PLATFORMA e-Pi

NORME INTERNE DE IMPLEMENTARE A REGULAMENTULUI GENERAL PENTRU PROTECȚIA DATELOR[1] (GDPR)

APLICABIL PENTRU TOȚI OPERATORII PLATFORMEI e-Pi

ȘI A SERVICIILOR e-Pi INTEGRATE PE ACEASTA:

- **e-Pi PLATFORM**
- **e-Pi ORG**
- **e-Pi PROFESSIONAL**
  - **e-Pi SPORT**
- **e-Pi SCIENCE**
  - **e-Pi PUBLISH**
  - **e-Pi TRAINING**
  - **e-Pi LEARNING**
- **e-Pi PROJECT**
- **e-Pi MEDICAL**

[1] **VERSIUNEA NR.1 emisă de către administratorul Platformei e-Pi (e-Pi ADMIN) la data de 25 Mai 2018**

PREAMBUL

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

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

GDPR încurajează prelucrarea computerizată a datelor personale în vederea creşterii eficienţei administrative şi a mobilităţii acestora între statele membre, cu condiţia implementării unui set de proceduri precise a prevederilor acestuia, la nivelul:

- operatorilor de date personale;
- împuterniciţilor operatorilor de date personale;
- autorităţilor naţionale responsabile de protecţia datelor personale.

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

- în toate documentele tehnice şi de prezentare ale Platformei e-Pi şi serviciilor e-Pi, termenul de **OPERATOR** defineşte angajatul unei organizaţii care utilizează aceste sisteme informatice, având pentru aceasta autorizarea expresă a organizaţiei (operator autorizat).
  Pentru evitarea oricărei confuzii, în prezentul document:
  - organizaţia care prelucrează date personale se va denumi ***"organizaţie operator de date personale"***;
  - angajaţii acesteia, care lucrează efectiv cu date personale, utilizând aplicaţii IT&C se vor denumit ***"operatori IT"*** sau ***"operatori IT autorizaţi"***.

e-PI ADMIN, în calitatea sa de administrator al Platformei e-Pi şi a serviciilor e-Pi integrate pe aceasta, dar şi în calitate de operator de date cu caracter personal în cadrul activităţilor sale proprii, îşi asumă responsabilitatea de a pune la dispoziţia tuturor operatorilor cu care are relaţii contractuale a unei proceduri unitare pentru implementarea GDPR şi pentru instruirea permanentă, proactivă, a acestora.

Procedura elaborată de către e-PI ADMIN prevede toate mecanismele necesare **informării persoanelor ale căror date personale sunt prelucrate** prin operatorii Platformei e-Pi şi a serviciilor e-Pi asupra:

- drepturilor garantate prin GDPR;
- metodelor de protejare a datelor personale;
- utilizării sistemelor e-Pi care maximizează eficienţa sistemelor de prelucrare computerizată a datelor personale prin Platforma e-Pi şi prin serviciile e-Pi.

În înţelesul GDPR, datele personale pot fi prelucrate computerizat *(Platforma e-Pi şi serviciile e-Pi prelucrează date personale EXCLUSIV computerizat)*, prin aplicaţii de tipuri foarte variate:

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

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

- în conformitate cu relaţiile reglementate pe care le are cu respectiva persoană;
- informând corect şi complet asupra modului de utilizare a datelor prelucrate;
- cu acordul expres al persoanei (cu excepţia situaţiilor 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 condiţiile în care există o prevedere legală expresă care să autorizeze operatorul de date în acest sens.

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

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

Procedura de implementare a GDPR la nivelul operatorilor de date care utilizează Platforme e-Pi presupune:

- elaborarea unui set de proceduri specifice interne;
- respectarea unui set de specificaţii tehnice şi de operare a aplicaţiilor 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 organizaţiei - operator de date personale implică asigurarea, în structura organizatorică proprie, a FUNCŢIEI DE RESPONSABIL CU PROTECŢIA DATELOR.

În situaţia organizaţiilor mici şi medii e-PI ADMIN recomandă crearea în organigramă a funcţiei de **responsabil cu protecţia datelor**, cu normă de lucru zilnică de maximum 2 (două) ore, inclusiv în zilele libere.

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

- costul excesiv al serviciului;
- **acordarea accesului la sistemele informatice proprii şi la datele procesate prin acestea a unui terţ, ceea ce creşte riscurile de încălcare a confidenţialităţii;**
- dificultatea asigurării permanenţei serviciului de protecţie a datelor, conform GDPR.

Îndeplinirea prevederilor funcţiei de responsabil de protecţia datelor de către oricare angajat al organizaţiei **NU** presupune, conform GDPR:

- **instruirea** acestuia, altfel decât prin instruirea asupra pachetului de proceduri puse la dispoziţie de către e-PI ADMIN, prin prezenta documentaţie;
- **certificarea** acestuia de vreo instituţie a statului sau de vreo organizaţie de certificare, publică sau privată.

Pentru maximum de formalism legal, e-PI ADMIN asigură un **SISTEM DE CERTIFICARE INTERNĂ A INSTRUIRII ADECVATE A RESPONSABILULUI DE PROTECŢIA DATELOR**, pentru toate organizaţiile partenere, utilizatoare ale sistemelor informatice, ale Platformei e-Pi sau altele.

1.1. Funcția de RESPONSABIL CU PROTECȚIA DATELOR în cadrul organizației

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

- implementarea şi asigurarea respectării procedurilor GDPR descrise în prezenta documentaţie:
  - instruirea periodică a angajaţilor care asigură prelucrarea datelor personale:
    - ale angajaţilor şi colaboratorilor organizaţiei;
    - ale beneficiarilor activităţii organizaţiei;
  - informarea persoanelor ale căror date sunt prelucrate de către organizaţie;
  - informarea managementului organizaţiei asupra procedurilor de implementare a GDPR;
- instruirea periodică asupra documentaţiei oficiale privind implementarea GDPR, prin sistemul periodic de instruire al Platformei e-Pi ***(e-Pi GDPR)***.

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

- furnizorii de servicii pentru prelucrarea datelor cu caracter personal - **ÎMPUTERNICIȚII** organizaţiei - operator;
- Autoritatea Naţională 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 securităţii datelor personale;
- încălcarea procedurilor de prelucrare a datelor personale;
- compromiterea securităţii datelor personale;
- compromiterea securităţii şi confidenţialităţii 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 Autorităţii Naţionale de Supraveghere a Prelucrării Datelor Personale, se realizează prin:

- procedura directă:
  - on-line, prin adresa web a autorităţii;
  - prin adresarea telefonică a autorităţii;
- procedura automatizată - notificarea Autorităţii prin Platforme e-Pi de către e-PI ADMIN.

Notificarea ANSPDP se realizează în următoarele situații:

1. demararea oricărei noi prelucrări de date personale de către organizaţia operator -prin procedura directă on-line;
2. solicitarea autorizării exprese pentru prelucrare de date cu caracter personal speciale (sensibile), în condiţiile legislaţiei naţionale în vigoare - procedura directă on-line;
3. identificarea unui risc imediat de compromitere a securităţii datelor personale prelucrate de către organizaţia - operator:
   4.1. la nivelul organizaţiei;
   4.2. la nivelul împuterniciţilor organizaţiei - operator, furnizori de servicii de prelucrare a datelor personale:
   a. procedura automatizată - în cazul serviciilor operate prin Platforma e-Pi:
   b. procedura directă.

Notificarea riscului de compromitere a securității datelor personale

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

Notificarea posesorilor de date trebuie să conţină:

- 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.

Acelaşi set de informaţii trebuie comunicate ANSPDP.

Utilizatorii Platformei e-Pi pot utiliza procedura automatizată pentru ambele tipuri de notificări pentru serviciile acesteia aflate în operare, prin:

- PORTALUL e-Pi şi sistemul de card personal multifuncţional e-Pi CARD;
- prin lansarea în bloc a unui mesaj de notificare către adresele de e-mail ale tuturor posesorilor de date afectaţi.

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 organizaţiei 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 GDRP şi a legislaţiei naţionale în domeniu, oricare organizaţie - operator de date personale trebuie să reglementeze intern următoarele aspecte procedurale:

- proceduri pentru managementul organizaţiei;
- proceduri pentru operatorii de date personale:
  - angajaţi ai organizaţiei;
  - colaboratori externi *(se vor utiliza contracte de colaborare care să conțină prevederile contractule specifice GDPR precizate în Capitolul 2./2.3)*;
- proceduri pentru achiziţia 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 şi prelucrărilor utilizând formate analogice.

1.2.1. Proceduri aplicate de către managementul organizației - operator

Procedurile pentru implementarea GDPR de către managementul organizaţiei - 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. **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 prelucării 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 funcţie de sensibilitatea datelor (care determină nivelul de securitate al prelucrării acestora):
  - date publicabile;
  - date confidenţiale;
  - date sensibile;
  - date protejate;
- în funcţie de posiblităţile de utilizare de către organizaţia - operator:
  - date de uz strict intern - date blocate;
  - date utilizabile între organizaţiile relaţionate:
    - subordonate;
    - supraordonate;
    - terţe organizaţii contractate.

    Datele utilizabile între organizaţii sunt:

    - date partajabile;
    - date transmisibile;
    - date publicabile.
- în funcţie de natura datelor:
  - date de identificare personală:
    - date subiective:
      - prenume;
      - porecla personală;
    - date obiective:
      - nume;
      - iniţialele părinţilor;
      - porecla familiei;
      - fotografie;
      - gen;
      - data naşterii;
      - locul naşterii:
        - continent;
        - ţară;
        - unitate administrativ-teritorială;
        - localitate;
        - adresă:
          - locuinţă;
          - 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:
        - cetăţenie;
        - rezidenţă;
        - etnie;
        - apartenenţă religioasă;
        - adrese:
            - domiciliu;
            - rezidenţă;
            - altele;
        - date educaţionale;
        - 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) şi sociale (de tipul etniei, religiei, mediului de trai, mediului de muncă, obiceiurilor de viaţă - 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 afecţiuni genetice şi metabolice (şi nu numai) fiind strâns legate de etnie, rasă sau obiceiuri determinate de religie.

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

- date prelucrate pentru managementul general al organizaţiei;
- date prelucrate pentru managementul activităţilor specifice ale organizaţiei.

Este evident că o parte a datelor privind activităţile specifice ale organizaţiei 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 organizaţii moderne implică prelucrarea unui pachet de date personale:

- ale angajaţilor;
- ale beneficiarilor activităţilor prestate de către angajaţi:
  - persoane fizice;
  - reprezentanţi ai persoanelor juridice;
- ale furnizorilor de bunuri şi servicii ai organizaţiei;
- ale personalului organizaţiilor cu care au raporturi instituţionale conform legii.

Managementul activităţilor specifice ale organizaţiei presupune extinderea pachetelor de date personale altele decât cele ale angajaţilor, detaliate în capitolul 1.2.1.2.b.

Datele personale prelucrate pentru asigurarea managementului organizaţiei - 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 organizaţiei;
- date privind activităţile specifice executate de către fiecare angajat al organizaţiei *(capitolul 1.2.1.2.b.)*.

Scopul principal al prelucrării acestor date sunt:

- analiza şi decizia managerială;
- raportarea financiar - contabilă conform legii;
- elaborarea de documente comerciale relevante;
- susţinerea activităţilor de promovare, marketing şi comerciale;
- orice altă activitate care este necesară derulării optime a activităţii organizaţiei-operator.

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

Datele personale prelucrate în cadrul activităţilor specifice ale organizaţiei - operator sunt relaţionate:

- datelor personale ale angajaţilor care asigură derularea respectivelor activităţi asupra beneficiarilor acestora;
- datelor financiar - contabile asociate resurselor organizaţiei - operator:
  - alocate derulării activităţilor;
  - rezultate din derularea activităţilor;
- asigurării datelor şi informaţiilor relevante STRICT NECESARE derulării optime a activităţilor.

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

e-PI ADMIN specifică inventarul datelor personale prelucrate conform scopului fiecărui **serviciu e-Pi** de informatizare a activităţilor specifice organizaţiilor - operator utilizatoare, pentru uzul RPD al acestora - acestea corespund interfeţelor de achiziţie de date personale specifice fiecărui serviciu e-Pi. Transmiterea acestor informaţii către posesorul datelor fiind obligaţia organizaţiei - 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.

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

- metode analogice: registrul scris al prelucrărilor de date;
- registrul electronic de evidenţă a prelucrărilor de date – organizaţia - operator de date personale TREBUIE să solicite în mod expres furnizorilor de servicii IT contractaţi în scopul computerizării prelucrărilor de date, inclusiv de date personale, ca aplicaţiile furnizate să fie prevăzute cu sisteme de auditare şi raportare a rezultatelor auditării, cu specificaţii descrise în capitolul 2.2.

Evidenţele prelucrărilor de date personale trebuie să poată fi puse la dispoziţia posesorilor respectivelor date:

- în format analogic - generat şi 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 *(capitolul2.3.).*

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

În funcţie 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 chitanţe pentru o încasare în numerar, uitarea intervenind la data expirării obligativităţii legale de păstrare a documentelor contabile (5 ani în prezent);
- pentru o durată limitată - exemplu: pe durata unui contract de muncă, uitarea intervenind în acelaşi termen ca mai sus;
- pe durată nelimitată - exemplu:
  - istoricul fiscal sau medical al unei persoane;
  - datele de evidenţă a populaţiei.

ESTE OBLIGATORIE MENŢIONAREA DURATEI DE PRELUCRARE A DATELOR ÎN TEXTUL DE INFORMARE ÎN VEDEREA OBŢINERII CONSIMŢĂMÂNTULUI 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 organizaţia operator

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

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

- dreptul de informare şi acces la date cu caracter personal,
- dreptul la rectificare,
- dreptul la ştergerea datelor („dreptul de a fi uitat”),
- dreptul la restricţionarea prelucrării,
- dreptul la portabilitatea datelor,
- dreptul la opoziţie,
- dreptul la decizie individuală automatizată.

1.2.1.5.a. Respectarea temeiului legal pentru prelucrarea datelor personale

În conformitate cu legislaţia naţională şi europeană *(Capitolul 3)*, situaţiile generale reglementate pentru care pot fi prelucrate datele cu caracter personal sunt:

- persoana vizată şi-a dat consimţământul;
- datele sunt necesare pentru executarea unui contract la care persoana vizată este parte;
- îndeplinirea unei obligaţii legale a societăţii,
- prelucrarea este necesară în scopul intereselor legitime ale societăţii.

Pe lângă aceste situaţii, organizaţia - operator poate prelucra date personale în condiţiile legilor speciale, în acest caz, managementul organizaţiei conformându-se prevederilor în cauză.

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

Managementul organizaţiei - operator de date personale trebuie să implementeze, în acord cu cele de mai sus, procedura pentru informarea şi obţinerea consimţământului posesorului de date personale pentru prelucrarea acestora, conform Procedurii de la Capitolul 1.3.

Redactarea conţinutului informativ al formatului pentru obţinerea consimţământului trebuie să asigure prezentarea explicită a tuturor procedurilor din Capitolul 1.2.

1.2.1.5.c. Managementul securității prelucrării datelor personale

Organizaţia - operator de date cu caracter personal asigură managementul securităţii datelor personale prin:

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

Anonimizarea datelor personale

Anonimizarea datelor personale este un mecanism esenţial în maximizarea protecţiei acestora: în procesele de prelucrare computerizată; în cadrul transferurilor de date necesare asigurării fluxurilor informaţionale; în condiţiile stocării şi arhivării pe termen lung a datelor.

e-Pi 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 complicat de utilizat în condiţiile în care responsabilitatea persoanei - posesor al datelor personale este foarte dificilă (din motive de pregătire IT, de conştiinţă civică, de vârstă, motive de ordin social şi educaţional, etc).

Totuşi, este important de înţeles de către operatorii de date personale că sistemele moderne de prelucrare computerizată permit grade progresive de anonimizare a datelor: faţă de operatorii autorizaţi de date personale, raportate: necesităţii de personalizare a datelor prelucrate; nivelului de sensibilitate al datelor prelucrate.

De exemplu:

- datele personale ale unui salariat al organizaţiei - 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 specificaţiile tehnice şi 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 cunoştinţă 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 organizaţia - operator, de fiecare dată când este necesar, pentru a proteja drepturile persoanei.**

DEZANONIMIZAREA DATELOR PERSONALE este un mecanism recomandat ca OBLIGATORIU de către e-Pi 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 organizaţii depinde de prelucrarea unui volum specific de date cu caracter personal, accesibile unui număr de persoane şi organizaţii autorizate în acest sens:

- de către organizaţia-operator;
- prin lege.

În acest context, este necesară o evaluare eficientă a impactului pe care aceste prelucrări le poate avea asupra datelor personale şi posesorilor acestora, dar şi asupra societăţii, urmată de stabilirea unor măsuri eficiente pentru anulare tuturor potenţialelor 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 organizaţiei - operator.

Pe de altă parte, în condiţiile implementării procedurilor interne descrise în prezentul capitol, managementul organizaţiei trebuie să evalueze şi să ia măsuri în consecinţă pentru:

- Evaluarea efectelor prelucrării incorecte a datelor personale în interesul direct al operatorului de date:
  - transmiterea datelor prelucrate:
    - în interes propriu;
    - în interesul unor organizaţii 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 şi care stă la baza unor decizii care produc efecte asupra persoanei fizice[2])*:
  - 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 securităţii datelor personale se poate realiza:

- la nivelul operatorilor autorizaţi ai organizaţiei - 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 condiţiilor şi specificaţiilor precizate la capitolul 2;
- prin nerealizarea sau nerespectarea condiţiilor contractuale cu împuterniciţii organizaţiilor-operator de date personale, conform *capitolului 3*.

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

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

Măsurile necesar a fi luate conform evaluării riscurilor de compromitere a securităţii datelor personale sunt parte a procedurilor stabilite la *capitolele 1.3. şi 2.1.*

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

Instruirea operatorilor IT autorizaţi de către organizaţia - operator de date personale este responsabilitatea RPD al organizaţiei şi 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 restricţionat la depozitele / arhivele organizaţiei:
  - cheie;
  - card de acces;
- accesul la formulare de prelucrare a datelor personale conform drepturilor de prelucrare - trebuie verificat de către un angajat cu funcţie de registrator/arhivar:
  - formularele trebuie marcate cu datele/însemnele organizaţiei;
  - identificarea persoanei care prelucrează datele trebuie să fie vizibilă şi completă;
  - sistemul de arhivare/depozitare al organizaţiei 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 terţilor 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 şi persoana ale cărei date sunt prelucrate trebuie să se facă în mod confidenţial:
    - participarea altor pesoane din cadrul organizaţiei trebuie reglementată[3];
    - acordul persoanei:

[3] Exemplu din medicină unde medicul ia în calcul:
- prelucrarea de date în prezenţa unei asistenţe este obligatorie:
- participarea studenţilor la procesul de tratament al pacientului;
- consult interdisciplinar;
- altele, conform specificului activităţilor 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 facilităţile securizate ale organizaţiei;
    - trebuie verificată de către un angajat cu funcţie de registrator/arhivar.

SECURITATEA ACCESULUI LA DATE ESTE RESPONSABILITATEA COMUNĂ A:

- OPERATORULUI AUTORIZAT:
- REGISTRATORULUI/ARHIVARULUI.

SUPRAVEGHEREA ASIGURĂRII SECURITĂŢII ACCESULUI LA DATE ESTE RESPONSABILITATEA RPD.

1.3.1.2. Prelucrarea computerizată a datelor

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

Proceduri specifice:

- asigurarea securităţii terminalelor prin care se operează date - accesul fizic în spaţiile unde funcţionează terminalele trebuie:
    - restricţionat, accesul fiind rezervat exclusiv operatorilor IT autorizaţi;
    - 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 securităţii transferurilor de date prin securizarea tuturor punctelor de conectare dintre terminale şi unităţile centrale de operare:
    - sisteme intranet;
    - sisteme internet;
    - sisteme mixte;
- asigurarea securităţii accesului la unităţile centrale de operare:

- accesul restricţionat, rezervat exclusiv personalului cu funcţie în procedurile de mentenanţă[4];
- accesul procedurat în cazul serviciilor externalizate către centre de date[5];

- asigurarea securităţii împotriva riscurilor transferurilor de date prin internet:
  - toate echipamentele periferice utilizate în prelucrarea datelor personale TREBUIE SĂ AIBĂ ACCES RESTRICŢIONAT LA INTERNET:
    - prin utilizarea de servicii securizate de conectivitate (VPN, MPLS, VPLS);
    - prin limitarea accesului operatorilor strict la domeniile web utilizate în activitatea organizaţiei (evitarea accesării de domenii web nesigure);
    - prin eliminarea utilizării serviciilor de poştă electronică publice (tip gmail sau yahoo);
- operatorii IT autorizaţi TREBUIE să evite orice formă de dispozitiv de memorie externă, încărcarea de documente sau alte tipuri de fişiere realizându-se exclusiv prin metode care nu prezintă riscuri de infectare a sistemelor de operare IT&C.

Recomandarea este ca toate comunicaţiile digitale ale organizaţiilor - operator de date personale să se realizeze exclusiv prin sistemele de telecomunicaţii securizate enumerate mai sus.

Serviciile de poştă 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 ORGANIZAŢIE SAU ÎN AFARA ACESTEIA.

1.3.2. Asigurarea securităţii prelucrării efective a datelor personale

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

1. Confidenţialitatea prelucrării datelor presupune asigurarea unui mediu de lucru cu posesorul datelor personale adecvat - schimbul de informaţii între persoană şi operatorul autorizat trebuie să se realizeze fără a putea fi interceptat de către terţi;

[4] Procedurile de mentenanţă trebuie solicitate tuturor furnizorilor de sisteme şi servicii IT&C de către RPD şi trebuie comunicate prin instructaj personalului organizaţiei.
[5] Procedurile de securitate şi asigurare a accesului trebuie puse la dispoziţie de către furnizorii IT&C (împuterniciţi ai organizaţiei - operator) şi comunicate personalului organizaţiei 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 (BENEFICIARII 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 organizaţia - operator, supravegheată de către RPD şi pusă în practică de către operatorii autorizaţi ai organizaţiei.

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 şi arhivele de date personale.

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

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

Clasificarea generală a drepturilor de acces utilizată în Platforma e-Pi:

- drept de administrator:
  - poate accesa şi prelucra date fără restricţii;
  - alocă drepturile de operator autorizat;
  - alocă drepturile de acces ale operatorilor autorizaţi;
  - poartă întrega răspundere a prelucrării datelor de către organizaţia-operator;
- drept de procesare de date:
  - complet;
  - restricţionat;
- drept de vizualizare de date;
- drept de vizualizare anonimizată de date;
- drept de prelucrare a datelor:
  - complet;
  - restricţionat;
- drept de vizualizare a rezultatelor prelucrărilor de date;
- drept de utilizare a rezultatelor prelucrărilor de date:
  - prin comunicare:
  - prin tipărire şi comunicare;
  - prin comunicare şi prin transfer;
  - prin partajare;
  - prin publicare.

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

Accesul la datele personale şi 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 e-Pi şi a serviciilor sale integrate, accesul liber securizat al persoanei la propriile date prelucrate se realizează prin PORTALUL e-Pi accesibil acesteia prin autentificare on-line.

1.4. Procedura nr. 3: Informarea persoanelor asupra condiţiilor de prelucrare a datelor şi a drepturilor acestora

Informarea persoanelor asupra condiţiilor de prelucrare a datelor personale şi 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-credinţă a respectivelor date.

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

- pot realiza în orice moment, informarea corectă şi completă a persoanei ale cărei date începe să le prelucreze, asupra condiţiilor de prelucrare şi 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 şi mecanismele de prelucrare a datelor pe care le utilizează.

Procedura de informare a persoanei este:

- adoptată de către organizaţia-operator;
- implementată şi verificată în permanenţă de către RPD;
- aplicată cu rigurozitate de către operatorii autorizaţi.

Platforma e-Pi 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 e-Pi CARD;
  - PORTALUL e-Pi.

Rigoarea şi eficienţa sistemului **e-Pi CARD** excede prevederile GDPR, constituind o **GARANȚIE ABSOLUTĂ** asupra respectării drepturilor persoanei în prelucrarea datelor personale prin Platforma e-Pi și serviciile e-Pi integrate.

NICI O PRELUCRARE DE DATE PERSONALE DE CĂTRE VREUN OPERATOR AL PLATFORMEI e-Pi NU POATE FI REALIZATĂ ŞI FINALIZATĂ ALTFEL DECÂT:

- **ÎN PREZENȚA POSESORULUI DE DATE;**
- **DUPĂ CITIREA CARDULUI e-Pi;**
- **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 funcţionarea societăţii moderne, datorită eficienţei crescute şi costurilor reduse. Idealul ar fi ca, prin procesare computerizată informaţională, în general şi a datelor personale, în particular, să se elimine suportul de hârtie în toate activităţile umane.

Platforma e-Pi este o dovadă operaţională 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 şi sigure, descrise de setul de specificaţii tehnice şi de operare prezentate în acest capitol. Aceste specificaţii asigură:

- SECURITATE;
- EFICIENȚĂ;
- ADAPTABILITATE.

Securitatea prelucrării datelor personale trebuie să asigure, conform GDPR:

- confidenţialitatea,
- integritatea,
- disponibilitatea şi rezistenţa continue ale sistemelor şi serviciilor de prelucrare,
- un proces pentru testarea, evaluarea şi aprecierea periodică ale eficacităţii măsurilor tehnice şi organizatorice.

Aceste caracteristici generale sunt detaliate în capitolul 2.1.

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

- implementare rapidă;
- cost de operare minimal;
- operare eficientă:
  - timp de lucru cât mai redus pentru fiecare operaţiune 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 eficienţi:
  - sub aspectul resurselor utilizate;
  - sub aspectul relevanţei rezultatelor prelucrării.

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

Din perspectiva GDPR esenţiale sunt:

- asigurarea securităţii informatice a sistemelor IT&C utilizate în prelucrarea datelor personale;
- disponibilitatea unor mecanisme de auditare şi 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 securităţii informatice a aplicaţiilor IT&C

Asigurarea securităţii informatice a aplicaţiilor IT&C utilizate în prelucrarea datelor personale este responsabilitatea partajată a:

- Organizaţiei - operator de date;
- împuterniciţilor organizaţiei-operator;
- furnizorului de aplicaţii IT&C.

În cazul Platformei e-Pi, e-Pi ADMIN are calitatea de împuternicit şi furnizor de aplicaţii IT&C pentru toate organizaţiile - operator conectate la platformă, care utilizează servicii e-Pi.

Organizaţia-operator, prin RPD, are obligaţia:

- asigurării implementării procedurilor de securitate a prelucrării datelor la nivelul operatorilor săi autorizaţi (capitolul 1.3.);
- asigurării condiţiilor de securitate generale la nivelul organizaţiei privind accesul la sistemele de prelucrare de date;
- verificării specificaţiilor tehnice ale sistemelor şi serviciilor informatice şi de telecomunicaţii achiziţionate pentru prelucrarea computerizată de date;
- asigurării sistemelor de back-up interne:
  - energetic (echipamente UPS, generatoare electrice);
  - de telecomunicaţii (redundanţa serviciilor de telecomunicaţii);
  - periferice IT&C (disponibilitatea permanentă de echipamente periferice de rezervă).

Împuternicitul trebuie să asigure:

- confidenţialitatea activităţilor sale realizate în beneficiul organizaţiei - operator de date;
- utilizarea de sisteme informatice şi de telecomunicaţii conforme specificaţiilor din capitolele următoare:
    - informarea organizaţiei - operator de date asupra obligaţiilor sale descrise în paragraful anterior.

2.1.1. Securitatea informatică

Securitatea informatică reprezintă ansamblul caracteristicilor prin care datele şi informaţiile sunt prelucrate computerizat:

- continuu;
- fără riscuri de:
    - afectare a calităţii;
    - afectare a volumului;
    - afectare a disponibilităţii:
        - pentru operatori;
        - pentru beneficiarii prelucrării;
    - afectare a drepturilor patrimoniale;
    - afectare a confidenţialităţii:
        - datelor;
        - prelucrării datelor;
        - rezultatelor prelucrării datelor.

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

- datele personale sunt proprietatea exclusivă a posesorului acestora;
- in cazul unor prelucrări de date complexe, care conţin şi date personale, puse la dispoziţia expresă a organizaţiei - operator sau persoanei operator de către posesorul de date (prin consimţământ sau contract):
    - datele personale sunt şi rămân proprietatea posesorului acestora;
    - ansamblul datelor prelucrate, precum şi rezultatele prelucrărilor de date, sunt şi rămân proprietatea organizaţiei - 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 INSTRUCȚIONILOR 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 (volume 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 creşte proporţional cu gradul de deschidere a unui sistem informatic:

- gradul 1 - utilizarea de reţele intranet;
- gradul 2 - conectare la internet;
- gradul 3 - operarea de sisteme în reţele 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 obţinută prin tehnologii care adresează:

- funcţionarea permanentă a sistemelor informatice, asigurând:
  - disponibilitatea datelor;
  - operaţionalitatea 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 şi operate încât:

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

Asigurarea ansamblului condiţiilor de funcţionare optimală a sistemelor informatice permite CERTIFICAREA ACESTORA.

Din punctul de vedere al sistemelor actuale de management informaţional computerizat, măsurile pentru asigurarea funcţionării optimale sunt adresate:

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

        - conectarea la cel puţin două reţele de transport de electricitate distincte;
    - utilizarea unui sistem eficient de back-up failure (preluarea întregii funcţii a centrului de date de către un centru de date secundar ”în oglindă”, în situaţia critică a încetării accidentale a funcţionării centrului de date principal);
    - asigurarea unei capacităţi de procesare eficientă, proporţională cu sistemele informatice operate în centrul de date - asigură disponibilitatea datelor prelucrate în condiţii de eficienţă pentru operator;
- conexiunilor de telecomunicaţii convergente ale centrelor de date:
    - disponibilitatea:
        - asigurarea redundanţei serviciilor de telecomunicaţii:
            - cel puţin doi furnizori de servicii diferiţi:
            - cel puţin două sisteme de telecomunicaţii (exemplu: fibră optică şi 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 reţele virtuale protejate;
        - utilizarea de sisteme de criptare a transferurilor de date;
- conexiunilor de telecomunicaţii convergente ale operatorilor:
    - utilizarea de servicii telecom redundante;
    - utilizarea de sisteme de criptare a transferurilor de date;
    - utilizarea de reţele virtuale protejate;
- echipamentelor periferice ale operatorilor:
    - utilizarea de echipamente periferice conform unui standard de calitate minimal recomandat;
    - asigurarea mentenanţei echipamentelor periferice;
    - limitarea expunerii echipamentelor la riscuri on-line prin limitarea utilizării aplicaţiilor internet fără legătură strictă cu activitatea organizaţiei-operator;
    - utilizarea de sisteme de back-up locale (aplicaţii cu operare off-line care dublează sistemele informatice operate on-line).

Standardul prezentat de asigurare a funcţionării sistemelor informatice în condiţii de securitate este utilizat de către Platforma e-Pi şi recomandat operatorilor de sisteme computerizate pentru management informaţional, indiferent de tipul soluţiilor informatice selectate pentru propria activitate asigură, totodată, toate cerinţele 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 funcţionare 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 situaţii critice;
  - restaurarea rapidă a funcţionării sistemelor informatice după rezolvarea situaţiilor critice.

Platforma e-Pi 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 şi foarte costisitoare, copiile analogice anulând unele dintre cele mai mari avantaje ale computerizării managementului informaţional, mai ales eliminarea consumului de hârtie.

2.1.1.1.c. Securitatea accesului la date

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

- accesarea ilegală de date;
- afectarea funcţionării sistemelor informatice pentru management informaţional.

Confidenţialitatea datelor este preocuparea prioritară a oricărui operator de sisteme de management informaţional şi 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 organizaţii, operatori autorizaţi şi beneficiari ai prelucrărilor de date.

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

De asemeni, în situaţia în care operarea datelor personale se poate realiza în format anonimizat, fără a se afecta scopul şi eficienţa utilizării în acest format, aceasta este recomandabil a se face.

Sistemele informatice care utilizează anonimizarea ca metodă de protecţie 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 specificaţiilor capitolului 2.1.1.1.a.

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

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

În esenţă, organizaţiile - 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 informaţionale reprezintă totalitatea transferurilor de date şi informaţii realizate în cadrul managementului informaţional (care include toate prelucrările de date, inclusiv cele personale):

- în cadrul organizaţiei - operator;
- între organizaţia - operator şi terţi.

Din punct de vedere tehnologic, fluxurile informaţionale asigură:

- funcţionarea optimală a sistemelor informatice utilizate de către organizaţia-operator şi operatorii autorizaţi ai acesteia - fluxurile din cadrul sistemelor interne de prelucrare a datelor;
- interconectarea organizaţiei - operator cu terţe părţi:
  - alte organizaţii;
  - persoane fizice ale căror date sunt prelucrate de către organizaţia-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 e-Pi 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 e-Pi -unicul sistem de comunicare prin internet cu persoane fizice: identificate prin:
  - cont,
  - parolă,
  - PIN,
  - card e-Pi.

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

Platforma e-Pi are un standard unic de securitate informatică pentru toate componentele sale, cu excepţia securităţii fluxurilor informaţionale externe, pentru care se aplică 4 niveluri de securitate progresive.

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

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

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

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

Totuşi, organizaţii - operator de date personale pot lucra ne-informatizat, situaţie 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 soluţie minimală de informatizare, a unui registru electronic de evidenţă 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 funcţionare standard periodică, la care să se adauge posibilitatea de a genera în orice moment, rapoarte de audit în timp real. Un model operaţional în acest sens este Platforma e-Pi.

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 următoarelor 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 securităţii informatice a organizaţiei - operator, fie că operează datele direct sau prin intermediari, este o prioritate a RPD.

Auditarea securităţii informatice trebuie să cuprindă evaluarea:

1. acţiunilor 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. locaţia autentificării:

1. din sediul organizaţiei;
2. la distanţă;

   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 securităţii informatice trebuie să poată fi optimizate conform:

- specificaţiilor organizaţiilor-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 dispoziţia RPD şi a managementului organizaţiei - operator, precum şi a persoanei ale cărei date sunt prelucrate, la cererea acesteia, a cel puţin următoarelor date:

- în istoric pentru o durată precizată (de la data de – la data de);
- actualizate la zi:
  - Informarea persoanei:
    - conţinutul informării;
    - emiterea informării;
    - confirmarea informării de către persoană;
  - Consimţământul informat al persoanei:
    - semnarea (fizică sau electronică) a consimţământului;
    - arhivarea adecvată a consimţământului;
  - Solicitările persoanei privind prelucrarea datelor personale:
    - restricţionare a prelucrării;
    - retragerea consimţământului;
    - ştergerea completă a datelor personale - atunci când este posibil legal;
    - comunicarea de date personale:
      - fizică;
      - prin PORTALUL e-Pi;
      - 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-DIRECŢIONALĂ ON-LINE dintre persoană şi organizaţia - operator de date, respectiv operatorii autorizaţi ai acesteia.

Acest mecanism asigură:

- informare în timp real a persoanei asupra:
  - condiţiilor de prelucrare a datelor şi modificărilor acestora;
  - incidentelor de securitate şi măsurilor aferente acestora;
  - altor situaţii specifice;
- primirea, din partea persoanei, de solicitări şi informaţii 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 e-Pi.

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

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

3. LEGISLAȚIE PRIVIND PRELUCRAREA COMPUTERIZATĂ A DATELOR CU CARACTER PERSONAL

3.1. Prevederi contractuale exprese pentru respectarea GDPR

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

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

În situaţia prelucrării directe prin sisteme informatice, dar şi prin împuterniciţi, utilizând sisteme informatice operate de către aceştia, prevederile contractuale trebuie să asigure, dar nu exclusiv, respectarea tuturor specificaţiilor tehnice descrise în capitolul 2.

În toate situaţiile, organizaţia - operator trebuie să contractualizeze personalul propriu şi al împuterniciţilor, astfel încât să se respecte, dar nu exclusiv, toate specificaţiile capitolului 1.

În situaţia prelucrării computerizate a datelor prin împuterniciţi, contractele semnate de către organizaţia - operator cu aceştia trebuie să prevadă, dar nu exclusiv, următoarele clauze:

1. **Calitatea de împuternicit** a organizaţiei în cauză, în conformitate cu Regulamentul (UE) 2016/679 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date (denumit în continuare ”GDPR”), ca şi orice legislaţie naţională subsecventă cu privire la domeniul protecţiei 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 şi/sau analogice contractate, conform descrierii tehnice şi comerciale a acestora;

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

<u>Celelalte clauze necesar a fi cuprinse în contractul organizației - operator pot fi adaptate conform modelului de contract standard utilizat de către e-Pi ADMIN:</u>

5. **Drepturile şi obligaţiile părţilor:**

5.1. Drepturile şi obligaţiile Operatorului

• Dreptul să primească informaţii de la împuternicit sau să verifice prin auditor mandatat dacă împuternicitul are şi pune în aplicare măsuri tehnice şi organizatorice adecvate, astfel încât prelucrarea să respecte cerinţele prevăzute de GDPR; verificarea va avea loc în baza unei notificări scrise prealabile, transmisă cu cel puţin 14 zile lucrătoare înainte de efectuarea verificării;

• Dreptul să primească asistenţă din partea împuternicitului, în special pentru îndeplinirea obligaţiei sale de a răspunde cererilor persoanelor vizate cu privire la exercitarea drepturilor lor prevăzute de GDPR;

• Dreptul de a face obiecţiuni cu privire la alţi sub-împuterniciţi;

• Să respecte obligaţiile sale conform GDPR în calitate de operator cu privire la datele cu caracter personal colectate sau prelucrate de împuternicit, pe seama sa;

• Obligaţia de a face informarea persoanelor vizate conform GDPR, inclusiv în ceea ce priveşte informarea cu privire la prelucrarea datelor de către împuternicit în temeiul acestui contract;

• Obligaţia să răspundă exclusiv de stabilirea temeiului legal pentru prelucrarea datelor cu caracter personal ce face obiectul prezentului contract;

• Obligaţia de a implementa măsuri tehnice şi organizatorice adecvate conform GDPR, inclusiv securizarea transferului datelor de la persoanele vizate către Împuternicit;

• Operatorul înţelege că din momentul ştergerii datelor după încheierea prestării serviciilor de către Împuternicit conform obligaţiilor GDPR, datele nu mai pot fi recuperate şi este întreaga responsabilitate a Operatorului să se asigure că şi-a făcut o copie completă a acestora.

• În toate situaţiile în care operatorul este cel care trebuie să execute o obligaţie, cum este, spre exemplu, informarea persoanei vizate cu privire la încălcarea securităţii datelor cu caracter personal, împuternicitul nu poate fi ţinut de inacţiunile operatorului din sfera acelei obligaţii.

5.2. Drepturile şi obligaţiile împuternicitului:

• Obligaţia să informeze operatorul în termen de maxim 10 zile, în cazul în care, în opinia împuternicitului, o instrucţiune încalcă GDPR şi/sau altă dispoziţie legală privind prelucrarea datelor cu caracter personal;

• Obligaţia să asigure securitatea datelor cu caracter personal prelucrate în numele operatorului în conformitate cu art 32 din GDPR;

• Obligaţia de a informa operatorul fără întârzieri nejustificate de o încălcare a securităţii datelor personale ale operatorului pe parcursul prelucrării realizate de către împuternicit;

• Obligaţia de a asista operatorul cu toate informaţiile necesare în vederea notificării, dacă este cazul, către autoritatea competentă pentru încălcarea securităţii datelor, dar fără a se substitui operatorului în obligaţia sa de notificare;

• Obligaţia de a acorda asistenţă operatorului să asigure respectarea obligaţiilor prevăzute la articolele 32-36 din GDPR;

• Obligaţia de a asista operatorul pentru soluţionarea cererilor persoanelor vizate sau de a transmite operatorului orice cerere primită de la persoanele vizate, în legătură cu datele personale care au fost colectate şi prelucrate de împuternicit, în termen de maxim 5 zile calendaristice de la primirea acesteia. Această asistenţa nu se aplică în situaţia în care operatorul are deja în instrumentele tehnice furnizate de către împuternicit posibilitatea de a soluţiona direct cererea persoanei vizate (de ex. dreptul la acces – unde operatorul are deja toate informaţiile cu privire la ce date colectează);

• Obligaţia să nu transmită date cu caracter personal şi/sau informaţii confidenţiale, ce pot fi date cu caracter personal, despre care a luat cunoştinţă în timpul executării contractului;

• Obligaţia să asigure instruirea personalului autorizat să prelucreze datele cu caracter personal, cu privire la confidenţialitatea acestor date;

• Obligaţia să includă obligaţii de confidenţialitate către angajaţi şi sub-împuterniciţi;

• Dreptul să dezvăluie anumite date cu caracter personal în virtutea unei obligaţii legale sau a unei alte condiţii prevăzute de legislaţie la solicitarea unei autorităţii, instituţii publice sau instanţe judecătoreşti.

• Dreptul de a recruta sub-împuterniciţi;

• Dreptul la acoperirea costurilor generate de asigurarea asistenţei operatorului în situaţiile prevăzute de GDPR, dacă acestea depăşesc costul serviciilor prestate de către împuternicit.

• Dreptul de a folosi informaţii statistice anonimizate ca urmare a activităţilor prestate ca urmare a acestui contract sau a întregii sale activităţi.

• Obligaţia de a şterge 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 părţi.
• 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 şi 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 şi natura, domeniul de aplicare, contextul şi scopurile prelucrării, precum şi riscul cu diferite grade de probabilitate şi gravitate pentru drepturile şi libertăţile persoanelor fizice, ca şi 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 şi 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 experţi în securitate cibernetică ;
    - acces limitat la baza de date pentru un număr foarte restrâns de angajaţi ai împuternicitului;
    - monitorizarea permanentă a accesului la baza de date;
    - criptarea conexiunii folosite de operator pentru accesarea serviciului folosind SSL ;
    - parolele clienţilor stocate criptat ;
    - copii de siguranţă regulate;
- În mod voluntar, împuternicitul poate trimite rezumatele concluziilor auditorilor de securitate (după ştergerea informaţiilor comerciale sau confidenţiale) realizate periodic către operatori pentru a demonstra activităţile sale continue pe acest subiect.

7. Limitarea răspunderii

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

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

8. Delimitarea răspunderii

Operatorul şi împuternicitul îşi delimitează responsabilităţile cu privire la asigurarea protecţiei datelor cu caracter personal (de exemplu asigurarea confidenţialităţii sau a securităţii prelucrării), în funcţie de accesul şi controlul efectiv exercitat asupra datelor, atât din punct de vedere contractual, cât şi tehnic

3.2. Reglementări legislative române

- Convenţia pentru protejarea persoanelor faţă de prelucrarea automatizată a datelor cu caracter personal din 28.01.1981 - Act Internaţional
- Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul comunicaţiilor electronice - Parlamentul României
- Legea nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date - Parlamentul României
- Legea nr. 238/2009 privind reglementarea prelucrării datelor cu caracter personal de către structurile/unităţile Ministerului Administraţiei şi Internelor în activităţile de prevenire, cercetare şi combatere a infracţiunilor, precum şi de menţinere şi 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 şi protecţia vieţii private în sectorul comunicaţiilor electronice - Parlamentul României
- Legea nr. 235/2015 pentru modificarea şi completarea Legii nr. 506/2004 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul comunicaţiilor electronice - Parlamentul României
- Legea nr. 682/2001 privind ratificarea Convenţiei pentru protejarea persoanelor faţă 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 şi pentru modificarea şi abrogarea unor decizii - Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal - ANSPDCP
- Hotărârea nr. 57/2017 referitoare la propunerea de Regulament al Parlamentului European şi al Consiliului privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal de către instituţiile, organele, oficiile şi agenţiile Uniunii şi privind libera circulaţie a acestor date şi de abrogare a Regulamentului (CE) nr. 45/2001 şi 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 funcţionarea Uniunii Europene privind poziţia Consiliului în ceea ce priveşte adoptarea unei directive a Parlamentului European şi a Consiliului privind protecţia 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 infracţiunilor sau al executării pedepselor şi privind libera circulaţie a acestor date şi de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului - Parlamentul European şi Consiliul Uniunii Europene

- Rectificare la Directiva 2009/136/CE a Parlamentului European şi a Consiliului din 25 noiembrie 2009 de modificare a Directivei 2002/22/CE privind serviciul universal şi drepturile utilizatorilor cu privire la reţelele şi serviciile de comunicaţii electronice, a Directivei 2002/58/CE privind prelucrarea datelor personale şi protejarea confidenţialităţii în sectorul comunicaţiilor publice şi a Regulamentului (CE) nr. 2006/2004 privind cooperarea dintre autorităţile naţionale însărcinate să asigure aplicarea legislaţiei în materie de protecţie 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 şi a Consiliului privind nivelul de protecţie adecvat asigurat de Statul Israel privind prelucrarea automată a datelor cu caracter personal [notificată cu numărul C(2011) 332] (Text cu relevanţă pentru SEE) - Comisia Comunităţilor Europene
- Decizia nr. 146/2010 în temeiul Directivei 95/46/CE a Parlamentului European şi a Consiliului privind nivelul de protecţie adecvat asigurat de Legea feroeză privind prelucrarea datelor cu caracter personal [notificată cu numărul C(2010) 1130] (Text cu relevanţă pentru SEE) - Comisia Comunităţilor Europene
- Directiva nr. 136/2009 de modificare a Directivei 2002/22/CE privind serviciul universal şi drepturile utilizatorilor cu privire la reţelele şi serviciile de comunicaţii electronice, a Directivei 2002/58/CE privind prelucrarea datelor personale şi protejarea confidenţialităţii în sectorul comunicaţiilor publice şi a Regulamentului (CE) nr. 2006/2004 privind cooperarea dintre autorităţile naţionale însărcinate să asigure aplicarea legislaţiei în materie de protecţie a consumatorului (Text cu relevanţă pentru SEE) - Parlamentul European şi Consiliul Uniunii Europene
- Decizia nr. 597/2008 de adoptare a dispoziţiilor de punere în aplicare privind responsabilul cu protecţia datelor în temeiul articolului 24 alineatul (8) din Regulamentul (CE) nr. 45/2001 privind protecţia persoanelor fizice cu privire la prelucrarea datelor cu caracter personal de către instituţiile şi organele comunitare şi privind libera circulaţie a acestor date - Comisia Comunităţilor Europene
- Regulamentul nr. 1024/2012 privind cooperarea administrativă prin intermediul Sistemului de informare al pieţei interne şi de abrogare a Deciziei 2008/49/CE a Comisiei ("Regulamentul IMI") (Text cu relevanţă pentru SEE) - Parlamentul European şi Consiliul Uniunii Europene

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

4.1. Reglementări ale instituțiilor Uniunii Europene

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

4.2. Reglementări legislative române

- Legea nr. 200/2004 privind recunoaşterea diplomelor şi calificărilor profesionale pentru profesiile reglementate din România - Parlamentul României
- Legea nr. 160/1998 pentru organizarea şi exercitarea profesiunii de medic veterinar - Parlamentul României
- Ordonanţa de urgenţă nr. 70/2017 privind modificarea şi completarea Legii nr. 160/1998 pentru organizarea şi exercitarea profesiunii de medic veterinar - Guvernul României
- Statutul medicului veterinar din 25.10.2016 - Colegiul Medicilor Veterinari - CMV
- Legea nr. 95/2006 privind reforma în domeniul sănătăţii - Parlamentul României
- Legea nr. 48/2017 privind aprobarea Ordonanţei de urgenţă a Guvernului nr. 45/2016 pentru modificarea şi completarea Legii nr. 95/2006 privind reforma în domeniul sănătăţii - Parlamentul României
- Ordonanţa de urgenţă nr. 109/2007 pentru modificarea şi completarea Legii nr. 200/2004 privind recunoaşterea diplomelor şi calificărilor profesionale pentru profesiile reglementate din România - Guvernul României
- Hotărârea Guvernului nr. 1.071/2013 privind aprobarea Strategiei Naţionale pentru Ocuparea Forţei de Muncă 2014-2020 şi a Planului de acţiuni pe perioada 2014-2020 pentru implementarea Strategiei naţionale 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 aparţin;
- limiteze posibilităţile de utilizare excesivă a datelor personale de către operatorii acestora;
- asigure un mecanisme eficient de control al operării datelor personale.

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

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

- pentru organizaţiile - operator;
- pentru operatorii autorizaţi ai organizaţiilor-operator;
- pentru administraţia care asigură controlul şi / sau coordonarea activităţilor organizaţiilor - operator:
    - locală;
    - centrală.

În prezent există legislaţie specială europeană, prezentată în *capitolul 3*, pentru managementul datelor persoanelor care prezintă risc de securitate socială, precum şi pentru alte domenii, cum sunt medicina, finanţele publice, justiţia.

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

În aceste condiţii, este considerată imperativă iniţierea şi coordonarea unui demers naţional şi european pentru elaborarea unui cadru normativ precis care să completeze prevederile GDPR, acoperind totalitatea activităţilor sociale care presupun prelucrarea de date cu caracter personal.

O atenţie specială este acordată în acest document problematicii prelucrării datelor medicale şi a celor de evidenţă a populaţiei, date care trebuie tratate cu maximă responsabilitate.

e-Pi ADMIN a iniţiat, 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 documentaţii, pe măsura obţinerii acestora.