



POLITICA GENERALĂ PRIVIND PRELUCRAREA ȘI PROTECȚIA DATELOR CU CARACTER PERSONAL LA NIVELUL INSTITUTULUI REGIONAL DE ONCOLOGIE IAȘI

I. SCOPUL POLITICII

Scopul prezentei Politici privind prelucrarea și protecția datelor cu caracter personal este de a asigura că Institutul Regional de Oncologie Iași, denumit în continuare **IRO Iași**, în calitate de operator de date cu caracter personal, precum și persoanele împuternicite de acesta respectă cerințele legale, statutare și de reglementare aplicabile în domeniul protecției datelor cu caracter personal.

Institutul Regional de Oncologie Iași, cu sediul în România, județul Iași, municipiul Iași, str. G-ral Henri Mathias Berthelot nr. 2-4, tel. 0374.278.810, fax 0374.278.802, e-mail: **manager@iroiasi.ro**, are calitatea de operator de date cu caracter personal pentru prelucrările efectuate în cadrul activităților sale.

Scopul Politicii este de a asigura respectarea prevederilor Regulamentului (UE) 2016/679 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date, precum și a legislației naționale aplicabile.

Prin prezenta Politică se stabilesc principiile, responsabilitățile, regulile și măsurile tehnice și organizatorice aplicabile în cadrul IRO Iași pentru:

- prelucrarea legală, echitabilă și transparentă a datelor cu caracter personal;
- protejarea drepturilor și libertăților persoanelor vizate;
- asigurarea confidențialității, integrității și disponibilității datelor cu caracter personal;
- prevenirea accesului neautorizat, pierderii, modificării, distrugerii sau divulgării neautorizate a datelor;
- limitarea accesului la date la persoanele care au atribuții de serviciu și o necesitate justificată de a cunoaște;
- prevenirea copierii, transferului sau extragerii neautorizate a datelor cu caracter personal din sistemele informatice ale IRO Iași;
- protejarea în mod special a datelor privind sănătatea și a celorlalte categorii speciale de date cu caracter personal prelucrate în cadrul activității medicale;
- gestionarea și raportarea incidentelor de securitate;
- asigurarea trasabilității operațiunilor relevante de prelucrare și transfer al datelor;
- aplicarea unor măsuri tehnice și organizatorice adecvate nivelului de risc asociat prelucrării;
- prevenirea utilizării neautorizate a dispozitivelor externe de stocare și controlul transferului de date între sistemele informatice ale IRO Iași și astfel de dispozitive.

Prezenta Politică se aplică tuturor sistemelor informatice, echipamentelor, aplicațiilor, bazelor de date, suporturilor de stocare și documentelor utilizate în cadrul IRO Iași, indiferent dacă acestea sunt în format electronic sau fizic.

II. DOMENIUL DE APLICARE

Prezenta Politică se aplică:

- conducerii IRO Iași;
- tuturor angajaților IRO Iași;
- personalului medical și personalului medico-sanitar;
- personalului administrativ și tehnic;
- medicilor colaboratori;



persoanei respective și care rezultă, în special, în urma analizei unei mostre de material biologic.

Date biometrice: date cu caracter personal care rezultă în urma unor tehnici de prelucrare specifice referitoare la caracteristicile fizice, fiziologice sau comportamentale ale unei persoane fizice, care permit sau confirmă identificarea unică a acesteia.

Date privind sănătatea: date cu caracter personal legate de sănătatea fizică sau mintală a unei persoane fizice, inclusiv date referitoare la prestarea de servicii de asistență medicală, care dezvăluie informații despre starea de sănătate a acesteia.

Autoritate de supraveghere: Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP), autoritate publică autonomă și independentă competentă în domeniul protecției datelor cu caracter personal în România.

Legislația privind protecția datelor: ansamblul actelor normative aplicabile prelucrării datelor cu caracter personal și protecției vieții private, inclusiv GDPR, legislația națională de punere în aplicare, precum și actele, deciziile, recomandările și orientările aplicabile emise de autoritățile competente.

GDPR: Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016.

Incident de securitate: orice eveniment sau situație care afectează sau poate afecta confidențialitatea, integritatea ori disponibilitatea datelor sau a sistemelor informatice și care poate conduce, după caz, la o încălcare a securității datelor cu caracter personal.

DPO: Responsabilul cu protecția datelor, desemnat în conformitate cu art. 37-39 din GDPR.

Dispozitiv extern de stocare: orice suport sau echipament utilizat pentru stocarea ori transferul de date în afara infrastructurii informatice interne, inclusiv stick USB, hard disk extern, card de memorie sau alte dispozitive similare.

IV. CADRUL LEGAL

Prezenta Politică se fundamentează pe legislația europeană și națională aplicabilă activității IRO Iași, în special:

1. Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor – GDPR);
2. Legea nr. 190/2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679, cu modificările și completările ulterioare;
3. Legea nr. 102/2005 privind înființarea, organizarea și funcționarea Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal, republicată, cu modificările și completările ulterioare;
4. Legea nr. 95/2006 privind reforma în domeniul sănătății, republicată, cu modificările și completările ulterioare;
5. Legea drepturilor pacientului nr. 46/2003, cu modificările și completările ulterioare;
6. Ordinul ministrului sănătății nr. 1.410/2016 privind aprobarea Normelor de aplicare a Legii drepturilor pacientului nr. 46/2003;
7. Ordonanța Guvernului nr. 124/1998 privind organizarea și funcționarea cabinetelor medicale, republicată, cu modificările și completările ulterioare, în măsura în care prevederile acesteia sunt aplicabile cabinetelor medicale organizate în cadrul IRO Iași, inclusiv structurilor medicale din cadrul Centrului de Screening;
8. Ordinul ministrului sănătății nr. 153/2003 pentru aprobarea Normelor metodologice privind înființarea, organizarea și funcționarea cabinetelor medicale, cu modificările



- și completările ulterioare, în măsura în care este aplicabil activităților și cabinetelor medicale din structura IRO Iași;
9. Legea nr. 16/1996 a Arhivelor Naționale, republicată, cu modificările și completările ulterioare, aplicabilă activităților de creare, evidență, păstrare, selecționare și arhivare a documentelor IRO Iași, inclusiv a documentelor care conțin date cu caracter personal;
 10. Legea nr. 53/2003 – Codul muncii, republicată, cu modificările și completările ulterioare, în ceea ce privește prelucrarea datelor cu caracter personal ale angajaților și ale candidaților;
 11. Legea nr. 333/2003 privind paza obiectivelor, bunurilor, valorilor și protecția persoanelor, republicată, cu modificările și completările ulterioare, în ceea ce privește măsurile de securitate și, după caz, prelucrarea imaginilor prin sisteme de supraveghere video;
 12. Hotărârea Guvernului nr. 301/2012 pentru aprobarea Normelor metodologice de aplicare a Legii nr. 333/2003, cu modificările și completările ulterioare;
 13. Legea contabilității nr. 82/1991, republicată, cu modificările și completările ulterioare, în ceea ce privește documentele financiar-contabile care pot conține date cu caracter personal;
 14. Ordinul ministrului finanțelor publice nr. 2.634/2015 privind documentele financiar-contabile, cu modificările și completările ulterioare, în măsura aplicabilității;
 15. Legea nr. 287/2009 privind Codul civil, republicată, cu modificările și completările ulterioare, în măsura în care dispozițiile acesteia sunt incidente activităților desfășurate de IRO Iași;
 16. Legea nr. 227/2015 privind Codul fiscal, cu modificările și completările ulterioare, în ceea ce privește prelucrarea datelor necesare îndeplinirii obligațiilor fiscale;
 17. Legea nr. 207/2015 privind Codul de procedură fiscală, cu modificările și completările ulterioare, după caz;
 18. Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice, cu modificările și completările ulterioare, în măsura în care este aplicabilă;
 19. actele normative aplicabile în domeniul arhivării electronice, evidenței și păstrării documentelor, în funcție de natura documentelor și a activităților desfășurate;
 20. deciziile, instrucțiunile, recomandările și ghidurile emise de Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP), în măsura în care sunt aplicabile activităților IRO Iași;
 21. alte acte normative europene și naționale aplicabile activităților desfășurate de IRO Iași și prelucrării datelor cu caracter personal, în funcție de domeniul și scopul prelucrării. Aplicarea prezentei Politici se realizează prin raportare la forma în vigoare a actelor normative menționate, precum și la orice alte dispoziții legale incidente activităților desfășurate de IRO Iași.

V. PRINCIPIILE PRELUCRĂRII DATELOR CU CARACTER PERSONAL

IRO Iași prelucrează datele cu caracter personal cu respectarea următoarelor principii:

1. legalitate, echitate și transparență;
2. limitarea scopului;
3. reducerea la minimum a datelor;
4. exactitatea datelor;
5. limitarea stocării;
6. integritatea și confidențialitatea;



7. responsabilitatea operatorului.
IRO Iași trebuie să poată demonstra respectarea principiilor prevăzute de Regulament.

VI. CATEGORII DE DATE CU CARACTER PERSONAL

În funcție de activitățile desfășurate, IRO Iași poate prelucra date aparținând următoarelor categorii de persoane:

- pacienți; angajați; candidați la angajare; aparținători și reprezentanți ai pacienților; colaboratori; studenți, rezidenți și persoane aflate în practică; furnizori și prestatori de servicii; reprezentanți ai autorităților și instituțiilor publice; vizitatori; alte persoane care interacționează cu IRO Iași.

Datele prelucrate pot include, după caz, date de identificare, date de contact, date profesionale, date financiar-contabile, date privind accesul în incintă, imagini video, date informatice și, în cazul pacienților și al personalului, date privind sănătatea. Datele privind sănătatea constituie categorie specială de date cu caracter personal și beneficiază de un nivel corespunzător de protecție.

VII. TEMEIUL JURIDIC AL PRELUCRĂRII

Prelucrarea datelor cu caracter personal se realizează numai în baza unui temei juridic aplicabil fiecărei activități de prelucrare.

În funcție de situație, temeiul poate fi:

- a. consimțământul persoanei vizate;
- b. executarea unui contract;
- c. îndeplinirea unei obligații legale;
- d. protejarea intereselor vitale;
- e. îndeplinirea unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice;
- f. interesul legitim, în condițiile prevăzute de Regulament.

În cazul categoriilor speciale de date, inclusiv al datelor privind sănătatea, se aplică suplimentar condițiile prevăzute de art. 9 din GDPR.

Consimțământul nu constituie temeiul implicit pentru toate prelucrările efectuate de IRO Iași.

În activitatea medicală și administrativă, prelucrarea se realizează, după caz, în baza obligațiilor legale, a interesului public în domeniul sănătății publice, a furnizării serviciilor medicale sau a altui temei juridic aplicabil.

VIII. RESPONSABILITĂȚI

1. MANAGERUL IRO IAȘI

- a. aprobă prezenta Politică și documentele subsecvente;
- b. dispune măsurile necesare pentru protecția datelor cu caracter personal;
- c. aprobă măsurile tehnice și organizatorice de securitate;
- d. stabilește responsabilitățile personalului;
- e. dispune instruirea personalului;
- f. aprobă, după caz, excepțiile de la măsurile de securitate stabilite prin prezenta Politică;
- g. dispune măsuri în cazul incidentelor de securitate;
- h. asigură resursele necesare implementării măsurilor de protecție a datelor.

2. RESPONSABILUL CU PROTECȚIA DATELOR (DPO)

- a. monitorizează respectarea prevederilor GDPR și a politicilor interne;
- b. oferă consiliere conducerii și personalului;

- c. monitorizează aplicarea măsurilor de protecție a datelor;
- d. monitorizează respectarea procedurii privind soluționarea solicitărilor persoanelor vizate și oferă consiliere în acest proces;
- e. participă la analiza incidentelor de securitate;
- f. formulează recomandări privind măsurile tehnice și organizatorice;
- g. cooperează cu autoritatea de supraveghere;
- h. efectuează verificări privind respectarea prezentei Politici.

3. RESPONSABILUL IT

- a. implementează măsurile tehnice de securitate aprobate;
- b. administrează sistemele informatice și drepturile de acces;
- c. implementează măsuri pentru prevenirea accesului neautorizat;
- d. asigură securizarea echipamentelor informatice;
- e. implementează măsuri de protecție împotriva programelor malware;
- f. gestionează, după caz, mecanismele de blocare și control al dispozitivelor USB;
- g. monitorizează funcționarea măsurilor tehnice de securitate;
- h. acordă acces la resursele informatice numai în baza drepturilor aprobate;
- i. participă la investigarea incidentelor de securitate;
- j. păstrează evidențele tehnice disponibile privind accesul și transferul de date, în limitele legii.

4. ANGAJAȚII ȘI COLABORATORII

- a. prelucrează datele numai în scop profesional;
- b. accesează numai datele necesare îndeplinirii atribuțiilor;
- c. păstrează confidențialitatea datelor;
- d. nu divulgă date către persoane neautorizate;
- e. nu utilizează conturile altor persoane;
- f. nu transmite date prin mijloace personale sau neautorizate;
- g. nu copiază date pe dispozitive personale;
- h. respectă regulile privind utilizarea dispozitivelor USB;
- i. raportează imediat orice incident sau suspiciune de incident;
- j. respectă toate instrucțiunile și măsurile tehnice și organizatorice stabilite de IRO Iași.

IX. POLITICA PRIVIND UTILIZAREA DISPOZITIVELOR USB ȘI A SUPTURILOR DE STOCARE EXTERNE

1. Regula generală

Având în vedere natura datelor prelucrate în cadrul IRO Iași, în special existența datelor privind sănătatea pacienților, utilizarea dispozitivelor externe de stocare reprezintă o activitate supusă unor restricții speciale.

Utilizarea dispozitivelor USB este interzisă în mod implicit, iar transferul de date pe suport USB este permis numai în situații excepționale, justificate profesional, aprobate și documentate, cu respectarea condițiilor prevăzute de prezenta Politică.

În consecință:

- a. nu este permisă conectarea stick-urilor USB personale la calculatoarele IRO Iași;
- b. nu este permisă conectarea hard diskurilor externe personale;
- c. nu este permisă conectarea telefoanelor mobile în scopul transferului de date;
- d. nu este permisă copierea datelor IRO Iași pe suporturi externe personale;



- e. nu este permisă transferarea documentelor, bazelor de date, imaginilor, fișierelor medicale sau altor informații de pe calculatoarele IRO Iași pe dispozitive externe neautorizate;
- f. nu este permisă utilizarea unui dispozitiv USB pentru extragerea datelor fără autorizare prealabilă;
- g. nu este permisă utilizarea suporturilor externe pentru prelucrarea datelor pacienților în afara infrastructurii informatice aprobate a IRO Iași.

Această măsură are ca scop reducerea riscului de pierdere, copiere, divulgare, modificare, infectare cu programe malware sau acces neautorizat la datele prelucrate de IRO Iași.

2. Calculatoarele autorizate pentru utilizarea dispozitivelor USB

Prin excepție de la regula generală, IRO Iași poate desemna un număr limitat de calculatoare la care utilizarea dispozitivelor USB este permisă. Calculatoarele respective vor fi stabilite printr-o listă aprobată de Managerul IRO Iași și administrată de structura IT.

Lista va conține cel puțin:

- a. identificarea calculatorului;
- b. locația;
- c. structura/compartimentul;
- d. scopul pentru care este permisă utilizarea USB;
- e. persoanele autorizate;
- f. tipul dispozitivelor USB acceptate;
- g. eventualele condiții suplimentare de utilizare.

Faptul că un calculator este autorizat pentru utilizarea USB nu conferă automat tuturor utilizatorilor dreptul de a copia date pe dispozitive externe.

3. Persoanele autorizate

Accesul la funcția USB poate fi acordat numai persoanelor care au o necesitate profesională justificată.

Autorizarea se realizează cu aprobarea conducerii IRO Iași, la propunerea structurii interesate și cu implementarea tehnică de către IT.

Pentru fiecare persoană autorizată se va stabili, după caz:

- a. scopul utilizării;
- b. tipul datelor care pot fi transferate;
- c. tipul dispozitivului acceptat;
- d. perioada autorizării;
- e. calculatorul/calculatoarele pe care este permisă utilizarea.

4. Dispozitive USB aprobate

În situațiile în care transferul pe suport extern este necesar pentru îndeplinirea atribuțiilor de serviciu, vor fi utilizate numai dispozitive aprobate de IRO Iași.

Utilizarea stick-urilor USB personale este interzisă.

Atunci când natura datelor o impune, dispozitivele aprobate vor fi protejate prin măsuri suplimentare, inclusiv criptare și/sau parolă.

5. Copierea datelor

Copierea datelor de pe calculatoarele IRO Iași pe un suport extern este permisă numai dacă:

- a. există o necesitate profesională justificată;
- b. persoana este autorizată;
- c. calculatorul este inclus în lista calculatoarelor autorizate;
- d. suportul extern este aprobat de IRO Iași;



- e. datele copiate sunt strict cele necesare;
- f. transferul este realizat în scop profesional și legal;
- g. sunt respectate măsurile tehnice și organizatorice stabilite de IT și DPO.

Copierea integrală a bazelor de date, dosarelor pacienților sau a altor categorii extinse de date nu este permisă decât dacă există o justificare profesională și legală și o autorizare expresă.

6. Copierea datelor pe dispozitive personale

Este strict interzisă copierea sau transferarea datelor cu caracter personal ale IRO Iași pe:

- a. stick-uri personale;
- b. hard diskuri personale;
- c. telefoane personale;
- d. calculatoare personale;
- e. conturi personale de e-mail;
- f. servicii personale de stocare în cloud;
- g. alte dispozitive sau servicii care nu sunt aprobate de IRO Iași.

Interdicția se aplică indiferent dacă datele respective sunt sau nu date privind sănătatea.

7. Utilizarea dispozitivelor USB pentru transmiterea documentelor

Atunci când documentele pot fi transmise prin mijloace informatice securizate puse la dispoziție de IRO Iași, se va utiliza cu prioritate această modalitate, fără copierea pe suport USB. Transferul pe suport USB va constitui o soluție excepțională, justificată de necesitatea activității.

8. Detectarea utilizării neautorizate

IRO Iași poate utiliza măsuri tehnice pentru:

- a. blocarea porturilor USB;
- b. permiterea accesului numai pentru dispozitive autorizate;
- c. identificarea dispozitivelor conectate;
- d. restricționarea copierii datelor;
- e. monitorizarea evenimentelor de securitate;
- f. prevenirea introducerii unor dispozitive care pot afecta securitatea sistemelor informatice.

Încercarea de eludare a măsurilor tehnice de securitate este interzisă.

X. SECURITATEA SISTEMELOR INFORMATICE

IRO Iași implementează măsuri tehnice și organizatorice adecvate riscurilor identificate.

Acestea pot include:

- a. autentificarea utilizatorilor;
- b. parole individuale;
- c. controlul accesului în funcție de atribuții;
- d. antivirus și soluții de protecție împotriva programelor malware;
- e. actualizarea sistemelor;
- f. backup și proceduri de restaurare;
- g. criptarea datelor, acolo unde este necesar;
- h. blocarea dispozitivelor externe neautorizate;
- i. monitorizarea evenimentelor de securitate;
- j. protecția fizică a echipamentelor;
- k. segmentarea și securizarea rețelelor;
- l. testarea periodică a măsurilor de securitate.

XI. UTILIZAREA CONTURILOR DE E-MAIL INSTITUȚIONALE

Conturile de e-mail instituționale sunt destinate exclusiv desfășurării activității profesionale. Utilizarea acestora în scopuri personale este interzisă.

Transmiterea automată a mesajelor e-mail este permisă numai în scop profesional și prin soluții informatice aprobate de IRO Iași, cu respectarea cerințelor de securitate, a drepturilor de acces și a instrucțiunilor stabilite de instituție.

Utilizarea mecanismelor de automatizare care implică prelucrarea datelor cu caracter personal se realizează cu respectarea Procedurii privind utilizarea sistemelor informatice a IRO Iași și a măsurilor tehnice și organizatorice aplicabile.

XII. CONFIDENȚIALITATEA ȘI CONTROLUL ACCESULUI

Accesul la date se acordă numai persoanelor autorizate și numai în măsura în care accesul este necesar pentru îndeplinirea atribuțiilor de serviciu.

Este interzis:

- a. utilizarea contului altui angajat;
- b. transmiterea parolei către alte persoane;
- c. lăsarea nesupravegheată a unui calculator conectat la sistem;
- d. fotografierea ecranului cu telefonul personal în situațiile în care sunt afișate date personale, dacă acest lucru nu este necesar și autorizat;
- e. copierea documentelor în scop personal;
- f. transmiterea documentelor către adrese personale de e-mail;
- g. utilizarea unor servicii cloud personale pentru stocarea documentelor IRO Iași.

XIII. INCIDENTE DE SECURITATE ȘI ÎNCĂLCAREA SECURITĂȚII DATELOR

Orice persoană care constată sau suspectează un incident de securitate are obligația de a-l raporta imediat conform procedurii interne privind gestionarea incidentelor de securitate.

Constituie incidente, inclusiv:

- a. pierderea unui dispozitiv care conține date personale;
- b. conectarea unui stick neautorizat;
- c. copierea neautorizată a datelor;
- d. transmiterea accidentală a unui document către un destinatar greșit;
- e. accesarea neautorizată a unui sistem;
- f. pierderea sau furtul unui calculator;
- g. divulgarea accidentală a datelor;
- h. infectarea unui sistem informatic;
- i. utilizarea unui suport extern neautorizat;
- j. orice situație care poate conduce la compromiterea confidențialității, integrității sau disponibilității datelor.

Personalul are obligația de a raporta incidentul fără întârziere și, în conformitate cu regulile interne ale IRO Iași, în termen de maximum 24 de ore de la momentul luării la cunoștință. Termenul intern de 24 de ore nu înlocuiește și nu modifică termenul legal de 72 de ore prevăzut de art. 33 GDPR pentru notificarea autorității de supraveghere.

XIV. DREPTURILE PERSOANELOR VIZATE

Persoanele vizate pot exercita, după caz și în condițiile prevăzute de GDPR și de legislația aplicabilă, următoarele drepturi:



- a. dreptul de acces;
- b. dreptul la rectificare;
- c. dreptul la ștergerea datelor;
- d. dreptul la restricționarea prelucrării;
- e. dreptul la portabilitatea datelor;
- f. dreptul la opoziție;
- g. dreptul de retragere a consimțământului, atunci când prelucrarea se bazează pe consimțământ;
- h. drepturile referitoare la procesul decizional automatizat și crearea de profiluri, în condițiile legii.

Exercitarea acestor drepturi se realizează prin transmiterea unei solicitări către IRO Iași, conform procedurii interne privind exercitarea drepturilor persoanelor vizate.

XV. DURATA PĂSTRĂRII DATELOR

Datele cu caracter personal sunt păstrate pentru perioada stabilită de legislația aplicabilă, de nomenclatorul arhivistic, de obligațiile financiar-contabile, de obligațiile medicale și de celelalte acte normative aplicabile fiecărei categorii de documente.

IRO Iași nu va păstra date cu caracter personal pentru o perioadă mai lungă decât cea necesară, cu excepția situațiilor în care există o obligație legală de păstrare sau un alt temei juridic aplicabil.

Perioadele de păstrare se stabilesc distinct pentru fiecare categorie de documente și activitate de prelucrare.

XVI. TRANSFERUL ȘI DIVULGAREA DATELOR

Datele cu caracter personal pot fi transmise numai către destinatari care au dreptul legal sau contractual de a le primi.

Pot fi destinatari, după caz:

- a. autorități și instituții publice;
- b. autorități din domeniul sănătății;
- c. case de asigurări de sănătate;
- d. organe judiciare;
- e. furnizori și prestatori de servicii;
- f. persoane împuternicite;
- g. alte entități, atunci când transmiterea este justificată legal.

Transmiterea datelor se realizează prin mijloace adecvate nivelului de risc.

XVII. PRELUCRAREA DATELOR DE CĂTRE PERSOANE ÎMPUTERNICITE

IRO Iași va utiliza numai persoane împuternicite care oferă garanții suficiente privind implementarea măsurilor tehnice și organizatorice adecvate.

Relația cu persoanele împuternicite va fi reglementată contractual, în condițiile art. 28 GDPR. Persoanele împuternicite nu vor putea utiliza datele în alte scopuri decât cele stabilite de IRO Iași.

XVIII. INSTRUIREA PERSONALULUI

Personalul care prelucrează date cu caracter personal va fi instruit cu privire la:

- a. obligațiile privind confidențialitatea;
- b. principiile GDPR;
- c. utilizarea sistemelor informatice;



- d. gestionarea parolelor;
- e. identificarea incidentelor;
- f. transmiterea datelor;
- g. utilizarea dispozitivelor externe;
- h. interdicția utilizării suporturilor personale;
- i. obligațiile privind raportarea incidentelor.

Instruirea va fi documentată.

XIX. CONTROLUL RESPECTĂRII POLITICII

Respectarea prezentei Politici poate fi verificată periodic de persoanele desemnate de conducerea IRO Iași.

Verificările pot include:

- a. verificarea drepturilor de acces;
- b. verificarea calculatoarelor autorizate pentru USB;
- c. verificarea aplicării restricțiilor privind dispozitivele externe;
- d. verificarea incidentelor de securitate;
- e. verificarea instruirii personalului;
- f. verificarea respectării procedurilor interne;
- g. verificarea măsurilor tehnice implementate de IT.

Rezultatele verificărilor pot sta la baza unor măsuri corective sau preventive.

XX. NERESPECTAREA POLITICII

Nerespectarea prezentei Politici poate conduce la aplicarea măsurilor administrative, disciplinare, contractuale sau, după caz, juridice prevăzute de legislația aplicabilă și de regulamentele interne ale IRO Iași.

Constituie încălcări, inclusiv:

- a. conectarea unui stick personal la un calculator IRO Iași;
- b. copierea neautorizată a datelor;
- c. transmiterea datelor către conturi personale;
- d. utilizarea unui dispozitiv extern neautorizat;
- e. dezactivarea sau ocolirea măsurilor tehnice de securitate;
- f. divulgarea neautorizată a datelor;
- g. utilizarea datelor în scop personal;
- h. neinformarea cu privire la un incident de securitate.

XXI. EXCEPȚII

Excepțiile de la prezenta Politică se aprobă numai în situații justificate și documentate.

În cazul utilizării dispozitivelor USB, excepția trebuie să precizeze cel puțin:

- a. persoana autorizată;
- b. calculatorul autorizat;
- c. dispozitivul autorizat;
- d. scopul transferului;
- e. categoria de date care poate fi transferată;
- f. perioada pentru care este valabilă autorizarea.

Excepțiile nu pot conduce la eliminarea obligațiilor privind confidențialitatea și securitatea datelor.



XXII. DOCUMENTE ASOCIATE

Prezenta Politică se aplică împreună cu:

- a. Procedura de sistem privind protecția datelor cu caracter personal;
- b. Registrul incidentelor de securitate;
- c. Formularul de raportare a incidentului de securitate;
- d. Angajamentul de confidențialitate;
- e. Nota de informare a angajaților;
- f. Nota de informare a pacienților;
- g. Regulamentul privind utilizarea sistemelor informatice;
- h. lista calculatoarelor autorizate pentru utilizarea dispozitivelor USB;
- i. documentele privind autorizarea utilizării suporturilor externe.

XXIII. DISPOZIȚII FINALE

Prezenta Politică este obligatorie pentru toate persoanele cărora li se aplică.

Prevederile acesteia se aduc la cunoștința personalului prin instruire, afișare, comunicare electronică sau prin alte mijloace stabilite de conducerea IRO Iași.

Politica va fi revizuită ori de câte ori intervin modificări legislative, organizaționale, tehnologice sau atunci când rezultatele evaluărilor de risc impun modificarea măsurilor de protecție.

Prezenta Politică intră în vigoare la data aprobării de către Managerul IRO Iași.

APROBAT,
Manager,
Ec. Mirela GROSU

