca sistemele informatice utilizate în prelucrarea datelor să fie astfel concepute și operate încât:

- să poată funcționa FĂRĂ ÎNTRERUPERE (fiabilitate și continuitate);
- să fie accesibile operatorilor și beneficiarilor prelucrărilor de date în orice moment (disponibilitate);
- să fie supuse unui mecanism eficient de mentenanță și control.

Asigurarea ansamblului condițiilor de funcționare optimală a sistemelor informatice permite CERTIFICAREA ACESTORA.

Din punctul de vedere al sistemelor actuale de management informațional computerizat, măsurile pentru asigurarea funcționării optime sunt adresate:

- centrului de date:
 - securitatea fizică:
 - protecția accesului;
 - reglementarea procedurilor de mentenanță a echipamentelor hardware (HW);
 - protecția antiseismică;
 - protecția electromagnetică;
 - securitatea energetică:
 - sisteme de back-up:
 - UPS;
 - generator electric;

- conectarea la cel puțin două rețele de transport de electricitate distincte;
 - utilizarea unui sistem eficient de back-up failure (preluarea întregii funcții a centrului de date de către un centru de date secundar "în oglindă", în situația critică a încetării accidentale a funcționării centrului de date principal);
 - asigurarea unei capacități de procesare eficientă, proporțională cu sistemele informatice operate în centrul de date - asigură disponibilitatea datelor prelucrate în condiții de eficiență pentru operator;
- conexiunilor de telecomunicații convergente ale centrelor de date:
 - disponibilitatea:
 - asigurarea redundanței serviciilor de telecomunicații:
 - cel puțin doi furnizori de servicii diferiți;
 - cel puțin două sisteme de telecomunicații (exemplu: fibră optică și radio);
 - asigurarea unei benzi suficiente raportat la numărul de conexiuni simultane pe unitatea de timp;
 - securitatea conexiunilor:
 - sistemele de firewall ale centrului de date;
 - utilizarea de rețele virtuale protejate;
 - utilizarea de sisteme de criptare a transferurilor de date;
- conexiunilor de telecomunicații convergente ale operatorilor:
 - utilizarea de servicii telecom redundante;
 - utilizarea de sisteme de criptare a transferurilor de date;
 - utilizarea de rețele virtuale protejate;
- echipamentelor periferice ale operatorilor:
 - utilizarea de echipamente periferice conform unui standard de calitate minimal recomandat;
 - asigurarea mentenanței echipamentelor periferice;
 - limitarea expunerii echipamentelor la riscuri on-line prin limitarea utilizării aplicațiilor internet fără legătură strictă cu activitatea organizației-operator;
 - utilizarea de sisteme de back-up locale (aplicații cu operare off-line care dublează sistemele informatice operate on-line).

Standardul prezentat de asigurare a funcționării sistemelor informatice în condiții de securitate este utilizat de către Platforma NET-DD și recomandat operatorilor de sisteme computerizate pentru management informațional, indiferent de tipul soluțiilor informatice selectate pentru propria activitate asigură, totodată, toate cerințele GDPR.

2.1.1.1.b. Securitatea datelor

Securitatea propriu-zisă a datelor, indiferent de sistemele informatice utilizate pentru prelucrarea acestora, este asigurată prin:

- implementarea standardului de funcționare a sistemelor informatice (2.1.1.1.a.);
- implementarea unui sistem de back-up periodic al datelor, pe suport hard, care asigură:
 - limitarea pierderilor de date în situații critice;
 - restaurarea rapidă a funcționării sistemelor informatice după rezolvarea situațiilor critice.

Platforma NET-DD utilizează un mecanism de back-up al datelor automat, cu periodicitate de 24 de ore.

Securitatea datelor poate fi completată cu:

- proceduri de copiere periodică suplimentare back-up-ului automat;
- proceduri de copiere pe suporturi analogice.

Aceste măsuri sunt considerate, însă, excesive și foarte costisitoare, copiile analogice anulând unele dintre cele mai mari avantaje ale computerizării managementului informațional, mai ales eliminarea consumului de hârtie.

2.1.1.1.c. Securitatea accesului la date

Din punct de vedere tehnologic, al asigurării securității informatice, asigurarea securității accesului la date presupune, în primul rând, protecția împotriva agresiunilor internetului, prin care se urmărește, indiferent în ce scop:

- accesarea ilegală de date;
- afectarea funcționării sistemelor informatice pentru management informațional.

Confidențialitatea datelor este preocuparea prioritară a oricărui operator de sisteme de management informațional și este asigurată prin acest set de măsuri tehnologice de securitate informatică.

Este evident că toate aceste măsuri pot fi anulate prin nerespectarea procedurilor prezentate în capitolul 1, de către organizații, operatori autorizați și beneficiari ai prelucrărilor de date.

Datele personale, atunci când sunt stocate și arhivate, pot fi securizate suplimentar prin **ANONIMIZARE**.

De asemenea, în situația în care operarea datelor personale se poate realiza în format anonimizat, fără a se afecta scopul și eficiența utilizării în acest format, aceasta este recomandabil să se facă.

Sistemele informatice care utilizează anonimizarea ca metodă de protecție a datelor personale trebuie să dispună de un mecanism eficient de anonimizare/dezanonimizare bine procedurat.

2.1.1.1.c.1. Securitatea fizică a accesului la date

La nivelul centrelor de date, securitatea fizică este asigurată conform specificațiilor capitolului 2.1.1.1.a.

La nivelul organizațiilor - operator de date, securitatea fizică a accesului la date presupune, pe lângă respectarea procedurilor de la capitolul 1:

- securizarea fizică (prin limitarea și auditarea accesului) a tuturor conexiunilor de telecomunicații:
 - internet;
 - intranet;
- securizarea echipamentelor periferice;
- blocarea porturilor de transfer de date, cu excepția conexiunilor de telecomunicații ale echipamentelor periferice (USB, CD-ROM, porturi de memorie externă).

În esență, organizațiile - operator trebuie să limiteze posibilitatea operatorilor sau persoanelor neautorizate de orice fel, de a copia sau transmite date din echipamentele periferice, prin orice metodă.

2.1.1.1.c.2. Securitatea fluxurilor informaționale

Fluxurile informaționale reprezintă totalitatea transferurilor de date și informații realizate în cadrul managementului informațional (care include toate prelucrările de date, inclusiv cele personale):

- în cadrul organizației - operator;
- între organizația - operator și terți.

Din punct de vedere tehnologic, fluxurile informaționale asigură:

- funcționarea optimală a sistemelor informatice utilizate de către organizația-operator și operatorii autorizați ai acesteia - fluxurile din cadrul sistemelor interne de prelucrare a datelor;
- interconectarea organizației - operator cu terțe părți:
 - alte organizații;
 - persoane fizice ale căror date sunt prelucrate de către organizația-operator;
 - publicul larg - prin site-uri internet.

Securitatea informatică este realizată tehnologic prin **securizarea maximă a TRANSFERURILOR INFORMAȚIONALE** implicate de ansamblul fluxurilor informaționale specifice fiecărei organizații - operator de date.

Fluxurile informaționale sunt evaluate, sub aspectul securității informatice, funcție de:

- originea datelor;
- sistemele interne de prelucrare a datelor;
- destinatarul datelor.

Originea datelor este important să fie cunoscută. Orice descărcare de fișiere de la destinatari necunoscuți constituie un risc major de securitate pentru orice sistem informatic.

Tehnologic, centrele de date controlează originea solicitărilor de conectare:

- prin sisteme antivirus;
- prin echipe de monitorizare cu operare permanentă.

Operatorii autorizați, însă, trebuie să respecte procedurile capitolului 2 pentru a nu expune inutil riscurilor de agresiune informatică sistemele pe care le utilizează:

ORICE MESAJ CU ORIGINE NECUNOSCUTĂ TREBUIE BLOCAT!

Destinatarul datelor TREBUIE:

- să fie CUNOSCUT;
- să aibă dreptul legal și procedural de a primi datele transmise, în formate reglementate.

NU este recomandată transmiterea de date personale prin e-mail, la adrese personale, ci EXCLUSIV prin sisteme de comunicații protejate.

Excepția de la această regulă trebuie să fie **CEREREA EXPRESĂ A POSESORULUI DE DATE**, după informarea acestuia asupra riscurilor la care se expune.

Platforma NET-DD utilizează pentru asigurarea optimală a securității fluxurilor informaționale:

- securitatea informatică a sistemelor informatice proprii;
- criptarea virtuală a tuturor transferurilor informaționale între operatorii autorizați;
- sisteme de rețele virtuale protejate care interconectează operatorii autorizați cu mecanismele proprii de criptare;
- sistemul propriu de mesagerie internă pentru operatorii autorizați;
- PORTALUL NET-DD -unicul sistem de comunicare prin internet cu persoane fizice: identificate prin:
 - cont,
 - parolă,
 - PIN,
 - card NET-DD.

În funcție de tipul datelor prelucrate și de gradul de risc al prelucrărilor de date se implementează măsuri de securitate informatică proporționale, clasificate în **NIVELURI DE SECURITATE INFORMATICĂ**.

Platforma NET-DD are un standard unic de securitate informatică pentru toate componentele sale, cu excepția securității fluxurilor informaționale externe, pentru care se aplică 4 niveluri de securitate progresive.

Cu cât nivelul de securitate necesar este mai ridicat, cu atât costurile induse organizațiilor - operator sunt mai mari, de aceea este recomandată o analiză corectă pentru a determina ce nivel de securitate este necesar și suficient, pentru fiecare situație în parte.

De exemplu: datele medicale anonimizate necesită un nivel scăzut de protecție (1), pe când datele medicale identificabile prezintă riscul maxim de protecție (4), egal cu cel al datelor bancare.

2.2. Mecanisme de auditare automatizate a operării aplicațiilor IT&C

Mecanismele de auditare automatizate a operării aplicațiilor IT&C utilizate în managementul informațional, care include prelucrarea computerizată de date personale este maximum eficientă și sigură.

Totuși, organizații - operator de date personale pot lucra ne-informatizat, situație în care toate aspectele auditării automatizate trebuie aplicate, prin metode analogice, de către RPD. O modalitate de a optimiza această activitate umană este implementarea, ca soluție minimală de informatizare, a unui registru electronic de evidență a prelucrării datelor personale, din care să se poată genera automatizat un set de rapoarte de audit precise.

Sistemele informatice utilizate în prelucrarea computerizată a datelor personale este recomandat să fie prevăzute cu un set minimal de sisteme de auditare automatizată, care să aibă o funcționare standard periodică, la care să se adauge posibilitatea de a genera în orice moment, rapoarte de audit în timp real. Un model operațional în acest sens este Platforma NET-DD.

2.2.1. Auditarea generală a operării de date personale

Sistemul pentru auditarea generală automatizată a operării de date personale, respectând prevederilor GDPR, trebuie să pună la dispoziția RPD și a managementului organizației - operator, precum și a persoanei ale cărei date sunt prelucrate, la cererea acesteia și a organizațiilor cu drept legal de certificare, monitorizare și control, a cel puțin următoarele date:

- în istoric pentru o durată precizată (de la data de – la data de);
- actualizate la zi:
 1. auditarea accesului la date:
 - a. istoricul complet de logare a operatorilor autorizați;
 - b. istoricul tentativelor de acces neautorizat;
 2. auditarea prelucrărilor de date personale:
 - a. raport de auditare a activității operatorilor autorizați:
 - i. per organizație - operator;
 - ii. per operator autorizat; raport de auditare a prelucrării datelor persoanei:
 - b. istoricul prelucrărilor; ultima prelucrare;
 3. auditarea calității datelor personale prelucrate:
 - a. raportul complet al datelor prelucrate la zi;
 - b. raport asupra datelor personale incomplete - per persoană;
 4. auditarea cantitativă a datelor personale prelucrate:
 - a. date;
 - b. fișiere;
 - c. arhive;

Sistemele de auditare a operării datelor personale trebuie să poată fi optimizate conform:

- specificațiilor organizațiilor - operator;
- modificărilor legislative de reglementare în materie.

2.2.2. Auditarea generală a securității informatice a organizației - operator

Auditarea generală a securității informatice a organizației - operator, fie că operează datele direct sau prin intermediari, este o prioritate a RPD.

Auditarea securității informatice trebuie să cuprindă evaluarea:

1. acțiunilor neautorizate ale operatorilor, care pot crea riscuri de securitate (capitolul 2.1.);
2. auditarea accesului operatorului autorizat:
 - a. istoricul autentificărilor:
 - i. la nivel de oră - minut al autentificării;
 - ii. durata autentificării;
 - iii. locația autentificării:
 1. din sediul organizației;
 2. la distanță;
 - b. raportat la persoană:
 - i. istoricul înregistrărilor de date;
 - ii. istoricul editărilor de date;
 - c. auditarea istoricului alocărilor de drepturi de acces per operator;
 - d. raportarea automatizată a istoricului tentativelor de acces neautorizat.

Auditarea incidentelor de securitate trebuie să asigure:

- identificarea incidentului de securitate asociată ALERTĂRII IMEDIATE:
 - a RPD;
 - a operatorilor;
- generarea automatizată a notificărilor de incident de securitate;
- generarea de rapoarte privind istoricul și natura incidentelor de securitate.

Sistemele de auditare a securității informatice trebuie să poată fi optimizate conform:

- specificațiilor organizațiilor-operator;
- modificărilor legislative de reglementare în materie.

2.2.3. Auditarea respectării prevederilor GDPR

Sistemul pentru auditarea automatizată a respectării prevederilor GDPR trebuie să pună la dispoziția RPD și a managementului organizației - operator, precum și a persoanei ale cărei date sunt prelucrate, la cererea acesteia, a cel puțin următoarelor date:

- în istoric pentru o durată precizată (de la data de – la data de);
- actualizate la zi:
 - Informarea persoanei:
 - conținutul informării;
 - emiterea informării;
 - confirmarea informării de către persoană;
 - Consimțământul informat al persoanei:
 - semnarea (fizică sau electronică) a consimțământului;
 - arhivarea adecvată a consimțământului;
 - Solicitățile persoanei privind prelucrarea datelor personale:
 - restricționare a prelucrării;
 - retragerea consimțământului;
 - ștergerea completă a datelor personale - atunci când este posibil legal;
 - comunicarea de date personale:
 - fizică;
 - prin PORTALUL NET-DD;
 - prin internet;

2.3. Mecanismul automatizat pentru asigurarea respectării drepturilor persoanei privind prelucrarea datelor personale

Mecanismul automatizat pentru asigurarea respectării drepturilor persoanei privind prelucrarea datelor personale TREBUIE să asigure COMUNICAREA BI-DIREȚIONALĂ ON-LINE dintre persoană și organizația - operator de date, respectiv operatorii autorizați ai acesteia.

Acest mecanism asigură:

- informare în timp real a persoanei asupra:
 - condițiilor de prelucrare a datelor și modificărilor acestora;
 - incidentelor de securitate și măsurilor aferente acestora;
 - altor situații specifice;
- primirea, din partea persoanei, de solicitări și informații relevante pentru prelucrarea datelor personale.

Mecanismul on-line de comunicare dintre persoană și operatorul de date poate fi:

- elementar - prin utilizarea:
 - site-ului operatorului de date;
 - mesageriilor comerciale;
- optimizată: PORTALUL NET-DD.

PORTALUL NET-DD asigură comunicarea bi-direcțională, în timp real, între persoană și operatorii de date utilizatori ai Platformei NET-DD:

- securizată;
- structurată;
- stabilă;
- auditabilă;
- multilingvă.

3. LEGISLAȚIE PRIVIND PRELUCRAREA COMPUTERIZATĂ A DATELOR CU CARACTER PERSONAL

3.1. Prevederi contractuale exprese pentru respectarea GDPR

Organizația - operator de date personale poate asigura prelucrarea respectivelor date:

- direct, utilizând:
 - propriul personal;
 - propriile sisteme informatice;
- prin împuterniciți, utilizând:
 - metode analogice;
 - metode computerizate.

În situația prelucrării directe prin sisteme informatice, dar și prin împuterniciți, utilizând sisteme informatice operate de către aceștia, prevederile contractuale trebuie să asigure, dar nu exclusiv, respectarea tuturor specificațiilor tehnice descrise în capitolul 2.

În toate situațiile, organizația - operator trebuie să contractualizeze personalul propriu și al împuterniciților, astfel încât să se respecte, dar nu exclusiv, toate specificațiile capitolului 1.

În situația prelucrării computerizate a datelor prin împuterniciți, contractele semnate de către organizația - operator cu aceștia trebuie să prevadă, dar nu exclusiv, următoarele clauze:

- 1. Calitatea de împuternicit** a organizației în cauză, în conformitate cu Regulamentul (UE) 2016/679 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date (denumit în continuare "GDPR"), ca și orice legislație națională subsecventă cu privire la domeniul protecției datelor cu caracter personal;
- 2. Obiectul exact al contractului:**
 - a. scopul/scopurile prelucrării datelor;
 - b. categoriile de persoane vizate de prelucrarea datelor, pentru fiecare scop în parte;
 - c. inventarul exact al datelor prelucrate pentru fiecare scop în parte;
- 3. Natura contractului** - precizarea serviciilor computerizate și/sau analogice contractate, conform descrierii tehnice și comerciale a acestora;

4. **Lista sub-împuterniciților**, atunci când aceștia există și descrierea activităților realizate de către aceștia în cadrul contractului, răspunderea pentru acestea revenind integral împuternicitului;

Celelalte clauze necesar a fi cuprinse în contractul organizației - operator pot fi adaptate conform modelului de contract standard utilizat de către NET-DD ADMIN:

5. Drepturile și obligațiile părților:

5.1. Drepturile și obligațiile Operatorului

- Dreptul să primească informații de la împuternicit sau să verifice prin auditor mandatat dacă împuternicitul are și pune în aplicare măsuri tehnice și organizatorice adecvate, astfel încât prelucrarea să respecte cerințele prevăzute de GDPR; verificarea va avea loc în baza unei notificări scrise prealabile, transmisă cu cel puțin 14 zile lucrătoare înainte de efectuarea verificării;
- Dreptul să primească asistență din partea împuternicitului, în special pentru îndeplinirea obligației sale de a răspunde cererilor persoanelor vizate cu privire la exercitarea drepturilor lor prevăzute de GDPR;
- Dreptul de a face obiecțiuni cu privire la alți sub-împuterniciți;
- Să respecte obligațiile sale conform GDPR în calitate de operator cu privire la datele cu caracter personal colectate sau prelucrate de împuternicit, pe seama sa;
- Obligația de a face informarea persoanelor vizate conform GDPR, inclusiv în ceea ce privește informarea cu privire la prelucrarea datelor de către împuternicit în temeiul acestui contract;
- Obligația să răspundă exclusiv de stabilirea temeiului legal pentru prelucrarea datelor cu caracter personal ce face obiectul prezentului contract;
- Obligația de a implementa măsuri tehnice și organizatorice adecvate conform GDPR, inclusiv securizarea transferului datelor de la persoanele vizate către Împuternicit;
- Operatorul înțelege că din momentul ștergerii datelor după încheierea prestării serviciilor de către Împuternicit conform obligațiilor GDPR, datele nu mai pot fi recuperate și este întreaga responsabilitate a Operatorului să se asigure că și-a făcut o copie completă a acestora.
- În toate situațiile în care operatorul este cel care trebuie să execute o obligație, cum este, spre exemplu, informarea persoanei vizate cu privire la încălcarea securității datelor cu caracter personal, împuternicitul nu poate fi ținut de inacțiunile operatorului din sfera acelei obligații.

5.2. Drepturile și obligațiile împuternicitului:

- Obligația să informeze operatorul în termen de maxim 10 zile, în cazul în care, în opinia împuternicitului, o instrucțiune încalcă GDPR și/sau altă dispoziție legală privind prelucrarea datelor cu caracter personal;

- Obligația să asigure securitatea datelor cu caracter personal prelucrate în numele operatorului în conformitate cu art 32 din GDPR;
- Obligația de a informa operatorul fără întârzieri nejustificate de o încălcare a securității datelor personale ale operatorului pe parcursul prelucrării realizate de către împuternicit;
- Obligația de a asista operatorul cu toate informațiile necesare în vederea notificării, dacă este cazul, către autoritatea competentă pentru încălcarea securității datelor, dar fără a se substitui operatorului în obligația sa de notificare;
- Obligația de a acorda asistență operatorului să asigure respectarea obligațiilor prevăzute la articolele 32-36 din GDPR;
- Obligația de a asista operatorul pentru soluționarea cererilor persoanelor vizate sau de a transmite operatorului orice cerere primită de la persoanele vizate, în legătură cu datele personale care au fost colectate și prelucrate de împuternicit, în termen de maxim 5 zile calendaristice de la primirea acestora. Această asistență nu se aplică în situația în care operatorul are deja în instrumentele tehnice furnizate de către împuternicit posibilitatea de a soluționa direct cererea persoanei vizate (de ex. dreptul la acces – unde operatorul are deja toate informațiile cu privire la ce date colectează);
- Obligația să nu transmită date cu caracter personal și/sau informații confidențiale, ce pot fi date cu caracter personal, despre care a luat cunoștință în timpul executării contractului;
- Obligația să asigure instruirea personalului autorizat să prelucreze datele cu caracter personal, cu privire la confidențialitatea acestor date;
- Obligația să includă obligații de confidențialitate către angajați și sub-împuterniciți;
- Dreptul să dezvăluie anumite date cu caracter personal în virtutea unei obligații legale sau a unei alte condiții prevăzute de legislație la solicitarea unei autorități, instituții publice sau instanțe judecătorești.
- Dreptul de a recruta sub-împuterniciți;
- Dreptul la acoperirea costurilor generate de asigurarea asistenței operatorului în situațiile prevăzute de GDPR, dacă acestea depășesc costul serviciilor prestate de către împuternicit.
- Dreptul de a folosi informații statistice anonimizate ca urmare a activităților prestate ca urmare a acestui contract sau a întregii sale activități.
- Obligația de a șterge toate datele colectate ca urmare a acestui contract în calitate de împuternicit în termen de maxim 6 luni de la încetarea contractului dintre cele două părți.
- Împuternicitul nu poate stabili scopuri sau mijloace de prelucrare a datelor cu caracter personal, acestea fiind stabilite exclusiv de către operator.

6. Clauze privind securitatea prelucrării

- Împuternicitul trebuie să îndeplinească măsuri tehnice și organizatorice adecvate pentru a asigura măsurile adecvate de securitate raportate la risc, conforme cu bunele practici în industrie. În stabilirea nivelului adecvat de securitate, împuternicitul trebuie să ia în considerare stadiul actual al dezvoltării, costurile implementării și natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și riscul cu diferite grade de probabilitate și gravitate pentru drepturile și libertățile persoanelor fizice, ca și riscurile care apar ca urmare a prelucrării, în special cu privire la cele care pot 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.

- În acest context împuternicitul a stabilit aplicarea internă a următoarelor măsuri organizatorice și tehnice de securitate pentru securitatea datelor personale, luând în considerare tipul de activitate prestată:
 - implementare standarde de securitate ISO27001/ISO27017/ISO27018;
 - audit periodic de securitate realizat de experți în securitate cibernetică ;
 - acces limitat la baza de date pentru un număr foarte restrâns de angajați ai împuternicitului;
 - monitorizarea permanentă a accesului la baza de date;
 - criptarea conexiunii folosite de operator pentru accesarea serviciului folosind SSL ;
 - parolele clienților stocate criptat ;
 - copii de siguranță regulate;

- În mod voluntar, împuternicitul poate trimite rezumatele concluziilor auditorilor de securitate (după ștergerea informațiilor comerciale sau confidențiale) realizate periodic către operatori pentru a demonstra activitățile sale continue pe acest subiect.

7. Limitarea răspunderii

Operatorul este de acord să exoneraze împuternicitul de orice răspundere pentru pagubele ce ar putea decurge din:

- nerespectarea contractului din cauza unor evenimente ce exced oricărei răspunderi a împuternicitului;
- respectarea instrucțiunilor operatorului sau nerespectarea instrucțiunilor operatorului justificată în prealabil printr-o notificare referitoare la nelegalitatea ei;
- lipsa sau vicierea acordului persoanelor vizate sau a utilizării unui temei legal greșit de către Operator;
- nerespectarea contractului din cauza unor acțiuni ale Operatorului.

8. Delimitarea răspunderii

Operatorul și împuternicitul își delimitează responsabilitățile cu privire la asigurarea protecției datelor cu caracter personal (de exemplu asigurarea confidențialității sau a securității prelucrării), în funcție de accesul și controlul efectiv exercitat asupra datelor, atât din punct de vedere contractual, cât și tehnic

3.2. Reglementări legislative române

- Convenția pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal din 28.01.1981 - Act Internațional
- Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice - Parlamentul României
- Legea nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date - Parlamentul României
- Legea nr. 238/2009 privind reglementarea prelucrării datelor cu caracter personal de către structurile/unitățile Ministerului Administrației și Internelor în activitățile de prevenire, cercetare și combatere a infracțiunilor, precum și de menținere și asigurare a ordinii publice - Parlamentul României
- Codul Civil din 2009 - Parlamentul României
- Legea nr. 272/2006 pentru completarea art. 7 din Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice - Parlamentul României
- Legea nr. 235/2015 pentru modificarea și completarea Legii nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice - Parlamentul României
- Legea nr. 682/2001 privind ratificarea Convenției pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal, adoptată la Strasbourg la 28 ianuarie 1981 - Parlamentul României
- Decizia nr. 200/2015 privind stabilirea cazurilor de prelucrare a datelor cu caracter personal pentru care nu este necesară notificarea, precum și pentru modificarea și abrogarea unor decizii - Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal - ANSPDCP
- Hotărârea nr. 57/2017 referitoare la propunerea de Regulament al Parlamentului European și al Consiliului privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către instituțiile, organele, oficiile și agențiile Uniunii și privind libera circulație a acestor date și de abrogare a Regulamentului (CE) nr. 45/2001 și a Deciziei nr. 1.247/2002/CE - COM (2017) 8 final - Senatul României
- Hotărârea nr. 106/2016 referitoare la Comunicarea Comisiei către Parlamentul European în conformitate cu art. 294 alin. (6) din Tratatul privind funcționarea Uniunii Europene privind poziția Consiliului în ceea ce privește adoptarea unei directive a Parlamentului European și a Consiliului privind protecția persoanelor

fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, identificării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor și la libera circulație a acestor date și de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului COM (2016) 213 final - Senatul României

- Hotărârea nr. 107/2016 referitoare la Comunicarea Comisiei către Parlamentul European în conformitate cu art. 294 alin. (6) din Tratatul privind funcționarea Uniunii Europene privind poziția Consiliului în ceea ce privește adoptarea unui regulament al Parlamentului European și al Consiliului privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal și libera circulație a acestor date (Regulament general privind protecția datelor) și de abrogare a Directivei 95/46/CE COM (2016) 214 final - Senatul României
- Legea nr. 55/2005 pentru ratificarea Protocolului adițional la Convenția pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal, cu privire la autoritățile de control și fluxul transfrontalier al datelor, adoptat la Strasbourg la 18 noiembrie 2001 - Parlamentul României
- Legea nr. 95/2006 privind reforma în domeniul sănătății - Parlamentul României
- Legea nr. 76/2008 privind organizarea și funcționarea Sistemului Național de Date Genetice Judiciare - Parlamentul României

3.3. Reglementări legislative europene

- Regulamentul nr. 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) (Text cu relevanță pentru SEE) - (General Data Protection Regulation - GDPR) - Parlamentul European și Consiliul Uniunii Europene
- Directiva nr. 46/1995 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date - Parlamentul European și Consiliul Uniunii Europene
- Directiva nr. 58/2002 privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice (Directiva asupra confidențialității și comunicațiilor electronice) - Parlamentul European și Consiliul Uniunii Europene
- Regulamentul nr. 45/2001 privind protecția persoanelor fizice cu privire la prelucrarea datelor cu caracter personal de către instituțiile și organele comunitare și privind libera circulație a acestor date - Parlamentul European și Consiliul Uniunii Europene
- Decizia nr. 484/2012 de punere în aplicare privind nivelul de protecție adecvat asigurat de Republica Orientală a Uruguayului privind prelucrarea automată a datelor cu caracter personal [notificată cu numărul C(2012) 5704] (Text cu relevanță pentru SEE) - Comisia Europeană
- Directiva nr. 680/2016 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în

scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor și privind libera circulație a acestor date și de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului - Parlamentul European și Consiliul Uniunii Europene

- Rectificare la Directiva 2009/136/CE a Parlamentului European și a Consiliului din 25 noiembrie 2009 de modificare a Directivei 2002/22/CE privind serviciul universal și drepturile utilizatorilor cu privire la rețelele și serviciile de comunicații electronice, a Directivei 2002/58/CE privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice și a Regulamentului (CE) nr. 2006/2004 privind cooperarea dintre autoritățile naționale însărcinate să asigure aplicarea legislației în materie de protecție a consumatorului (Jurnalul Oficial al Uniunii Europene L 337 din 18 decembrie 2009) - Jurnalul Oficial al Uniunii Europene
- Decizia nr. 61/2011 în temeiul Directivei 95/46/CE a Parlamentului European și a Consiliului privind nivelul de protecție adecvat asigurat de Statul Israel privind prelucrarea automată a datelor cu caracter personal [notificată cu numărul C(2011) 332] (Text cu relevanță pentru SEE) - Comisia Comunităților Europene
- Decizia nr. 146/2010 în temeiul Directivei 95/46/CE a Parlamentului European și a Consiliului privind nivelul de protecție adecvat asigurat de Legea feroeză privind prelucrarea datelor cu caracter personal [notificată cu numărul C(2010) 1130] (Text cu relevanță pentru SEE) - Comisia Comunităților Europene
- Directiva nr. 136/2009 de modificare a Directivei 2002/22/CE privind serviciul universal și drepturile utilizatorilor cu privire la rețelele și serviciile de comunicații electronice, a Directivei 2002/58/CE privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice și a Regulamentului (CE) nr. 2006/2004 privind cooperarea dintre autoritățile naționale însărcinate să asigure aplicarea legislației în materie de protecție a consumatorului (Text cu relevanță pentru SEE) - Parlamentul European și Consiliul Uniunii Europene
- Decizia nr. 597/2008 de adoptare a dispozițiilor de punere în aplicare privind responsabilul cu protecția datelor în temeiul articolului 24 alineatul (8) din Regulamentul (CE) nr. 45/2001 privind protecția persoanelor fizice cu privire la prelucrarea datelor cu caracter personal de către instituțiile și organele comunitare și privind libera circulație a acestor date - Comisia Comunităților Europene
- Regulamentul nr. 1024/2012 privind cooperarea administrativă prin intermediul Sistemului de informare al pieței interne și de abrogare a Deciziei 2008/49/CE a Comisiei ("Regulamentul IMI") (Text cu relevanță pentru SEE) - Parlamentul European și Consiliul Uniunii Europene

4. LEGISLAȚIA PRIVIND CARDUL ELECTRONIC PERSONAL MULTIFUNCȚIONAL e-ID PERSONAL CARD - CARDUL PROFESIONAL EUROPEAN

4.1. Reglementări ale instituțiilor Uniunii Europene

- Directiva nr. 36/2005 privind recunoașterea calificărilor profesionale - Parlamentul European și Consiliul Uniunii Europene
- Regulamentul de punere în aplicare nr. 983/2015 privind procedura de eliberare a cardului profesional european și aplicarea mecanismului de alertă în temeiul Directivei 2005/36/CE a Parlamentului European și a Consiliului (Text cu relevanță pentru SEE) - Comisia Europeană
- Regulamentul nr. 1024/2012 privind cooperarea administrativă prin intermediul Sistemului de informare al pieței interne și de abrogare a Deciziei 2008/49/CE a Comisiei ("Regulamentul IMI") (Text cu relevanță pentru SEE) - Parlamentul European și Consiliul Uniunii Europene
- Directiva nr. 55/2013 de modificare a Directivei 2005/36/CE privind recunoașterea calificărilor profesionale și a Regulamentului (UE) nr. 1024/2012 privind cooperarea administrativă prin intermediul Sistemului de informare al pieței interne (Regulamentul IMI) (Text cu relevanță pentru SEE) - Parlamentul European și Consiliul Uniunii Europene

4.2. Reglementări legislative române

- Legea nr. 200/2004 privind recunoașterea diplomelor și calificărilor profesionale pentru profesiile reglementate din România - Parlamentul României
- Legea nr. 160/1998 pentru organizarea și exercitarea profesiei de medic veterinar - Parlamentul României
- Ordonanța de urgență nr. 70/2017 privind modificarea și completarea Legii nr. 160/1998 pentru organizarea și exercitarea profesiei de medic veterinar - Guvernul României
- Statutul medicului veterinar din 25.10.2016 - Colegiul Medicilor Veterinari - CMV
- Legea nr. 95/2006 privind reforma în domeniul sănătății - Parlamentul României
- Legea nr. 48/2017 privind aprobarea Ordonanței de urgență a Guvernului nr. 45/2016 pentru modificarea și completarea Legii nr. 95/2006 privind reforma în domeniul sănătății - Parlamentul României
- Ordonanța de urgență nr. 109/2007 pentru modificarea și completarea Legii nr. 200/2004 privind recunoașterea diplomelor și calificărilor profesionale pentru profesiile reglementate din România - Guvernul României
- Hotărârea Guvernului nr. 1.071/2013 privind aprobarea Strategiei Naționale pentru Ocuparea Forței de Muncă 2014-2020 și a Planului de acțiuni pe perioada 2014-2020 pentru implementarea Strategiei naționale din 11.12.2013 - Guvernul României

5. Deficiențele prevederilor GDPR

GDPR este un regulament necesar pentru crearea unui cadru normativ care să:

- stabilească drepturile persoanei privitor la prelucrarea, analogică sau computerizată, a datelor care îi aparțin;
- limiteze posibilitățile de utilizare excesivă a datelor personale de către operatorii acestora;
- asigure un mecanism eficient de control al operării datelor personale.

Pe de altă parte, însă, GDPR este, așa cum spune și denumirea, un **REGULAMENT GENERAL**, astfel, modalitatea precisă de reglementare a situațiilor particulare nu este stabilită prin acesta.

Lipsa reglementărilor privind operarea datelor personale în toate situațiile speciale/specifice este principala **DEFICIENTĂ** a GDPR, nerezolvarea imediată a acesteia constituind o situație de risc:

- pentru organizațiile - operator;
- pentru operatorii autorizați ai organizațiilor-operator;
- pentru administrația care asigură controlul și / sau coordonarea activităților organizațiilor - operator:
 - locală;
 - centrală.

În prezent există legislație specială europeană, prezentată în *capitolul 3*, pentru managementul datelor persoanelor care prezintă risc de securitate socială, precum și pentru alte domenii, cum sunt medicina, finanțele publice, justiția.

O mare parte a acestei legislații este anterioară aplicării GDPR, deci nu este coordonată acestuia.

În aceste condiții, este considerată imperativă inițierea și coordonarea unui demers național și european pentru elaborarea unui cadru normativ precis care să completeze prevederile GDPR, acoperind totalitatea activităților sociale care presupun prelucrarea de date cu caracter personal.

O atenție specială este acordată în acest document problematicii prelucrării datelor medicale și a celor de evidență a populației, date care trebuie tratate cu maximă responsabilitate.

NET-DD ADMIN a inițiat, în acest sens, constituirea unui **GRUP DE LUCRU INTERMINISTERIAL** care să elaboreze cadrul legislativ de aplicare a GDPR în România.

Rezultatele acestui demers vor fi publicate în completarea prezentei documentații, pe măsura obținerii acestora.