SPITALUL ORĂȘENESC „SFÂNTA FILOFTEIA'' MIZIL
Strada Spitalului nr.21,Mizil.Tel.250505,Fax 251115

POLITICA DE SECURITATE CU PRIVIRE LA PRELUCRAREA DATELOR CU CARACTER PERSONAL ÎN CADRUL SPITALULUI ORĂȘENESC „SFÂNTA FILOFTEIA" MIZIL

1. CADRU LEGISLATIV

Cadrul legislativ privind protecția datelor personale și securitatea informatica este constituit la nivel european și național de următoarele normative:

- Regulamentul European 2016/679 – Regulamentul General pentru Protecția Datelor
- Legea 190/2018 – transpunerea și aplicarea Regulamentului 679/2016
- Directiva EU 1148/2016 – Directiva NIS (Networking Information Security)
- Legea 362/2018 – transpunerea și aplicarea Directivei NIS
- Regulamentul 881/2019 – Regulamentul de CyberSecurity (CyberSecurity Act)

2. TERMENI ŞI EXPRESII

a) ***administrator de reţea*** - persoană calificată în domeniul tehnologiei informaţiei, desemnată să gestioneze utilizatorii, resursele hardware şi software şi modul de acces la resursele reţelei de date; în cazul spitalului firma cu care spitalul are încheiat contract **servicii de întreţinere şi administrare reţea calculatoare, service şi mentenanţă echipamente periferice, service şi mentenanţă computere personale şi servicii găzduire web hosting**
b) ***blocare acces staţie de lucru*** - set de comenzi specific staţiei de lucru care permite interzicerea imediată a accesului de la tastatură la staţia de lucru;
c) ***dispozitiv wireless*** - echipament de tehnică de calcul şi comunicaţii care poate asigura conectarea la reţele de comunicaţii prin unde radio;
d) ***echipamente periferice*** - imprimantele, scanerele, multifuncţionalele, unităţile mobile disc flexibil, unităţile mobile hard disk, modemurile;
e) ***fişier multimedia*** - fişier având o organizare internă dedicată stocării unei combinaţii de formate text, audio, fotografie, animaţie, film şi conţinut interactiv;
f) ***medii/suporturi externe de stocare a datelor*** - bandă magnetică, disc fix, dischetă, casetă, CD-ROM/RW, DVD-ROM/RW, chei USB flash/stick, HDD extern portabil;
g) ***nume de utilizator (user name)*** - cod alfanumeric atribuit persoanei care urmează să acceseze resurse ale sistemului informatic;
h) ***parola de acces (password)*** - cod (şir de caractere) primit odată cu staţia/aplicaţia, folosit pentru accesarea resurselor. Parola trebuie schimbată de utilizator de la prima folosire, astfel încât să nu fie cunoscută decât de acesta;
i) ***patch cord*** - cablul de reţea care face legătura între staţie şi priza de reţea montată pe perete;
j) ***resursele sistemului informatic*** - echipamentele de tehnologia informaţiei (servere, staţii de lucru, imprimante, scanere etc.), reţelele de comunicaţii de date LAN, MAN, WAN, alte componente şi instalaţii (climatizare, alimentare cu energie, stingere incendiu, control acces fizic etc.), mediile de stocare a datelor, software-ul de bază, aplicaţiile informatice, programele utilitare, datele, bazale de date, fişierele, sistemele de protecţie a datelor, personalul ce exploatează şi întreţine resursele sistemului informatic, documentaţiile de proiectare, documentaţiile de exploatare etc., procedurile de lucru, planurile de continuitate, teoriile ce stau la baza algoritmilor de prelucrare etc.;
k) ***reţea de date/reţea de comunicaţii de date*** - subansamblu al sistemului informatic format din patch corduri, prize de reţea, cablaj structurat, echipamente de comunicaţii, protocoale de comunicaţii şi software pentru administrarea comunicaţiilor. Reţeaua de date are rolul de a oferi suport hardware şi software pentru interconectarea staţiilor de lucru, serverelor, imprimantelor etc. şi pentru acces la serviciile informatice, inclusiv la poştă electronică şi internet;

l) *serviciu informatic* - unul sau mai multe subsisteme ale sistemului informatic care permit desfăşurarea unui proces de lucru în cadrul organizaţiei;
m) *sistem informatic* - ansamblul de elemente care asigură introducerea, prelucrarea, stocarea, transmiterea şi extragerea datelor pe cale electronică realizat în scopul oferirii de servicii informatice;
n) *staţie de lucru* - ansamblul format din calculator şi echipamentele periferice destinat realizării sarcinilor de serviciu, conectat sau nu la reţeaua de date a MFP şi care are sau nu acces la alte resurse ale sistemului informatic;
o) *staţie de lucru mobilă/staţie mobilă* - laptop, tabletă electronică, agendă electronică, telefon mobil inteligent;
p) *UPS* - sursă neîntreruptibilă de tensiune; asigură alimentarea cu energie electrică a consumatorilor, un timp limitat, în cazul lipsei tensiunii în reţeaua publică;
r) *utilizatorul /responsabilul staţiei de lucru* - persoana angajată care a primit dreptul de acces la staţia de lucru şi drepturi de utilizare a resurselor sistemului informatic.
s) intranet – rețeaua internă de calculatoare
ș) cont – o entitate specificată pritr-un identificator și/sau parolă pentru accesul la sistemul de comunicație și/sau la o resursă de calcul

3. SCOP

(1) În calitate de operator de date cu caracter personal, ***Spitalul Orășenesc „Sfânta Filofteia” , Mizil*** (denumit în continuare *Spitalul*) urmăreşte în permanenţă şi se asigură că prelucrarea datelor cu caracter personal respectă cu stricteţe principiile şi legislaţia privind protecţia datelor cu caracter personal, în particular prevederile Regulamentului (UE) 2016/679 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE (in continuare „RGPD”)
(2) Prelucrarea datelor cu caracter personal se realizează prin mijloace mixte (manuale şi automate), cu respectarea cerinţelor legale şi în condiţii care să asigure securitatea, confidenţialitatea şi respectarea drepturilor persoanelor vizate.
(3) Prezenta Politică este elaborată în scopul asigurării integritatii, confidentialitatii, disponibilitatii și securităţii informaţiilor din cadrul ***Spitalului Orășenesc „Sfânta Filofteia”, Mizil***.
(4)***Confidentialitatea*** se refera la protectia datelor impotriva accesului neautorizat. Utilizatorul raspunde personal de confidentialitatea datelor incredintate prin procedurile de acces la sistemele informatice si de comunicatii
(5) ***Integritatea*** se refera la masurile si procedurile utilizate pentru protectia datelor impotriva modificarilor sau distrugerii neautorizate.
(6) ***Disponibilitatea*** se asigura prin functionarea continua a tuturor componentelor sistemelor informatice si de comunicatii. Sistemele informatice utilizate au nevoie de nivele diferite de disponibilitate in functie de impactul sau daunele produse ca urmare a nefunctionarii corespunzatoare.
(4) De asemenea, politica de securitate are ca scop stabilirea cadrului necesar pentru elaborarea politicilor si procedurilor de securitate.
(5) Prezenta Politică de Securitate stabilește măsuri tehnice și organizatorice implementate de *Spitalul Orășenesc „Sfânta Filofteia”, Mizil* pentru îndeplinirea obligațiilor referitoare la confidențialitatea și securitatea prelucrărilor efectuate în cadrul activității sale.
(6) Prin cerințe minime de securitate este avut în vedere un complex de măsuri tehnice, informatice, organizatorice, logistice și proceduri prin care se asigură un nivel de securitate al prelucrărilor în conformitate cu legislația națională, precum și cu cerințele Regulamentului European privind Protecția Datelor Personale GDPR 2016/679.

4. OBIECTIVE

Această politică este stabilită astfel încât:

- să fie în conformitate cu statutul, regulamentele, legile și alte documente oficiale în vigoare privind administrarea resurselor informatice
- să stabilească practici prudente și acceptabile privind utilizarea resursele informaționale și de comunicații ale *Spitalului Orășenesc „Sfânta Filofteia”, Mizil*
- să instruiască utilizatorii care au dreptul de folosire a acestor resurse privind responsabilitățile asociate unei astfel de utilizări
- să ducă la creşterea confidenţialităţii, integrităţii şi disponibilităţii datelor şi informaţiilor vehiculate în cadrul sistemelor informatice şi de comunicaţii utilizate în cadrul spitalului

- să ofere mijloace de ghidare şi susţinere a activităţii referitoare la securitatea informaţiei în cadrul spitalului, prin definirea de controale şi măsuri ce vizează identificarea și reducerea riscurilor şi vulnerabilităţilor de securitate manifestate în cadrul acestora
- să ducă la creșterea nivelului general de cunoștințe în domeniul securității, în scopul îmbunătățirii climatului general de securitate în spital;

5. DOMENIU APLICARE ȘI RESPONSABILITĂȚI

4.1.Domeniu de aplicare

Politica se aplică tuturor angajaților *Spitalului Orășenesc „Sfânta Filofteia", Mizil*, persoanelor care efectuează practică în cadrul spitalului, persoanelor imputernicite care acceseaza resursele informatice si de comunicatie ale *Spitalului Orășenesc „Sfânta Filofteia", Mizil, etc.*

4.2.Responsabilități

Comitetul Director:

- aprobă politica de securitate a informațiilor.
- promovează prezenta politică.
- stabilește și aprobă politica generală, politicile subsecvente și obiectivele privind confidențialitatea datelor,
- asigură disponibilitatea resurselor necesare pentru managementul proceselor legate de confidențialitatea datelor,
- se asigură că responsabilul cu protectia datelor este implicat în mod corespunzator și în timp util în toate aspectele legate de protecția datelor cu caracter personal,
- sprijină responsabilul cu protecția datelor în îndeplinirea sarcinilor, asigurându-i resursele necesare pentru executarea acestor sarcini
- se asigură că responsabilul cu protecția datelor nu primește niciun fel de instrucțiuni în ceea ce privește îndeplinirea sarcinilor atribuite,
- comunică importanța respectării cerințelor Regulamentului UE 2016/679 - GDPR,
- îndrumă și sprijină personalul să contribuie la eficacitatea gestionarii datelor de natură personală,
- promovează imbunătățirea continuă.

Responsabilul cu protectia datelor are atribuții în ceea ce privește:

- informarea si consilierea conducerii, precum si a angajatilor care se ocupa de prelucrare cu privire la obligatiile care le revin in temeiul Regulamentului UE 2016/679 – GDPR
- monitorizarea respectarii Regulamentului UE 2016/679 – GDPR, a altor dispozitii de drept al uniunii sau de drept intern referitoare la protectia datelor si a politicilor operatorului in ceea ce priveste protectia datelor cu caracter personal
- furnizarea de consiliere la cerere in ceea ce priveste evaluarea impactului asupra protectiei Datelor si monitorizarea functionarii acesteia,
- cooperarea cu Autoritatea de Supraveghere,
- asumarea rolului de punct de contact pentru autoritatea de supraveghere privind aspectele legate de prelucrare, inclusiv consultarea prealabila precum si, daca este cazul, consultarea cu privire la orice alta chestiune.

Șefii/Coordonatorii secțiilor/compartimentelor, asistentele șefe/coordonatoare sunt responsabili pentru

- implementarea de zi cu zi a cerintelor privind gestionarea in siguranta a datelor cu caracter personal,
- asigurarea ca masurile de securitate tehnice, fizice si procedurale stabilite sunt aplicate in mod corespunzator si de catre personalul din subordine,
- asigurarea resurselor si efectuarea analizelor necesare pentru a se asigura ca informatiile si activele informationale sunt protejate in mod corespunzator in zona lor de responsabilitate,
- informarea responsabilului cu protectia datelor despre incalcarile reale sau presupuse ale politicilor de confientialitate a datelor din zona lor de responsabilitate (incidente privind confidentialitatea datelor).

Responsabilul IT/Administratorul de rețea:

- propune modificari ale politicii de securitate a informatiilor.

- elaboreaza si propune pentru aprobare proceduri de securitate a resurselor informatice si de comunicatii
- trateaza incidentele de securitate in scopul minimizarii efectului distructiv al acestora asupra resurselor informatice si de comunicatii.
- asigura existenta jurnalelor si a traseelor pentru orice tip de acces in sistem
- asigura activarea tuturor mecanismelor de securitate.

Utilizatorii datelor / sistemelor (angajati si terti care actioneaza intr-o modalitate similara, cum ar fi contractori, consultanti, studenti aflati in practica, etc.):

- cunosc și respectă prevederile politicii de securitate a informațiilor.
- răspund direct de securitatea si continutul informatiilor si resursele informatice si de comunicatii incredintate direct sau indirect.
- respectă toate politicile privind confidențialitatea și protecția datelor aplicabile pentru locurile lor de muncă.
- sunt responsabili pentru mentinerea protectiei si confidentialitatii tuturor informatiilor incredintate,
- informarea responsabilului cu protectia datelor și responsabilului IT despre incalcarile reale sau presupuse ale politicilor de confientialitate a datelor din zona lor de responsabilitate (incidente privind confidentialitatea datelor).
- informarea responsabilului cu protectia datelor despre solicitarile de acces venite din partea persoanelor vizate.

6. MĂSURI TEHNICE ȘI ORGANIZATORICE IMPLEMENTATE

(1) Spitalul Orășenesc „Sfânta Filofteia", Mizil a adoptat măsuri tehnice și organizatorice adecvate pentru protejarea datelor cu caracter personal împotriva distrugerilor accidentale sau ilegale, pierderii, modificării, dezvăluirii, accesului neautorizat sau oricărei alte forme de prelucrare ilegală.

(2) În calitate de operator de date cu caracter personal, pentru a îndeplini cerințele legislației în vigoare și a proteja drepturile persoanelor vizate atât în momentul stabilirii mijloacelor de prelucrare a datelor cu caracter personal cât și a prelucrării în sine, spitalul aplică măsuri tehnice și organizatorice adecvate, astfel:

- Personalul spitalului a fost informat și instruit cu privire la prevederile Regulamentului UE 2016/679, astfel că *Spitalul Orășenesc „Sfânta Filofteia", Mizil* prelucrează datele cu caracter personal cu respectarea principiilor prevăzute în Regulamentul UE 2016/679.

(3) Art. 5 alin (1) al GDPR enumeră aceste principii și le transformă în piatra de temelie a oricărei operațiuni de prelucrare. Aceste principii sunt extrem de importante, pentru că ele sunt asimilate unor adevărate reguli fundamentale pe care trebuie să se bazeze orice prelucrare de date cu caracter personal.

Datele cu caracter personal sunt:

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

Cu alte cuvinte, spitalul se asigură că:

● are temeiuri corecte pentru colectarea și utilizarea datelor cu caracter personal;

● nu utilizează datele în moduri care au efecte negative nejustificate asupra persoanelor în cauză;

● este transparent cu privire la modul în care intenționează să utilizeze datele și să ofere persoanelor respective o informare detaliată în momentul colectării datelor lor personale.

b) colectate în scopuri <u>determinate, explicite și legitime</u> și nu sunt prelucrate ulterior într-un mod incompatibil cu aceste scopuri; Prelucrarea ulterioară în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice nu este considerată incompatibilă cu scopurile inițiale („limitări legate de scop");

Cu alte cuvinte, spitalul se asigură că:

● oferă persoanelor vizate, în informarea prezentată la momentul colectării datelor lor personale, o trecere în revistă a scopurilor pentru care colectează fiecare categorie de date;

● nu schimbă scopul pentru care au fost colectate datele, fără informarea prealabilă a persoanelor vizate și parcurgerea tuturor pașilor tranzitorii necesari, atunci când e cazul (spre exemplu, dacă e nevoie să se obțină consimțământul persoanei vizate pentru această nouă prelucrare).

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

Cu alte cuvinte, spitalul:
● colectează un număr de date nici mai mic și nici mai mare pentru atingerea scopului propus;
● nu colectează date pe principiul *"nu se știe niciodată când vom avea nevoie de ele*".
d) **exacte și, în cazul în care este necesar, să fie actualizate; spitalul ia toate măsurile necesare pentru a se asigura că datele cu caracter personal care sunt inexacte, având în vedere scopurile pentru care sunt prelucrate, sunt șterse sau rectificate fără întârziere („exactitate");**
Cu alte cuvinte, atunci când prelucrează date, spitalul:
● verifică regulat exactitatea datelor prelucrate sau, dacă acest lucru nu e posibil,
● pune la dispoziția persoanelor vizate un mecanism prin intermediul căruia să își poată corecta, completa sau actualiza datele personale respective. **(în cadrul spitalului la avizierele destinate informării GDPR este afișat formular privind dreptul de rectificare a datelor personale ale persoanelor vizate)**
e) păstrate într-o formă care permite identificarea persoanelor vizate pe o perioadă care nu depășește perioada necesară îndeplinirii scopurilor în care sunt prelucrate datele („limitări legate de stocare"),
Drept pentru care, spitalul:
● nu stochează / prelucrează datele personale colectate pentru o perioadă mai mare de timp decât aceea necesară îndeplinirii scopului (la momentul colectării, în informare, persoanei vizate i se aduce la cunoștință pentru ce perioadă de timp, se va face prelucrarea)
● revizuiește periodic datele prelucrate, pentru a identifica ce date sunt prelucrate, care nu mai respecta principiul limitării perioadei de stocare și vor trebui, prin urmare, șterse ori anonimizate.
f) **prelucrate într-un mod care asigură securitatea adecvată a datelor cu caracter personal, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luarea de măsuri tehnice sau organizatorice corespunzătoare („integritate și confidențialitate").**
Drept pentru care:
- Persoanele care prelucrează, în numele Spitalului date cu caracter personal au semnat un Acord de confidențialitate.
- ➢ *Spitalul Orășenesc „Sfânta Filofteia", Mizil* prelucrează datele cu caracter personal cu respectarea drepturilor persoanelor vizate prevăzute în Regulamentul 2016/679.

(4) Regulamentul recunoaște persoanelor vizate o serie de drepturi
- Dreptul la informare art. 13 și 14 GDPR.
- Dreptul de acces la date art. 15 GDPR
- Dreptul la ștergerea datelor art. 17 GDPR
- Dreptul la rectificarea datelor art. 16 GDPR:
- Dreptul la restricționarea datelor art. 18 GDPR
- Dreptul la portabilitatea datelor art. 20 GDPR.
- Dreptul la opoziție art. 21 GDPR.
- Dreptul de a nu face obiectul unei decizii bazate exclusiv pe prelucrarea automata art. 22 GDPR.
- Dreptul de a nu face obiectul unei decizii bazate exclusiv pe prelucrarea automată dreptul de a depune o plângere la o autoritate de supraveghere art. 77 GDPR.
- Dreptul la o cale de atac judiciară competentă art. 78 GDPR.

➢ A fost desemnat prin decizie un responsabil cu protecția datelor cu caracter personal DPO
➢ S-a emis o decizie de către manager la propunerea DPO pentru realizarea unui audit privind situația existentă pentru a determina
  - tipul de date ce se prelucrează la nivelul organizației, în vederea cartografierii precum
  - și resursele umane necesare (lista persoanelor) care vor sprijini implementarea prevederilor Regulamentului.

➢ S-a decis realizarea echipei de documetare şi implementare a cerintelor RGPD. Au fost aleşi membri din toate compartimentele spitalului în care sunt prelucrate date. Fiecare membru al echipei are rolul de *a coordona* activităţile din compartimentele subordonate şi de *a-şi asuma responsabilităţi*, astfel încât proiectarea, implementarea, funcţionarea, monitorizarea periodică şi sistematică a activităţii de prelucrarea datelor să se desfăşoare în condiţii de legalitate. Se urmareste imbunatatirea continua a acestei activitați.

- Spitalul prelucrează numai datele cu caracter personal care sunt necesare pentru îndeplinirea scopurilor și numai în baza unor temeiuri legale
- Persoanele vizate (pacienți, salariați etc.) sunt informate cu privire la protecția datelor cu caracter personal
- Potrivit art. 33 alin. 5 RGPD, la nivelul spitalului există un registru al incidentelor de securitate ce cuprinde o descriere a situației de fapt în care a avut loc încălcarea securității datelor cu caracter personal, a efectelor acesteia și a măsurilor de remediere întreprinse.
- Angajații spitalului au fost instruiți pentru a înștiința echipa managerială fără întârzieri nejustificate după ce iau cunoștință de o încălcare a securității datelor cu caracter personal
- La nivelul spitalului este reglementată modalitatea de notificare a autorităților de supraveghere competente în termen de 72 de ore în caz de încălcare a securităților datelor. Potrivit art. 33 alin. 1 RGPD, în cazul în care are loc o încălcare a securității datelor cu caracter personal, operatorul notifică acest lucru autorității de supraveghere competente, fără întârzieri nejustificate și, dacă este posibil, în termen de cel mult 72 de ore de la data la care a luat cunoștință de aceasta, cu excepția cazului în care este puțin probabil să genereze un risc pentru drepturile și libertățile persoanelor fizice. În cazul în care notificarea către autoritate nu are loc în termen de 72 de ore, aceasta este însoțită de o explicație motivată pentru întârziere.
- Potrivit art. 34 alin. 1 RGPD, la nivelul spitalului este reglementată modalitatea de informare a persoanelor vizate în caz de încălcare a securității. Astfel, în cazul în care încălcarea securității datelor cu caracter personal este susceptibilă să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice, spitalul informează persoana vizată fără întârzieri nejustificate cu privire la această încălcare
- Spitalul adoptă măsuri de prevenire a pierderilor de date, atât pentru componentele hardware, cât și pentru aplicațiile software.
- Spitalul adoptă măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate ridicat, corespunzător riscurilor identificate în ceea ce privește gestionarea parolelor, condițiilor de folosire a porturilor USB de către angajați, protecția fizică a serverului, accesul restricționat prin user și parole, utilizarea adreselor de e-mail
- Rețeaua Wi-Fi la nivelul spitalului este securizată
- La nivelul spitalului există o inventariere a echipamentelor din rețeaua internă (laptop, computer desktop, server, telefon mobil, router, imprimantă) respectiv rețeaua externă pentru a identifica potențialele riscuri
- Dosarele care conțin documente și date cu caracter personal sunt depozitate în condiții de securitate și confidențialitate.
- Spitalul folosește antivirus pentru serverul de e-mail
- Spitalul criptează/protejează prin parole atașamentele din e-mailuri transmise
- Spitalul filtrează e-mailurile recepționate la nivelul spitalului pentru a reduce spam-ul și tentativele de phishing
- Spitalul a adoptat ca măsură de securitate pseudonimizarea (înlocuirea cu un pseudonim- ca o măsură de securitate) și criptarea datelor cu caracter personal
- Salariații sunt informați cu privire la faptul că este interzisă păstrarea actelor în orice alte locaţii (exemplu: domiciliul, autoturismul salariatului).
- Salariații sunt informați cu privire la faptul că transmiterea cu poșta a actelor institutiilor din afara localităţii în care îşi are sediul spitalul se va face doar cu scrisoare recomandată cu confirmare de primire.

(5) Pentru îndeplinirea prevederilor legale aferente și în vederea satisfacerii cerințelor păstrării în siguranță a datelor și informațiilor, *Spitalul Orășenesc „Sfânta Filofteia", Mizil* a elaborat și implementat măsuri organizatorice și tehnice orientate pe anumite direcții de acțiune.

7. RESPONSABILUL CU PROTECȚIA DATELOR

(1) Persoanele vizate au posibilitatea de a comunica în orice moment cu **Responsabilul pentru protecția datelor personale**, în mod direct, pentru orice subiect legat de prezenta Politică, utilizând date de contact de maijos:
Responsabil cu protecția datelor personale:
email: juridic@spitalmizil.ro
telefon: 0737505476

8. POLITICI SI PROCEDURI ASOCIATE

Prezenta politică trebuie interpretată împreună cu toate celelalte politici, proceduri, regulamente adoptate la nivelul spitalului în ceea ce privește protecția datelor cu caracter personal.

9. DISPOZIȚII FINALE

(1) Prezenta politică de securitate va fi disponibilă pe site-ul spitalului. Toți angajații vor fi informați cu privire la prezenta politică.
(2) Prezenta politică de securitate se completează și cu procedurile întocmite cu privire la prelucrarea datelor cu caracter personal.
(3) Încălcarea prevederilor prezentei politici constituie abatere disciplinară şi atrage răspunderea, potrivit legii.