POLITICA GENERALĂ

PRIVIND

SECURITATEA PRELUCRĂRII DATELOR CU CARACTER PERSONAL

ÎN SPITALUL JUDEȚEAN DE URGENȚĂ BACĂU

SCOPUL POLITICII

Scopul acestei politici generale privind securitatea prelucrării datelor cu caracter personal din cadrul SJU BACĂU este de a crea un mediu sigur și încrezător, în vederea prevenirii și protejării împotriva amenințărilor de securitate, precum și pentru asigurarea continuității activității în contextul protecției și securității datelor cu caracter personal, în conformitate cu Regulamentul General privind Protecția Datelor (GDPR).

Politica include reglementarea utilizării internetului și a poștei electronice, securizarea fizică a mediului de lucru, respectarea reglementărilor privind securitatea fizică, instruirea utilizatorilor în responsabilitățile asociate protecției fizice a datelor cu caracter personal, menținerea integrității, cofidențialității și disponibilității informațiilor și a datelor cu caracter personal, efectuarea de back-up și restaurarea datelor în caz de incidente, reglementarea utilizării dispozitivelor electronice mobile, stabilirea regulilor de acces la datele cu caracter personal și sistemele de prelucrare a acestora și managementul continuității activității privind securitatea datelor cu caracter personal. Această abordare comprehensivă are ca scop cultivarea unei culturi a securității datelor și încrederii printre angajații instituției.

DOMENIUL DE APLICARE

Domeniul de aplicare al acestei politici include toți angajații care sunt autorizați în prelucrarea datelor cu caracter personal în cadrul SJU BACĂU.
Prezenta politică va fi considerată ca având caracter general și se va aplica tuturor prelucrărilor efectuate de SJUB , în calitate de Operator de date cu caracter personal.

DESCRIEREA POLITICII

Prezenta politică are ca scop asigurarea integrității, confidențialității și disponibilității informației și a datelor cu caracter personal în cadrul SJU BACĂU.

Prezenta politică își propune asigurarea securității prelucrării datelor cu caracter personal prin abordarea a șapte mecanisme diferite:

- **Securitatea utilizării e-mailului și a internetului**
- **Securitatea mediului de lucru**
- **Copiile de siguranță a informației**
- **Utilizarea dispozitivelor mobile**
- **Controlul accesului la date cu caracter personal**
- **Practica birou curat – ecran curat**
- **Managementul continuității activității privind securitatea datelor cu caracter personal**

I. SECURITATEA UTILIZĂRII E-MAILULUI ȘI A INTERNETULUI

Securitatea este responsabilitatea fiecăruia.

Fiecare utilizator este obligat să verifice confidențialitatea datelor primite sau transmise.

Utilizatorii trebuie să folosească poșta electronică a instituției numai în beneficiul SJUB.

Când angajații SJUB utilizează poșta electronică trebuie să respecte următoarele reguli:

Este permis:

- Verificarea e- mailul zilnic pentru a verifica dacă există mesaje noi;
- Înainte de a transmite un e-mail, utilizatorii se vor asigura privind adresa la care doresc să transmită acel e-mail ca fiind cea corectă, prin dubla verificare a adresei de e-mail în FOCG/FSZ/Sistemul informtic, etc.;
- Utilizatorii vor folosi semnătura standard a instituției pentru a semna toate e-mailurile de serviciu.

Nu este permis:

- Listarea e-mailurilor, decât dacă acest lucru este necesar pentru desfășurarea activității;
- Utilizarea e-mailului în scopuri personale;
- Deschiderea e-mailurilor de tip SPAM;
- Deschiderea linkurilor sau a atașamentelor de la persoane necunoscute;
- Trimiterea, retrimiterea sau primirea de informații confidențiale sau date cu caracter personal ce privesc SJUB, folosind conturi utilizator care nu sunt proprietatea Spitalului. Exemple de astfel de conturi, sunt (dar nu sunt limitate numai la acestea: Gmail, Hotmail, Yahoo mail, AOL mail), precum și adrese de email puse la dispoziție de alți Furnizori de Servicii Internet;
- Răspunderea la mesajele de e-mail care solicită o schimbare a parolei și solicită să informații personale, indiferent cât de oficială pare sursa;
- Transmiterea e-mailurilor ce conțin materiale pentru adulți, sau ce conțin informații despre droguri, rasism, terorism, violență;
- Trimiterea de mesaje cu caracter de intimidare sau hărțuire;
- Încercarea logării cu ID-ul si parola altcuiva;
- Folosirea conturilor de mail internet base (gen gmail, yahoo).

Reguli utilizare Internet

Trebuie (Este permis):

- Trebuie folosit internetul doar în interes de serviciu;
- Programele pentru acces la rețeaua Internet sunt destinate utilizatorilor autorizați pentru a fi folosite exclusiv în scopuri de serviciu;
- Trebuie verificat dacă orice informație folosită este corectă, actuală și completă (de. ex. utilizarea site-urilor oficiale ale instiuțiilor publice, platforme informatice oficiale – Lege5.ro, CaPeSaRo, etc);
- Trebuie respectate legile dreptului de autor referitoare la informația, software-ul, etc găsite și utilizate (de ex. pentru personalul care utilizează/prelucrează informații/documente cu restricții de copiere/difuzare).

Nu trebuie (Nu este permis):

- Nu este permisă folosirea internetului în scop personal;
- Nu este permis accesul la site-uri cu conținut pentru adulți sau ce conțin informații despre droguri, rasism, terorism, violenta, etc;
- Nu este permisă descărcarea și instalarea pe calculator a software-lor (programelor) de pe internet;
- Nu este permisă utilizarea computerelor aparținând SJUB pentru accesul neautorizat în alte calculatoare sau rețele;
- Nu este permisa utilizarea identității altei persoane.

Reguli utilizarea mediilor de stocare mobile (Memory Stick USB, Hard disk extern, CD, etc.)

Reguli de bună practică:

- Mediile pe care a fost stocat back-up-ul trebuie să fie depozitate într-o locație sigură;
- Este interzisă utilizarea mediilor de stocare mobile în cadrul instituției fără acordul conducerii unității;
- Accesul la mediile pe care se face salvarea (back-up-ul) trebuie să fie controlat (backup-ul va fi făcut de către o persoană autorizată);
- Este interzisa scoaterea din cadrul instituției a mediilor de stocare mobile. Dacă este necesar scoaterea acestora, scoaterea se va face pe baza unei autorizări, și vor trebui păstrate înregistrări cu aceste evenimente;
- Toate mediile de stocare mobile trebuie înregistrate pentru a se limita posibilitatea pierderii informațiilor;
- Toate mediile de stocare trebuie să fie marcate cu un nivel de confidențialitate, să se țină evidență a celor care au voie să le vadă, iar copiile să fie etichetate cu persoanele care le pot accesa. Nivelul de confidențialitate se referă la gradul de sensibilitate și importanță al informațiilor. Cu cât un nivel de confidențialitate este mai ridicat, cu atât informațiile sunt considerate mai sensibile și mai importante pentru securitatea și integritatea unei entități.

Iată câteva exemple de niveluri de confidențialitate:

- Public: Informațiile publice sunt acele date care nu conțin informații sensibile și care pot fi făcute disponibile publicului larg fără riscuri majore.
- Intern: Informațiile interne sunt destinate utilizării și accesului restricționat la membrii unei instituții sau grup restrâns. Deși pot fi sensibile pentru instituție, nu prezintă riscuri mari dacă sunt accesate de persoanele autorizate.
- Confidențial: Informațiile confidențiale sunt sensibile și necesită protecție împotriva accesului neautorizat. Ele pot include, de exemplu, date personale, informații financiare sau strategice ale instituției.
- Mediile de stocare vor trebui depozitate conform specificațiilor producătorului, de exmplu: atunci când cumperi sau utilizezi un mediu de stocare, cum ar fi un disc dur, un stick USB sau un server, producătorul furnizează adesea instrucțiuni și recomandări pentru depozitarea și utilizarea corectă a acestuia. Aceste specificații includ de obicei informații despre temperatură, umiditate,

manipulare și alte condiții de mediu ideale pentru ca mediul de stocare să funcționeze în mod optim.

Responsabilitatea Utilizatorilor resurselor informatice:

- Fiecare utilizator este responsabil pentru securitatea informațiilor și datelor cu caracter personal pe care le deține și utilizează. Securitatea este responsabilitatea fiecăruia;
- Fiecare utilizator este obligat să verifice confidențialitatea datelor;
- Utilizatorii trebuie sa folosească resursele puse la dispoziție numai in beneficiul SJUB
- Fiecare utilizator este responsabil pentru ceea ce face in cadrul sistemului informatic;
- Dacă se observă ceva neobișnuit (neconformitate, potențial risc, incident), utilizatorul trebuie să anunțe superiorul direct sau DPO-ul.

II. SECURITATEA MEDIULUI DE LUCRU

Zonele de securitate fizică sunt protejate prin măsuri corespunzătoare de control al accesului pentru a se asigura că accesul fizic în instituție este permis doar personalului autorizat.

Perimetrul fizic al clădirii sau al amplasamentelor unde se găsesc echipamente de procesare a informației/datelor cu caracter personal sunt izolate fizic. Pereții exteriori ai clădirii sunt o construcție solidă și toate ușile exterioare sunt protejate împotriva accesului neautorizat prin intermediul mecanismelor de control, încuietori etc. Arhiva este protejată fizic în conformitate cu reglementările interne și cu prevederile legale în vigoare.

Ușile și ferestrele de la birouri, în special de la conducerea instituției și arhiva sunt încuiate în absența personalului. La terminarea programului toate locațiile vor fi încuiate. În timpul programului, lăsarea biroului descuiat fără prezenta personalului, va fi considerat incident de securitate.

Informațiile confidențiale și datele cu caracter personal, documentele de valoare, contractele etc., nu vor fi lăsate pe birouri, ci vor fi așezate corespunzător în fișete, dulapuri, sertare, protejate împotriva sustragerilor, incendiilor, inundațiilor.

Orice eveniment/incident legat de securitatea instituției și a personalului va fi raportat și consemnat, iar atunci când gravitatea acestuia impune va fi raportat conducerii instituției împreună cu corecțiile și acțiunile corective ce se impun a fi luate.

Angajații care observă dispariția unor documente, informații etc. din birouri sunt obligați să raporteze și coordonatorului structurii și să contacteze responsabilul pentru protecția datelor în situația în care sunt implicate date cu caracter personal.

Securitatea echipamentelor

Prevenirea pierderii, avarierii, furtului sau compromiterea echipamentelor și întreruperea activităților de prelucrare din cadrul instituției:

- echipamentele trebuie sa fie amplasate și protejate astfel încât să se reducă riscurile fata de amenințările și pericolele de mediu și față de posibilitatea de acces neautorizat;
- echipamentele trebuie sa fie protejate împotriva penelor de curent sau a altor întreruperi cauzate de probleme ale utilităților suport;

- cablurile de alimentare cu energie electrică și telecomunicații purtătoare de date sau servicii de suport pentru informație trebuie protejate față de interceptări, interferente și avarii;
- echipamentele trebuie sa fie corect întreținute pentru a se asigura disponibilitatea continua și integritatea acestora;
- echipamentele, produsele software sau datele cu caracter personal nu trebuie scoase în afara spațiului de lucru fără o autorizare prealabilă;
- utilizatorii trebuie sa se asigure că echipamentele nesupravegheate au o protecție corespunzătoare;
- respectarea cerințelor privind asigurarea biroului curat pentru hârtii și medii de stocare letrice și asigurarea ecranului curat pentru mijloacele electronice de prelucrare a datelor cu caracter personal;

se va acorda atenție ținerii în siguranță a echipamentelor IT, în special a dispozitivelor mobile (Laptopuri, tablete și telefoane mobile), securității dispozitivelor personale folosite in activitatea profesională.

III. COPIILE DE SIGURANȚĂ A INFORMAȚIEI

Pentru aplicațiile și bazele de date de pe serverele din cadrul SJUB există o soluție de back-up total și restaurare a datelor. Salvarea datelor se face pe 2 hard-disk-uri astfel externe, în mod încrucișat, serverele aflându-se în locații diferite.

Testarea copiilor de siguranță și realizarea unei restaurări de verificare completă a datelor se va efectua la fiecare 3 luni de către administratorul de sistem IT.

Mesajele de poștă electronică primite/transmise sunt descărcate în profilele utilizatorilor unde se păstrează și arhivează. Pentru mesajele email nu se face back-up.

Documentele pe suport hârtie care nu se află în uz, se păstrează în dosare, se arhivează și se depozitează în arhiva instituției.

Documentele păstrate în arhiva sunt trecute într-un Registru al arhivei pentru o regăsire facilă. Camera este protejată împotriva accesului fizic, iar ușa de la intrare este închisă permanent.

Predarea/primirea documentelor din/în arhiva se face pe bază de semnături și consemnarea acestora în Registrul arhivei.

Durata de păstrare a documentelor în arhiva este propusă de către deținător și aprobată de șeful ierarhic. După depășirea duratei de arhivare, documentele arhivei sunt distruse prin tocare de către o firmă autorizată, după aprobarea unei comisii pe bază de proces verbal.

IV. UTILIZAREA DISPOZITIVELOR MOBILE

Pentru a asigura securitatea informațiilor și a datelor cu caracter personal prelucrate de către SJUB, angajații autorizați să folosească echipamente proprii trebuie să aibă instalat pe dispozitive mobile personale software anti-virus și de management al dispozitivelor mobile (MDM). Aceste software-uri au scopul de stoca pe dispozitiv toate informațiile legate de instituție, inclusiv calendarele, e-mailurile și

alte aplicații într-o zonă securizată protejată prin parolă. SJUB trebuie să instaleze acest software înainte de a se utiliza dispozitivul personal în scopuri de lucru.

Angajații nu trebuie să utilizeze aplicații bazate pe cloud sau copii de rezervă care să permită transferul datelor legate de instituție către terți. Efectuarea oricăror modificări ale hardware-ului sau ale software-ului aparatului în afară actualizărilor de instalare autorizate și de rutină este interzisă.

Angajații nu trebuie să folosească pe dispozitivele electronice personale mobile servicii de mesagerie online (exemplu: WhatsApp, Facebook Messenger, Telegram s.a.m.d) în desfășurarea activității profesionale care presupune/implică utilizarea/prelucrarea datelor cu caracter personal.

Angajații ale căror dispozitive personale au capacități de cameră video sau de înregistrare nu vor utiliza aceste funcții în interiorul instituției.

Accesul la resursele informatice și informaționale ale SJUB se va realiza doar prin soluții securizate și aprobate de către instituție, traficul va fi monitorizat și utilizatorul va fi tras la răspundere dacă va utiliza necorespunzător sau abuziv aceste resurse.

Utilizatorul nu are dreptul și îi este strict interzis să depoziteze pe dispozitivul personal date cu caracter personal ale SJUB.

În ceea ce privește materialele elaborate de utilizatori în interesul instituției, este interzisă orice formă de reproducere, utilizare parțială sau totală sau transmitere a acestora unor terți - persoane neautorizate, fără acordul scris al conducerii spitalului.

Un angajat nu poate să stocheze informațiile prelucrate de către SJUB pe calculatoarele proprii, pe stickuri de memorie, pe carduri de memorie, pe hard discuri externe, pe CD-uri sau dv-duri, în contul de email.

Numele conturilor, parolele contului sau datele de conectare la rețeaua internă a SJUB nu trebuie divulgate nimănui.

În cazul întreruperii raporturilor de muncă, angajatul este obligat să prezinte SJUB echipamentul pentru a fi eliminate datele cu caracter personal, aplicațiile, informațiile și conexiunile la rețeaua SJUB.

Angajatul va permite și accepta instalarea soluțiilor de criptare, soluțiilor antivirus și de acces la distanță agreate de SJUB incluzând aplicații pentru a putea proteja datele cu caracter personal și celelalte informații ale SJUB aflate pe dispozitiv.

Angajatul se obligă să raporteze pierderea sau furtul oricărui dispozitiv personal care a fost activat pentru utilizarea în interes de serviciu către superiorul ierarhic, responsabilul IT, DPO-ul și celei mai apropiate secții de Poliție, în termen de maxim 24 de ore.

SJUB are dreptul, în orice moment, să monitorizeze și să păstreze orice comunicații care se desfășoară în cadrul instituției, precum transferul de date, mesageria vocală, jurnalele de telefon, utilizarea Internetului și traficul în rețea.

În plus, niciun angajat nu poate să dezactiveze cu bună știință niciun software sau sistem de rețea identificat ca instrument de monitorizare și securizare.

Angajații au responsabilitatea să protejeze dispozitivele personale utilizate în interesul SJUB pentru a evita pierderea, distrugerea sau furtul echipamentului.

Pentru a asigura confidențialitatea datelor instituției, angajații trebuie să aibă instalat pe dispozitivul

mobil personal un software de tip "remote-wipe", instalat de către responsabilul IT înainte de utilizarea dispozitivele în scopuri de lucru. Acest software permite ca datele legate de instituție să fie șterse de la distanță în cazul pierderii sau furtului dispozitivului. Ștergerea datelor instituției poate afecta alte aplicații și date.

Angajații trebuie să notifice imediat conducerea SJUB în cazul în care dispozitivul personal este pierdut, furat sau deteriorat.

În cazul demisiei sau încetării contractului de muncă toate datele instituției vor fi eliminate de către responsabilul IT de pe dispozitivele mobile personale.

Angajații care nu au primit autorizație în scris de la conducerea SJUB nu vor avea permisiunea de a utiliza dispozitive personale în îndeplinirea responsabilităților ce îi revin conform contractului de muncă.

Nerespectarea politicilor SJUB poate conduce la acțiuni disciplinare, inclusiv la încetarea contractului de muncă.

V. CONTROLUL ACCESULUI LA DATE CU CARACTER PERSONAL

Înregistrarea / dezactivarea utilizatorului

Înregistrarea utilizatorului în sistemele de procesare a informației și a datelor cu caracter personal se face după angajarea acestora în cadrul instituției. După comunicarea administratorului IT a datelor de identificare ale noului utilizator (nume, prenume, departament şi drepturi de acces), administratorul IT va crea un cont de poștă electronică pe serverul e-mail al instituției și un cont pentru aplicațiile software din cadrul instituției.

Contul de poștă electronică va fi de tipul: nume.prenume@spitaluljudeteanbacau.ro.

La suspendarea/încetarea contractului de muncă, respectiv la reluarea activității sau la angajare, șeful compartimentului informează administratorul IT în vederea suspendării/alocării, după caz, a contului asociat utilizatorului respectiv. După plecarea angajatului, accesarea datelor din contul de utilizator se va face numai de către șeful ierarhic al utilizatorului pentru o perioadă de maxim 12 luni, apoi pot fi șterse de către administratorul IT. Administratorul IT va ține evidenta conturilor utilizator (nume, drepturi, dată creare, dată suspendare).

Este interzis accesul altei persoane la resursele rețelei prin folosirea contului şi a parolei unui angajat.

Utilizarea parolelor

Toți utilizatorii trebuie sa urmeze următoarele bune practici de securitate în ceea ce privește selecția și utilizarea parolelor. Aceste practici sunt:

- să selecteze parole de calitate: lungimea parolei este de minim 8 caractere si va conține minim o litera mare, minim un caracter special și minim o cifră;
- să nu conțină caractere identice consecutive;
- să nu se bazeze pe ceva ușor de dedus sau de obținut pe baza datelor personale sau familiare, de exemplu, nume si prenume, date de naștere, numere de telefon sau de autoturism etc.
- dacă există suspiciunea că parola a fost divulgată sau compromisă aceasta trebuie schimbată imediat prin contactarea administratorului IT;

- să nu utilizeze aceeași parolă, atât pentru scopuri profesionale, cât și personale;
- să păstreze confidențialitatea parolei (să nu o scrie pe biletele, birouri, tastaturi, monitoare etc.);
- să nu salveze automat parolele in aplicațiile instalate (de exemplu, webmail).

Echipament nesupravegheat de către utilizatori

Utilizatorii trebuie să se asigure că echipamentul de prelucrare a informației și a datelor cu caracter personal de la locul de muncă lăsat nesupravegheat este protejat corespunzător, prin efectuarea următoarelor acțiuni:

- la terminarea programului de lucru se va închide echipamentul şi sesiunea de lucru printr-o politică de log-off/shutdown/lock, precum şi monitorul;
- se va activa, la maxim 10 minute de inactivitate, un screen saver ce va solicita parola la repornirea sesiunii de lucru;
- imprimantele şi copiatorul vor fi pornite permanent şi se află în responsabilitatea deținătorilor;
- după tipărire, utilizatorii își vor lua imediat din imprimantă documentele proprii, în caz contrar acestea pot fi distruse de către responsabilul echipamentului;
- corespondența şi faxurile vor fi primite/trimise la/de la locurile stabilite în instituție.

Identificarea si autentificarea utilizatorului

Toți utilizatorii vor trebui să se autentifice cu un username şi parola înainte de a iniția sesiuni la rețea.

Autentificarea în rețea cu username-ul şi parola altui utilizator este strict interzisă şi va fi considerată incident de securitate. Responsabilitatea acestei acțiuni revine atât asupra persoanei care a efectuat operațiunea cât şi asupra celei care a divulgat parola asociată contului propriu.

Prelucrări manuale de date cu caracter personal

Documentele care conțin date cu caracter personal sunt ținute în fișete sau dulapuri închise cu cheie sau cu un alt mecanism de securizare. Documentele care conțin date cu caracter personal, folosite pentru realizarea anumitor operațiuni se vor preda persoanelor abilitate sau se vor închide imediat după terminarea acestora.

Prelucrarea datelor cu caracter personal se va efectua numai de către utilizatorii cu atribuții în acest sens (precizate în fișele de post, decizii interne, etc). Moduri de realizare a controlului confidențialității privind datele cu caracter personal al angajaților instituției:

- Informare asupra obligațiilor angajaților în desfășurarea activităților de prelucrare a datelor cu caracter personal și Acord de confidențialitate
- Accesul pe bază de user și parolă la resursele informatice ale instituției.

Obligațiile angajaților a căror activitate presupune prelucrarea datelor cu caracter personal

Angajații a căror activitate presupune prelucrarea datelor cu caracter personal au următoarele obligații, cuprinse în fișa postului:

- să cunoască și să aplice prevederile actelor normative din domeniul prelucrării datelor cu caracter personal precum și ale prezentei politici și să participe la instruirile specifice domeniului GDPR;

- să informeze persoanele vizate cu privire la: identitatea operatorului, scopul în care se face prelucrarea datelor, destinatarii sau categoriile de destinatari ai datelor, obligativitatea furnizării tuturor datelor cerute și consecințele refuzului de a le pune la dispoziție, drepturile prevăzute de lege, în special drepturile de acces, de intervenție asupra datelor și de opoziție, condițiile în care pot fi exercitate aceste drepturi;
- să prelucreze numai datele cu caracter personal necesare îndeplinirii atribuțiilor de serviciu și să acorde sprijin operatorului pentru realizarea activităților specifice ale acestuia;
- să păstreze confidențialitatea datelor prelucrate, a contului de utilizator, a parolei/codului de acces la sistemele informatice/baze de date prin care sunt gestionate date cu caracter personal;
- să respecte măsurile de securitate, precum și celelalte reguli stabilite de operator;
- să informeze de îndată conducerea instituției despre împrejurări de natură a conduce la o diseminare neautorizată de date cu caracter personal sau despre o situație în care au fost accesate/prelucrate date cu caracter personal prin încălcarea normelor legale, despre care a luat la cunoștință.

VI. PRACTICA BIROU CURAT – ECRAN CURAT

Reguli impuse utilizării computerelor

- Toate computerele vor fi setate să se blocheze automat după 10 minute de inactivitate (Lock & LogOff);
- Toate calculatoarele trebuie închise la sfârșitul zilei de lucru;
- La finalul programului de lucru, laptopurile trebuie încuiate într-o cameră dedicată/sertar cu cheie sau blocate prin utilizarea unui cablu de Securitate;
- Atunci când o stație de lucru nu este utilizată aceasta trebuie să fie închisă;
- Toate stațiile de lucru trebuie închise complet la sfârșitul zilei de lucru.

Informații de suport fizic și electronice

- Toți angajații sunt obligați să securizeze la sfârșitul zilei de lucru toate informațiile sensibile, fie în formă tipărită, fie în format electronic;
- Toate informațiile fizice sensibile trebuie să fie securizate/încuiate în interiorul unui dulap. Dulapurile trebuie să fie ținute închise în orice moment;
- Documentele tipărite care conțin informații sensibile sau/și date cu caracter personal trebuie să fie îndepărtate din imprimante cât mai curând posibil;

Documentele tipărite care conțin informații sensibile sau/și date cu caracter personal care nu mai sunt de folos trebuie să fie distruse prin introducerea în tocătoare dacă nu mai sunt necesare. La finalul zilei, înainte de aruncarea hârtiilor distruse de tocător, resturile trebuie amestecate.

Semnături digitale, Tokenuri și protecția media

- Toate token-urile cu semnăturile digitale, smart card-urile, parolele trebuie păstrate într-un dulap

(metalic) încuiat;

- CD-urile, DVD-urile, USB-urile, Cardurile de memorie, Hard discurile portabile sau alte suporturi de stocare a informațiilor electronice trebuie păstrate doar în spații securizate.

Angajații instituției și zonele de lucru

- Angajații trebuie să se asigure că toate informațiile sensibile sau/și date cu caracter personal aflate pe suport de hârtie sau în format electronic sunt amplasate într-o zonă sigură a spațiului lor de lucru;
- Angajații vor utiliza documentele care conțin date cu caracter personal doar cât timp este necesar, minimizând la maxim durata de expunere pe birou, după care vor fi imediat depozitate înapoi în zona sigură și securizată (încuiată);
- La sfârșitul zilei sau atunci când angajatul părăsește biroul, chiar și pentru o perioadă scurtă de timp, echipamentul de calcul trebuie blocat sau închis, materialele fizice depozitate într-un fișet/dulap închis cu cheie și/sau ușa cabinetului/biroului încuiată, după caz;
- Cardurile de acces (legitimații active) unde este cazul, utilizate pentru accesul la informații/încăperi restricționate nu trebuie lăsate în locuri nesupravegheate;
- Atunci când nu sunt utilizate, dulapurile/fișetele care conțin informații confidențiale sau sensibile trebuie să fie închise și încuiate PERMANENT;
- Angajatului îi este impus ca parolele să nu fie lăsate pe bilete plasate pe ecran, sub tastatura sau alte locuri accesibile;
- Documentele tipărite care conțin informații confidențiale sau sensibile trebuie preluate imediat din imprimantă pentru a nu fi expuse;
- Documentele care conțin date sensibile sau/și care conțin date cu caracter personal sau care au un regim special și care urmează a fi DISTRUSE vor fi introduse în tocătoare, în cazul în care nu există diponibile astfel de aparate, se vor rupe în așa fel încât să nu fie posibilă refacerea documentelor.
- Sub nicio formă nu vor rămâne expuse pe birou documente care să conțină informații sensibile sau/și care conțin date cu caracter personal, după programul de lucru.

Amplasarea ecranelor

- Ecranele monitoarelor trebuie amplasate în așa maniera încât persoanele neautorizate să nu le poată observa/captura/fotografia;
- În cazul în care acestea sunt amplasate la vedere, se impune ca afișajele/monitoarele să fie acoperite cu folie de confidențialitate pentru protejarea informației afișate.

VII. MANAGEMENTUL CONTINUITĂȚII ACTIVITĂȚII PRIVIND SECURITATEA DATELOR CU CARACTER PERSONAL

Mecanismul managementului continuității activității este coordonat de conducerea SJUB. Instituția are obligația de a fi pregătită pentru a face față diverselor evenimente interne și externe care pot perturba activitatea normală. Aceste evenimente includ dezastre majore precum: cutremure, inundații, trăsnete, alunecări de teren, acte de terorism, explozii de gaze, scurt-circuite electrice, incendii, acte de vandalism, etc.
Dezastrele sunt clasificate astfel:

- Minore: Indisponibilitatea informațiilor pentru 24-48 de ore.
- Majore: Indisponibilitatea informațiilor pentru 48-72 de ore.

Securitatea datelor cu caracter personal este integrată în mecanismul de management al continuității activității pentru a reduce impactul asupra instituției și a asigura recuperarea datelor la un nivel acceptabil, printr-un set de măsuri de securitate preventive și de recuperare.
Se consideră că procesul de recuperare post-dezastru este finalizat atunci când 80% din funcțiile instituției sunt operaționale, restul urmând să fie recuperate ulterior. Ordinea priorităților pentru salvare, recuperare, restaurare sau înlocuire a elementelor sistemului informațional este următoarea:

1. Oamenii implicați în dezastre.
2. Sistemele de comunicare (centrala telefonică, comunicații de voce GSM, apoi de date, Internet).
3. Informațiile confidențiale, datele cu caracter personal, bazele de date, suporții de back-up.
4. Serverele și serviciile asociate.
5. Dosarele cu documente și arhiva fizică.
6. Sistemele informatice necesare pentru prelucrarea datelor (laptopuri, medii de stocare, PC-uri).
7. Echipamente informatice și copiatoare.
8. Sursele de alimentare cu energie (generatoare, UPS, baterii).
9. Sediul și infrastructura fizică.

În situații deosebit de grave, cu distrugeri și pierderi semnificative, este recomandată așteptarea intervenției forțelor speciale de intervenție (protecția civilă, pompieri, jandarmi etc.). Recuperarea se va face sub coordonarea autorităților competente, după ce au fost asigurate măsurile necesare de securitate în acțiunile de recuperare.

Scenarii și strategii de recuperare

Următoarele măsuri vor fi luate pentru a asigura minimul de impact al unui risc asupra activității, în cazul în care acest risc se produce și devine un incident major de securitate. Aceste măsuri se adresează acelor riscuri ce nu pot fi eliminate în totalitate prin măsuri preventive, și în care riscul rezidual poate avea același impact asupra activității.

Risc	**Descriere**	**Măsuri de recuperare**

1	Îmbolnăvire a unui grup de personal din același departament	În cazul în care perioada de convalescență a întregului grup de personal vital unui proiect sau unui proces depășește perioada maximă acceptată până la recuperare a activității, instituția trebuie să funcționeze la nivel de "avarie": • Un alt grup, de urgenta, cu capabilități asemănătoare va prelua procesul de producție al grupului afectat; • Grupul de urgenta va efectua doar acțiunile prioritare în cadrul proiectului respectiv și va îndeplini sarcinile absolut necesare pentru asigura respectarea termenelor stabilite contractual. În cazul în care nu toate aceste termene vor putea fi atinse, acele termene vitale pentru contract (stabilite de comun acord cu beneficiarul) vor fi prioritare; • Grupul de urgenta va înceta să funcționeze doar în momentul în care grupul inițial afectat poate funcționa la capacitate maximă și poate prelua sarcinile.
2	Pierderea informațiilor/datelor în format electronic sau fizic de pe mediile originale	În cazul pierderii informațiilor de pe mediul de stocare original, cele mai recente copii vor fi restaurate. Întrucât strategiile de backup includ copii ale datelor în mai multe locuri, riscul de o pierdere totală a fost eliminat. Procedura de restaurare trebuie inclusă în procedura de backup. De asemenea, procedura de restaurare trebuie să aibă un timp de restaurare mai mic decât perioada maximă acceptată a downtime-ului pentru fiecare sistem în parte.
3	Pierderea sau deteriorarea unor echipamente vitale datorită problemelor hardware	În cazul problemelor hardware, soluția sau serviciul afectat vor fi restaurate pe sistemul "cold spare" și vor funcționa la capacitate redusă temporar. O dată cu instalarea unui nou sistem capabil de a prelua întreaga capacitate, sistemul temporar va fi de comisionat și va trece din nou în stadiu de "cold spare".
4	Distrugerea sediului fizic ca urmare a unui dezastru (foc, inundație, cutremur...)	În cazul în care sediul fizic al instituției a suferit un dezastru de tip incendiu, inundație, cutremur etc, următorii pași trebuise urmați pentru a asigura continuitatea activității într-un sediu temporar secundar sau prin lucru distribuit: • În timpul dezastrului (incendiu, cutremur etc.) prioritatea cea mai mare este evacuarea personalului din sediul afectat. Din orice punct de vedere, viața umană are prioritate. Pentru aceasta, planul de evacuare pe timp de incendiu trebuie să fie la zi conform legislației în vigoare și testat cel puțin o dată pe an; • În timpul evacuării, conform planului de evacuare vor fi contactate serviciile de urgenta prin apel la 112 (pompieri, salvare, politie etc.); • După ce tot personalul a fost evacuat și se află în siguranță, activitățile vitale vor fi mutate în sediul secundar. • Pentru restaurarea activității IT, vor fi folosite echipamente achiziționate în regim de urgenta (furnizorii cu stocuri), backup-urile vor fi restaurate urmând procedurile existente • Derularea activității în regim de avarie la un nivel minim, se va face până la rezolvarea crizei cu sediul principal. • Incidentul de securitate este încheiat doar când toate funcțiile și toate activitățile SJUB revin la 80% din normal în sediul principal (chiar dacă aceasta înseamnă reconstruirea parțială sau totală a sediului) • Aceasta revenire trebuie făcută într-un timp mai scurt decât timpul maxim definit 48-72 de ore.

5	Cedarea infrastructurii instituției	În cazul cedării parțiale sau totale a infrastructurii interne a instituției, planul de continuitate conține următoarele proceduri: • În cazul în care echipamentele necesare infrastructurii și pe care se bazează elemente cheie cedează, noi echipamente vor fi achiziționate în regim de urgenta de la furnizori. • Pentru restaurarea configurațiilor, se va folosi cel mai recent back-up verificat și testat • În cazul unui incident de securitate produs de atacatori sau de software malițios, trebuie urmați pașii: o Identificarea sursei atacului; o Carantina a zonei afectate astfel încât amenințarea să nu se extindă; o Curățarea zonei afectate; o Restaurarea din backup-uri; o Verificarea și punerea înapoi în funcțiune; o Îmbunătățirea procedurilor viitoare.
6	Furtul și descoperirea codurilor sursa ale software-ului ce intră în proprietatea instituției	Deoarece impactul unui asemenea incident este major, toate măsurile de minimizare a riscului au fost efectuate. Pentru a minimiza pierderile suferite, se recomandă următoarele acțiuni: • Anunțarea autorităților pentru a lua măsurile necesare (în caz de furt de proprietate intelectuală); • Stabilirea unei strategii pentru rescrierea codului și pentru dezvoltarea de aplicații noi.
7	Comunicația cu exteriorul nu funcționează. Schimbul de informații vital pentru instituție este paralizat.	În acest caz, toate comunicațiile vitale vor fi mutate pe legătura secundară fie prin intervenție umană, fie printr-un sistem automat. Un tichet va fi deschis la furnizorul de Internet sau de comunicații. Incidentul este încheiat în momentul în care legătura este refăcuta în totalitate.

Aspectele legate de securitatea datelor se bazează pe identificarea evenimentelor care pot întrerupe procesele instituției. Riscurile asociate acestor evenimente sunt evaluate în termeni de probabilitate și impact, incluzând durata întreruperii, nivelul pagubelor și perioada necesară pentru redresare. Evaluarea riscurilor este documentată în **"Raportul privind identificarea și evaluarea riscurilor privind protecția datelor în cadrul SJUB" – Anexa nr. 1**. Acest raport identifică riscurile, stabilește nivelul de risc și oferă recomandări pentru minimizarea riscurilor, pe baza criteriilor și obiectivelor instituției.

DISPOZIȚII FINALE

Conducerea Spitalului Județean de Urgență Bacău autorizează prezentul document.
Acest document completează întreg setul de politici/reglementări aprobat de conducerea Spitalului Județean de Urgență Bacău.

ANEXE

Anexa nr. 1 - Raportul privind identificarea și evaluarea riscurilor privind protecția datelor în cadrul SJU BACĂU

Anexa 1

Raport - Identificarea și Evaluarea Riscurilor privind protecția datelor cu caracter personal în cadrul Spitalului Județean de Urgență Bacău

1. INTRODUCERE

Acest raport documentează vulnerabilitățile descoperite pe parcursul etapei de evaluare riscuri şi vulnerabilităţi privind securitatea datelor cu caracter personal prelucrate în cadrul Spitalului Județean de Urgență Bacău şi furnizează recomandări pentru eliminarea sau minimalizarea efectelor riscurilor identificate.

Metodologie:

- Analiza activităţilor de prelucrare a datelor cu caracter personal şi a fluxului de date;
- Analiza politicilor, procedurilor, regulamentelor interne şi a codurilor de conduită existente în vederea actualizării cu cerinţele GDPR;
- Analiza măsurilor existente de securitate a datelor cu caracter personal prelucrate;
- Analiza măsurilor existente de securitate a sistemelor informatice;
- Analiza contractelor de prestări servicii şi de altor tipuri de contracte cu terţii şi în vederea actualizării acestora cu clauze privind protecţia datelor cu caracter personal sau a întocmirii de Acte adiţionale la Contracte;
- Analiza conformităţii website-ului la cerinţele GDPR;

Pentru a efectua identificarea vulnerabilităţilor, au fost efectuate următoarele activităţi:

- Interviuri cu personalul din instituţie;
- Analiza documentelor de sistem;
- Vizite la sediul instituției şi discuţii cu personalul (utilizatorii) cheie.

1.1. DEFINIȚII ȘI ABREVIERI ALE TERMENILOR

“Securitatea prelucrării datelor cu caracter personal" - măsuri tehnice şi organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător care să asigure confidenţialitatea, integritatea, disponibilitatea şi rezistenţa continue ale sistemelor şi serviciilor de prelucrare şi capacitatea de a restabili disponibilitatea datelor cu caracter personal şi accesul la acestea în timp util în cazul în care are loc un incident de natură fizică sau tehnică;

"Accesibilitatea" - înseamnă că informaţiile sau datele cu caracter personal sunt accesibile în orice moment;

"Autentificarea" - se referă la confirmarea unei identităţi reale, corecte, certe a unei entităţi sau a unui utilizator;

"Integritatea datelor" - presupune confirmarea că datele cu caracter personal prelucrate sunt complete şi nemodificate;

"Confidenţialitatea datelor " - vizează protecţia divulgării neautorizate sau accesului neautorizat la datele cu caracter personal transmise, stocate sau prelucrate într-un alt mod.

"**Risc"** – gradul de probabilitate ca o vulnerabilitate să genereze în mod accidental sau ilegal, distrugerea, pierderea, modificarea, divulgarea neautorizată sau accesul neautorizat la datele cu caracter personal transmise, stocate sau prelucrate într-un alt mod.

"Evaluarea riscului " - un proces constând în cinci etape: descrierea vulnerabilităţilor, identificarea ameninţărilor/pericolelor, identificarea riscurilor de a compromite integritatea datelor, descrierea riscurilor, identificarea mijloacelor de protecţie şi întocmirea recomandărilor de măsuri corective.

"Regulament GDPR" - REGULAMENTUL (UE) 2016/679 AL PARLAMENTULUI EUROPEAN ŞI AL CONSILIULUI din 27 aprilie 2016 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE (Regulamentul general privind protecţia datelor)

1.2. DOMENIUL DE APLICARE A EVALUĂRII DE RISC

Rolul acestei evaluări este de a identifica posibilele riscuri cu privire la securitatea datelor cu caracter personal prelucrate de către Spitalul Judeţean de Urgenţă Bacău, în calitate de operator de date.

Resursele utilizate pentru prelucrarea datelor cu caracter personal în cadrul Spitalului Judeţean de Urgenţă Bacău identificate de-a lungul procesului de evaluare a riscului se împart în următoarele tipuri de categorii:

- **Informaţii**: baze de date şi fişiere de date, documente ce conţin date cu caracter personal, contracte şi acorduri, documentaţii de sistem, manuale de utilizare, materiale pentru instruire, proceduri operaţionale, planuri de continuitate a activităţii, informaţii arhivate, etc.
- **Resurse software**: software de aplicaţii şi baze de date, software de sistem, etc.
- **Resurse fizice**: echipamente de calcul şi comunicaţii, dispozitive mobile, medii de stocare, alte echipamente.
- **Resurse umane;**

2. SECURITATEA PRELUCRĂRII. ASPECTE GENERALE PRIVIND CONFIDENTIALITATEA SI SECURITATEA DATELOR

Spitalul Judeţean de Urgenţă Bacău prelucrează date cu caracter personal în scopuri precum: prestarea serviciilor medicale solicitate de către Pacienţi, stabilirea unui diagnostic medical, furnizarea de asistenţă medicală sau socială sau a unui tratament medical, gestionarea sistemelor şi serviciilor de sănătate sau de asistenţă socială, în scopuri de recrutare - în contextul prelucrării datelor candidaţilor pentru angajare, evaluarea capacităţii de muncă a angajatului, în scopul gestionării programărilor, reclamaţiilor, sugestiilor sau a oricăror solicitări, în contextul prelucrării datelor tuturor persoanelor care pătrund în incinta spitalului, încheierea şi executarea de contracte, arhivare, îndeplinirea altor obligaţii legale etc.

Conform art. 32 din Regulamentul UE, Spitalul Judeţean de Urgenţă Bacău, în calitate de operator de date are obligativitatea de a implementa măsuri tehnice şi organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător, incluzând printre altele, după caz:

a) pseudonimizarea şi criptarea datelor cu caracter personal;

b) capacitatea de a asigura confidenţialitatea, integritatea, disponibilitatea şi rezistenţa continue ale sistemelor şi serviciilor de prelucrare;

c) capacitatea de a restabili disponibilitatea datelor cu caracter personal şi accesul la acestea în timp util în cazul în care are loc un incident de natură fizică sau tehnică;

d) un proces pentru testarea, evaluarea şi aprecierea periodice ale eficacităţii măsurilor tehnice şi organizatorice pentru a garanta securitatea prelucrării".

Un rol important in evaluarea nivelului adecvat de securitate îl reprezintă riscurile pe care le implica prelucrarea, riscuri ce pot fi generate, accidental ori ilegal, de distrugerea, pierderea, modificarea, divulgarea neautorizata sau accesul neautorizat la datele cu caracter personal transmise, stocate sau prelucrate într-un alt mod.

3. PREZENTAREA METODEI DE EVALUARE A RISCULUI

Identificare riscurilor are la bază o serie de vulnerabilităţi şi ameninţări aferente prelucrării de date cu caracter personal în cadrul Spitalului Judeţean de Urgenţă Bacău care au fost identificate în urma discuţiilor cu personalul aparţinând Spitalului Judeţean de Urgenţă Bacău şi analiza fluxului de date în instituţie.

Analiza riscului presupune abordarea sistemica a luării deciziilor, realizării procedurilor şi acţiunilor practice în procesul de soluţionare a problemelor de avertizare (preîntâmpinare), ori de reducere a pericolului de a compromite integritatea datelor. Metoda de evaluare a riscului utilizată în cazul Spitalului Judeţean de Urgenţă Bacău s-a derulat în următoarele faze:

a) Descrierea vulnerabilităţilor

b) Identificarea ameninţărilor/pericolelor

c) Identificarea riscurilor de a compromite integritatea datelor

d) Descrierea riscurilor

e) Identificarea mijloacelor de protecţie şi întocmirea recomandărilor de măsuri corective

4. IDENTIFICAREA RISCURILOR. RECOMANDĂRI ŞI MIJLOACE DE PROTECŢIE

În urma analizei efectuate, în cadrul Spitalului Judeţean de Urgenţă Bacău au fost identificate următoarele riscuri privind securitatea datelor cu caracter personal precum şi recomandări privind utilizarea unor mijloace de protecţie împotriva riscurilor:

Nr. Crt.	Vulnerabilitate	Amenințare/ Pericol	Riscul de a compromite	Descrierea Riscului	Recomandări măsuri corective
1.	Posibilitatea deteriorării mediilor de stocare	Deteriorarea mediului de stocare	Disponibilitatea și integritatea datelor	Deteriorarea mediilor de stocare (hârtia, medii de stocare optice sau magnetice)	Testarea periodică a mediilor de stocare
2.	Posibilitatea utilizării de software neautorizat (freeware, shareware, fără licență)	Pierderea informației Cod malițios	Integritatea, disponibilitatea, confidențialitatea datelor	Utilizarea software-ului neautorizat poate duce la pierderea integrității datelor	Implementarea unui sistem prin care utilizatorii să nu aibă dreptul de a-și instala software neautorizat pe calculator
3.	Spațiu de depozitare necorespunzător	Pierderea informației	Confidențialitatea și integritatea datelor	Chiar dacă există spatii special amenajate pentru depozitare, este posibil ca în cazul unui incendiu ca informația să fie pierdută	Este recomandat ca informațiile importante să fie stocate și într-o altă locație
4.	Lipsa parțială a mecanismelor de identificare și autentificare a utilizatorilor	Furtul Utilizarea neautorizată	Confidențialitatea și integritatea datelor	Dacă nu este asigurată o securitate corespunzătoare informațiile pot fi sustrase de pe computerul gazda	Implementarea unui sistem pentru jurnalizarea activităților de pe un computer
5.	Posibilitatea virusării fișierelor, programelor	Pierderea informației Utilizarea neautorizată Cod malițios	Confidențialitatea și integritatea datelor	În cazul virusării se pot pierde informațiile, sau pot fi copiate în mod fraudulos	Implementarea unui sistem antivirus eficient, cu licență și verificarea ca antivirusul să fie actualizat cel puțin o dată pe lună
6.	Posibilitatea furtului de fișiere sau baze de date	Pierderea informației Utilizarea neautorizată	Confidențialitatea și integritatea datelor	Dacă nu este asigurată o securitate corespunzătoare informațiile pot fi sustrase de pe computerul gazda	Implementarea unui sistem pentru jurnalizarea activităților de pe un computer
7.	Erori și omisiuni de date cauzate de	Pierderea informațiilor	Confidențialitatea, disponibilitatea	Informațiile pot fi sustrase, modificate sau distruse prin	Creșterea responsabilității utilizatorilor prin

	personalul angajat		şi integritatea datelor	erorile personalului angajat	sesiuni de instruire şi informare asupra obligaţiilor angajaţilor în desfăşurarea activităţilor de prelucrare a datelor cu caracter personal si semnarea unui acord de confidenţialitate.
8.	Date importante sunt stocate pe memorii USB	Utilizare voit defectuoasă	Confidenţialitate a datelor	Pierderea sau furtul acestor dispozitive poate compromite datele	Criptarea memoriilor USB folosite
9.	Nu se face "log-out" când se părăseşte staţia de lucru	Utilizarea neautorizată	Confidenţialitate a şi integritatea datelor	Informaţiile pot fi sustrase de pe computerul gazdă, se poate face furt de identitate	Implementarea unui mecanismul care să oblige log-out când se părăseşte staţia de lucru
10.	Setări de securitate ale aplicaţiilor setate necorespunzător	Refuzul serviciului Accesare neautorizată a datelor Schimbări neautorizate ale softwareului Distrugerea datelor Furt şi fraudă	Confidenţialitate a, disponibilitatea şi integritatea datelor	Informaţiile pot fi sustrase, modificate sau distruse dacă setările de securitate ale aplicaţiilor sunt setate necorespunzător	Implementarea unui sistem de autentificare şi identificare a utilizatorilor
11.	Absenţa sistemului automat de detecţie şi de stingere a incendiilor	Distrugerea informaţiilor	Disponibilitatea şi integritate	Informaţiile pot fi distruse în absenţa sistemului automat de stingere a incendiilor	Instalarea unui sistem de detecţie şi stingere a incendiului în locaţiile în care sunt stocate informaţii vitale
12.	Absenţa software-ului de detectare a intruziunilor	Acces neautorizat Distrugere informaţii Schimbare neautorizată de software	Confidenţialitate a, disponibilitatea şi integritatea datelor	Informaţiile pot fi sustrase, modificate sau distruse în absenţa software-ului de detecţie a intruziunilor	Soluţii de monitorizare a prelucrărilor automate şi manual Implementarea unui sistem antivirus cu management centralizat Implementarea unui

					sistem de autentificare şi jurnalizare a activităţilor
13.	Lipsa mesajelor de atenţionare a utilizatorilor	Erori umane Disfuncţionalităţi tehnice	Confidenţialitatea, disponibilitatea şi integritatea datelor	Informaţiile pot fi modificate sau distruse în lipsa unor mesaje de atenţionare	Instruire utilizatori pentru a preîntâmpina modificarea sau distrugerea accidentală a informaţiilor
14.	Absenţa actualizării regulate a software-ului antivirus	Cod maliţios	Confidenţialitatea, disponibilitatea şi integritatea datelor	Informaţiile pot fi sustrase, modificate sau distruse dacă nu se utilizează o soluţie AV centralizată	Implementarea unui sistem antivirus cu management centralizat
15.	Lipsa unui plan pentru continuitatea activităţii sau a procedurilor de recuperare şi restaurare a informaţiilor	Pierderea informaţiei	Disponibilitatea datelor	Poate fi compromisă continuitatea activităţii în lipsa unui plan de recuperare, restaurare a informaţiilor.	Implementarea unor măsuri necesare pentru a asigura continuitatea activităţii
16.	Lipsa conformării website-ului la cerinţele GDPR	Utilizare defectuoasă, pierderea informaţiei	Confidenţialitatea, disponibilitatea şi integritatea datelor	Poate fi compromisă securitatea prelucrării datelor	Conformarea la GDPR prin elaborarea de politici de confidenţialitate/ cookies
17.	Lipsa instruirilor personalului angajat in mod specific asupra managementului breşelor de securitate	Pierderea informaţiilor	Confidenţialitatea, disponibilitatea şi integritatea datelor	Compromiterea datelor cu caracter personal	Elaborarea unui program de conştientizare a personalului angajat privind identificarea breşelor de securitate şi acţiunile ce trebuie întreprinse
18.	Publicarea datelor cu caracter personal pe site-urile proprii	Divulgarea informaţiilor Acces neautorizat	Confidenţialitatea, disponibilitatea şi integritatea datelor	Compromiterea datelor cu caracter personal	Anonimizarea datelor cu caracter personal (semnătura)
19.	Lipsa alinierii contractelor de produse/servicii/lucrări la prevederile Regulamentului	Divulgarea informaţiilor Acces neautorizat	Confidenţialitatea, disponibilitatea şi integritatea datelor	Compromiterea datelor cu caracter personal	Analiza contractelor de prestări servicii şi de altor tipuri de contracte cu terţii şi în vederea actualizării acestora cu clauze

	General 679/2016				privind protecţia datelor sau a întocmirii de acte adiţionale la contracte
20.	Lipsa alinierii normelor/regulamentelor interne cu prevederile şi implicaţiile Regulamentului General 679/2016	Divulgarea informaţiilor Acces neautorizat	Confidenţialitatea, disponibilitatea şi integritatea datelor	Compromiterea datelor cu caracter personal	Completarea politicilor şi procedurilor interne cu prevederile GDPR.
21.	Folosirea neautorizată a canalelor de comunicare nesecurizate (WhatsApp, Messenger/Facebook)	Divulgarea informaţiilor Acces neautorizat	Confidenţialitatea, disponibilitatea şi integritatea datelor	Compromiterea datelor cu caracter personal	Utilizarea platformelor de comunicare oficiale şi securizate ale instituţiei şi instruirea personalului angajat cu privire la folosirea unor astfel de aplicaţii

Manager,

Ec. Ion-Marius SAVIN