Servicii de mentenanță a
Portalului certificatelor de concediu medical

Anexa 1 la formularul F 4.1

OFERTA TEHNICA

Digitally signed by Cojocari Andrei
Date: 2021.02.04 12:20:03 EET
Reason: MoldSign Signature
Location: Moldova

Cuprins

Oferta matriciala “Cerina” – “Raspuns” 3

Aplicare a politicilor de securitate– 2600 cuvinte 23

Cerinta	Răspuns
Baza juridico-normativă sub care se desfășoară proiectul include legislația națională în vigoare, convențiile și tratatele internaționale, la care Republica Moldova este parte. Crearea și funcționarea sistemelor informaționale este reglementată de următoarele acte legislative și normative:	Confirmam ca am luat la cunostinta si asumam desfășurarea proiectului in acord cu Baza juridico-normativă sub care se desfășoară proiectul include legislația națională în vigoare, convențiile și tratatele internaționale, la care Republica Moldova este parte. La crearea și funcționarea sistemelor informaționale se va tine cont de reglementările următoarelor acte legislative și normative:
• *Legea nr.411-XII din 28.03.1995 „Ocrotirii sănătății”;* • *Legea nr.982 din 11 mai 2000 privind accesul la informație;* • *Legea nr.1069 din 22 iunie 2000 „Cu privire la informatică”;* • *Legea nr.467 din 21 noiembrie 2003 cu privire la informatizare și la resursele informaționale de stat;* • *Legea nr.412-XV din 09.12.2004 „Cu privire la Statistica oficială”* • *Legea 100-XV din 26 aprilie 2001 „Privind actele din starea civilă”* • *Legea nr. 71 din 22 martie 2007 cu privire la registre;* • *Legea nr.133 din 08 iulie 2011 privind protecția datelor cu caracter personal;* • *Hotărârea Guvernului Republicii Moldova №.586 din 24.07.2017 pentru aprobarea Regulamentului privind modul de ținere a Registrului medical;* • *Hotărârea Guvernului nr.632 din 8 iunie 2004 despre aprobarea Politicii de edificare a societății informaționale în Republica Moldova;* • *Hotărârea Guvernului nr.1123 din 14 decembrie 2010 privind aprobarea Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal;* • *Hotărârea Guvernului Republicii Moldova №. 101 din 5 februarie 2008 privind instituirea „Registrului de stat al formularelor medicale de strictă evidență”;* • *Hotărârea Guvernului Republicii Moldova №.272 din 6 martie 2002 privind măsurile de creare a*	• *Legea nr.411-XII din 28.03.1995 „Ocrotirii sănătății”;* • *Legea nr.982 din 11 mai 2000 privind accesul la informație;* • *Legea nr.1069 din 22 iunie 2000 „Cu privire la informatică”;* • *Legea nr.467 din 21 noiembrie 2003 cu privire la informatizare și la resursele informaționale de stat;* • *Legea nr.412-XV din 09.12.2004 „Cu privire la Statistica oficială”* • *Legea 100-XV din 26 aprilie 2001 „Privind actele din starea civilă”* • *Legea nr. 71 din 22 martie 2007 cu privire la registre;* • *Legea nr.133 din 08 iulie 2011 privind protecția datelor cu caracter personal;* • *Hotărârea Guvernului Republicii Moldova №.586 din 24.07.2017 pentru aprobarea Regulamentului privind modul de ținere a Registrului medical;* • *Hotărârea Guvernului nr.632 din 8 iunie 2004 despre aprobarea Politicii de edificare a societății informaționale în Republica Moldova;* • *Hotărârea Guvernului nr.1123 din 14 decembrie 2010 privind aprobarea Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal;* • *Hotărârea Guvernului Republicii Moldova №. 101 din 5 februarie 2008 privind instituirea „Registrului de stat al formularelor medicale de strictă evidență”;* • *Hotărârea Guvernului Republicii Moldova №.272 din 6 martie 2002 privind măsurile de creare a sistemului informațional automatizat „Registrul de stat al unităților de drept";*

sistemului informațional automatizat „Registrul de stat al unităților de drept";

- *Hotărârea Guvernului RM №.1128 din 14.10.2004 privind aprobarea Concepției Sistemului Informațional Medical Integrat;*
- *Ordinul nr. 87 din 01.06.2006 cu privire la aprobarea reglementării tehnice "Procesele ciclului de viață al software-ului" RT 38370656 - 002:2006*
- *Ordinul MS RM nr. 695 din 13.10.2010 „Cu privire la Asistența Medicală primară din Republica Moldova";*
- *Ordinului MS nr.190 din 23 iunie 2003 „Cu privire la instituirea structurii sistemului sănătății raionale/municipale", ce prevede structura și responsabilitățile secțiilor de informatică și statistică medicală din cadrul instituțiilor medicale publice;*
- *Ordinul MS RM nr. 828 din 31.10.2011 „Cu privire la aprobarea formularelor de evidență medicală primară;*
- *Ordinul MS „Cu privire la întocmirea și prezentarea dărilor de seamă statistice medicale anuale de către instituțiile medico-sanitare", actualizat anual;*
- *Ordinul MS nr. 404 din 30 octombrie 2007 "Cu privire la delimitarea juridică a asistenței medicale primare la nivel raional";*
- *Ordinul nr. 1086 din 30.12.2016 cu privire la aprobarea Regulamentelor-cadru de organizare și funcționare ale prestatorilor de servicii de sănătate*
- *Ordinul nr. 1080 din 28 decembrie 2017 „Cu privire la aprobarea Nomenclatorului Instituțiilor medico-sanitare Publice de asistență medicală primară la nivel de raion";*
- *Ordin nr. 47 din 10.02.2016 Cu privire la aprobarea Nomenclatorului prestatorilor privați de servicii de sănătate*
- *Ordin nr. 466 din 11.06.2015 cu privire la aprobarea Nomenclatorului instituțiilor medico-sanitare spitalicești*
- *Ordinul MS Nr. 1023 din 29.12.2011 privind aprobarea formularelor statistice de evidență medicală primară ;*
- *Ordinul nr. 1087/721 din 30.12.2016 despre aprobarea Regulamentului privind înregistrarea persoanei la medicul de familie din instituția medico-sanitară ce prestează asistență medicală*

- *Hotărârea Guvernului RM №.1128 din 14.10.2004 privind aprobarea Concepției Sistemului Informațional Medical Integrat;*
- *Ordinul nr. 87 din 01.06.2006 cu privire la aprobarea reglementării tehnice "Procesele ciclului de viață al software-ului" RT 38370656 - 002:2006*
- *Ordinul MS RM nr. 695 din 13.10.2010 „Cu privire la Asistența Medicală primară din Republica Moldova";*
- *Ordinului MS nr.190 din 23 iunie 2003 „Cu privire la instituirea structurii sistemului sănătății raionale/municipale", ce prevede structura și responsabilitățile secțiilor de informatică și statistică medicală din cadrul instituțiilor medicale publice;*
- *Ordinul MS RM nr. 828 din 31.10.2011 „Cu privire la aprobarea formularelor de evidență medicală primară;*
- *Ordinul MS „Cu privire la întocmirea și prezentarea dărilor de seamă statistice medicale anuale de către instituțiile medico-sanitare", actualizat anual;*
- *Ordinul MS nr. 404 din 30 octombrie 2007 "Cu privire la delimitarea juridică a asistenței medicale primare la nivel raional";*
- *Ordinul nr. 1086 din 30.12.2016 cu privire la aprobarea Regulamentelor-cadru de organizare și funcționare ale prestatorilor de servicii de sănătate*
- *Ordinul nr. 1080 din 28 decembrie 2017 „Cu privire la aprobarea Nomenclatorului Instituțiilor medico-sanitare Publice de asistență medicală primară la nivel de raion";*
- *Ordin nr. 47 din 10.02.2016 Cu privire la aprobarea Nomenclatorului prestatorilor privați de servicii de sănătate*
- *Ordin nr. 466 din 11.06.2015 cu privire la aprobarea Nomenclatorului instituțiilor medico-sanitare spitalicești*
- *Ordinul MS Nr. 1023 din 29.12.2011 privind aprobarea formularelor statistice de evidență medicală primară ;*
- *Ordinul nr. 1087/721 din 30.12.2016 despre aprobarea Regulamentului privind înregistrarea persoanei la medicul de familie din instituția medico-sanitară ce prestează asistență medicală primară în cadrul asigurării obligatorii de asistență medicală*

- *Ordinul comun al MS și CNAM nr. 596/404A din 21.07.2016 privind aprobarea Normelor metodologice de aplicare a Programului unic al asigurării obligatorii de asistență medicală*
- *Ordinul comun al MS și CNAM nr. 1131/658A din 29.12.2017 Criteriile de contractare a instituțiilor*

primară în cadrul asigurării obligatorii de asistență medicală • *Ordinul comun al MS și CNAM nr. 596/404A din 21.07.2016 privind aprobarea Normelor metodologice de aplicare a Programului unic al asigurării obligatorii de asistență medicală* • *Ordinul comun al MS și CNAM nr. 1131/658A din 29.12.2017 Criteriile de contractare a instituțiilor medico-sanitare în cadrul sistemului asigurării obligatorii de asistență medicală pentru anul 2018* • *Hotărâre de Guvern Nr.128 din 20.02.2014 privind platforma tehnologică guvernamentală comună (MCloud)*	*medico-sanitare în cadrul sistemului asigurării obligatorii de asistență medicală pentru anul 2018* • *Hotărâre de Guvern Nr.128 din 20.02.2014 privind platforma tehnologică guvernamentală comună (MCloud)*

Principiile de bază • *principiul legitimității*, potrivit căruia funcțiile și operațiile efectuate de utilizatori sunt legale și conforme cu drepturile omului și legislația națională în vigoare; • *principiul autenticității datelor*, care presupune că informațiile păstrate pe dispozitive de stocare a datelor sau pe suport de hârtie corespund stării reale a obiectelor; • *principiul identificării*, conform căruia pachetelor informaționale li se atribuie un cod de clasificare la nivel de sistem, prin care este posibilă identificarea univocă și raportarea la acestea; • principiul temeiniciei datelor, care prevede că introducerea datelor se efectuează doar în baza înscrierilor din documentele acceptate ca surse de informații; • *principiul auditului sistemului*, care presupune înregistrarea informației despre schimbările care au loc, pentru a face posibilă reconstituirea istoriei unui document sau starea lui la o etapă anterioară; • *principiul independenței de platforma software,* conform căruia poate fi construit pe baza modulelor elaborate la comandă sau a produselor software existente. Conceptul nu limitează în nici un fel abordarea dezvoltării sistemului atât timp cât sunt satisfăcute nevoile identificate și se oferă cea mai mare valoare pentru prețul oferit. • *principiul accesibilității și integrabilității*, care presupune că, chiar dacă oferă funcționalități multiple, este construit ca un element integral și folosit de utilizatori prin intermediul unei interfețe unice. Mai mult decât atât, acest principiu prevede că expansiunea și dezvoltarea sistemului se vor face prin protocoale și puncte de conexiune proiectate din start; • *principiul confidențialității informației*, care prevede răspunderea personală, în conformitate cu legislația în vigoare, a colaboratorilor responsabili de prelucrarea informației în sistem pentru utilizarea și difuzarea neautorizată a informației;	**Am luat cunoștință cu principiile de bază ce vor fi utilizate în cadrul implementării proiectului.**

• *principiul compatibilității*, conform căruia trebuie să fie compatibil cu sistemele existente atât în țară, cât și peste hotarele ei; • *principiul orientării spre utilizator*, potrivit căruia structura, conținutul, mijloacele de acces și navigarea sunt focalizate spre utilizatori; • *principiul extensibilității*, conform căruia componentele oferă facilități de ajustare și extindere a funcționalităților existente pentru conformare cu necesitățile în continuă schimbare; • *principiul dezvoltării progresive*, potrivit căruia elaborarea sistemului și modificarea permanentă a componentelor sale se efectuează în conformitate cu tehnologiile informaționale avansate; • *principiul consecutivității*, care presupune elaborarea și implementarea proiectului pe etape; • principiul eficienței funcționării, care presupune optimizarea raportului dintre calitate și cost; • *principiul utilizării standardelor deschise*, care se aplică pentru a asigura atât interoperabilitatea cu sistemele externe, cât și păstrarea informației, în conformitate cu normele în vigoare; • *principiul securității informaționale*, care presupune asigurarea nivelului dorit de integritate, exclusivitate, accesibilitate și eficiență a protecției datelor împotriva pierderii, denaturării, distrugerii și utilizării neautorizate. Securitatea sistemului presupune rezistența la atacuri și protecția caracterului secret, a integrității și pregătirii pentru lucru, cit și a datelor acestuia.	

Scopurile lucrărilor în cadrul Portalului Portalul certificatelor de concediu medical a fost lansat în producție în septembrie 2019 și a permis personalului medical înregistrarea datelor certificatelor de concediu medical necesare pentru calcularea indemnizațiilor pentru incapacitatea temporară de muncă. Totodată pe parcursul utilizării Portalului s-a constatat faptul că în situațiile în care utilizatorii admit erori la introducerea datelor în Portal, sau întârzie înregistrarea lor, este greu de efectuat corecțiile necesare asupra datelor. Astfel în unele cazuri este necesar de anulat unul sau câteva certificate de concediu medical pentru a restabili ordinea corectă a certificatelor și de modificare a datelor certificatelor de concediu medical. Scopurile dezvoltării modificărilor în cadrul Portalului sunt următoarele: • Posibilități mai extinse de a face corecții în datele certificatelor de concediu medical; • Posibilitatea de a înregistra necondiționat datele certificatelor de concediu medical; • Actualizarea automată a statutului certificatelor de concediu medical după emiterea deciziei de către CNAS; • Transmiterea automată a tuturor certificatelor de concediu medical fără intervenția ulterioară a utilizatorilor. • Micșorarea timpului de procesare a datelor certificatelor de concediu medical; • Creșterea calității datelor înregistrate. În prezenta documentație sunt reflectate informații privind tehnologia folosită și modul în care sunt prelucrate datele. Prestatorul va avea acces la codul sursă al sistemului și își va asuma riscurile ce decurg din modificările acestuia. Asumarea serviciilor implică acordarea garanției asupra Portalului pentru o perioadă de minim 12 luni după semnarea actului de predare primire pentru modificările software (cod sursa) realizate pe perioada contractului. De asemenea prestatorul serviciilor va documenta toate operațiunile de modificare a sistemului și le va	**Am luat cunoștință cu scopul lucrărilor în cadrul portalului**

<table>
<tr><td>prezenta Beneficiarului împreuna cu codul sursa care a suportat modificări.</td><td></td></tr>
<tr><td>Obiectivele proiectului
Sistemul descris în continuare face obiectul achiziției serviciilor de mentenanța în scopul asigurării bunei funcționări.
Portalul certificatelor de concediu medical necesită optimizarea modului de înregistrare și corectare a datelor certificatelor de concediu medical. De asemenea este nevoie de optimizat modul de transmitere a datelor și recepționare a răspunsului din partea CNAS.</td><td>Am luat cunoștință cu obiectivele proiectului</td></tr>
<tr><td>Astfel în cadrul serviciilor de mentenanță corectivă a Portalului vor fi efectuate următoarele lucrări:
<table>
<tr><th>Nr.</th><th>Descriere</th></tr>
<tr><td>1.</td><td>Eliminarea restricției de modificare a certificatului de concediu medical din "Primar" în "Continuare" și invers.</td></tr>
<tr><td>2.</td><td>Eliminarea restricției de înregistrare a certificatelor de concediu medical "Continuare" dacă pe certificatul anterior a fost aprobată decizie de refuz.</td></tr>
<tr><td>3.</td><td>Eliminarea restricției de înregistrare a certificatelor "Continuare" dacă a fost specificată ieșirea la serviciu.</td></tr>
<tr><td>4.</td><td>Posibilitatea de afișare a certificatelor de concediu medical pe o persoană eliberate de către orice prestator.</td></tr>
<tr><td>5.</td><td>Posibilitatea de a înregistra certificate de concediu medical în continuare fără restricția de necesitate a introducerii certificatului precedent.</td></tr>
<tr><td>6.</td><td>Posibilitate de a transmite automat certificate de concediu medical în cazul în care se formează lanțul logic (perioade consecutive fără lacune) al perioadelor pentru care au fost acordate certificatele.</td></tr>
</table></td><td>Am luat cunoștință și asumăm următoarele:
- vom analiza și dezvolta următoare funcționalități al sistemului și vom actualiza documentația în conformitate cu lista lucrărilor în cadrul serviciilor de mentenanța corectivă a Portalului:
<table>
<tr><th>Nr.</th><th>Descriere</th></tr>
<tr><td>1.</td><td>Eliminarea restricției de modificare a certificatului de concediu medical din "Primar" în "Continuare" și invers.</td></tr>
<tr><td>2.</td><td>Eliminarea restricției de înregistrare a certificatelor de concediu medical "Continuare" dacă pe certificatul anterior a fost aprobată decizie de refuz.</td></tr>
<tr><td>3.</td><td>Eliminarea restricției de înregistrare a certificatelor "Continuare" dacă a fost specificată ieșirea la serviciu.</td></tr>
<tr><td>4.</td><td>Posibilitatea de afișare a certificatelor de concediu medical pe o persoană eliberate de către orice prestator.</td></tr>
<tr><td>5.</td><td>Posibilitatea de a înregistra certificate de concediu medical în continuare fără restricția de necesitate a introducerii certificatului precedent.</td></tr>
<tr><td>6.</td><td>Posibilitate de a transmite automat certificate de concediu medical în cazul în care se formează lanțul logic (perioade consecutive fără lacune) al perioadelor pentru care au fost acordate certificatele.</td></tr>
<tr><td>7.</td><td>Posibilitatea de recepționare de la CNAS a statutului actualizat al certificatului de</td></tr>
</table></td></tr>
</table>

7.	Posibilitatea de recepționare de la CNAS a statutului actualizat al certificatului de concediu medical înregistrat și de al actualiza în Portal.
8.	Posibilitatea de a vizualiza certificatele de concediu medical "Continuare" pentru care nu există un certificat care să se termine cu ziua anterioară zilei de start a certificatului "Continuare".
9.	Activarea opțiunii indemnizație pentru maternitate cu posibilitatea de a elibera certificatul la o data anterioara (inclusiv cu 30 săptămâni înapoi de la ziua curentă). Pentru gravidele care se află la întreținerea soțului se vor completa data căsătoriei, datele soțului prin specificarea IDNP/CPAS, și preluarea datelor din Registrul dle stat al populației prin platforma de MConnect.
10.	Actualizarea documentației, manualelor și ghidurilor de utilizare.

	concediu medical înregistrat și de al actualiza în Portal.
8.	Posibilitatea de a vizualiza certificatele de concediu medical "Continuare" pentru care nu există un certificat care să se termine cu ziua anterioară zilei de start a certificatului "Continuare".
9.	Activarea opțiunii indemnizație pentru maternitate cu posibilitatea de a elibera certificatul la o data anterioara (inclusiv cu 30 săptămâni înapoi de la ziua curentă). Pentru gravidele care se află la întreținerea soțului se vor completa data căsătoriei, datele soțului prin specificarea IDNP/CPAS, și preluarea datelor din Registrul dle stat al populației prin platforma de MConnect.
10.	Actualizarea documentației, manualelor și ghidurilor de utilizare.

În procesul de lucru Dezvoltatorul de comun cu reprezentanții AGE și CNAS vor stabili specificația tehnică pentru schimbul de date cu platforma MConnect. Dezvoltatorul va asigura corespunderea funcțiilor de interdependență a Portalului certificatelor de concediu medical și sistemului informațional CNAS pentru implementarea cerințelor de schimb de date.	**Am luat cunoștință și ne asumăm să participăm ca consultanți pentru stabilirea criteriilor pentru schimb de date între Beneficiar, AGE și CNAS. Vom asigura corespunderea funcțiilor de interdependență a Portalului certificatelor de concediu medical și sistemului informațional CNAS în baza acordului pentru schimb de date între Beneficiar și CNAS.**
Toate cerințele sunt obligatorii.	**Am luat cunoștință.**
Pe lângă cerințele funcționale Dezvoltatorul va prezenta documentația aferentă proiectului si anume: • Documentul de analiză și proiectare pentru funcționalitățile solicitate; • Rezultatele testării pe mediul de test; • Manualele și instrucțiunile de utilizare actualizate.	**Am luat cunoștință și asumăm livrarea următoarelor documente:** - Documentul de analiză și proiectare pentru funcționalitățile solicitate; - Rezultatele testării pe mediul de test; - Manualele și instrucțiunile de utilizare actualizate.

Durata estimată pentru serviciile de modificare a funcționalităților în cadrul Portalul certificatelor de concediu medical este până la 90 zile lucrătoare de la semnarea contractului.	**Am luat cunoștință.** **Avind în vedere totalitatea cerințelor expuse în caietul de sarcină ne asumăm executarea lucrărilor în termen de 90 zile**
Asumarea serviciilor implică acordarea garanției asupra Portalului certificatelor de concediu medical pentru o perioadă de 12 luni după semnarea actului de predare primire pentru modificările software (cod sursa) realizate pe perioada contractului. De asemenea prestatorul serviciilor va documenta toate operațiunile de modificare a sistemului și le va prezenta Beneficiarului împreuna cu codul sursa care a suportat modificări.	**Am luat cunoștință și asumăm următoarele:** - Acordarea garanției asupra Portalului certificatelor de concediu medical pentru o perioadă de 12 luni după semnarea actului de predare primire pentru modificările software (cod sursa) realizate pe perioada contractului; • Documentul de analiză și proiectare pentru funcționalitățile solicitate; • Rezultatele testării pe mediul de test; • Manualele și instrucțiunile de utilizare actualizate. Imprimarea manualelor de utilizare este responsabilitatea Beneficiarului.
Specificații tehnice Arhitectura Portalului permite funcționarea pe infrastructura M-Cloud și funcționează centralizat pe infrastructura hardware concepută pentru disponibilitate 99.9% cu următoarele caracteristici generale: • respectă standardele în vigoare a tehnologiilor informaționale; • asigură flexibilitate în vederea adaptării permanente la normele juridice și în vederea dezvoltării softului după implementare; • utilizează o arhitectura orientata pe servicii pentru a acomoda cu ușurință noi modificări cu intervenții exclusiv asupra componentei de actualizat, minimizând costurile și timpul necesar realizării modificărilor; • întreține în limba romana interfața utilizator, conținutul registrelor, bazelor de date și documentelor generate; • permite ca utilizatorul să se autentifice o singură dată pentru a accesa toate funcționalitățile modulului;	**Am luat cunoștință cu specificațiile tehnice**

• utilizează serviciul guvernamental M-Pass pentru autentificare; • asigură schimbul de date cu CNAS prin intermediul platformei MConnect; • corespunde cerințelor standardelor securității și confidențialității informației si prelucrării datelor cu caracter personal; • asigură o siguranță sporita în exploatare.	
Beneficiar al sistemul este Ministerul Sănătății, Muncii și Protecției Sociale. Documentul de Analiză elaborat de Furnizor va constitui primul livrabil și va fi supus aprobării și acceptării de către MSMPS în comun cu CNAM și CNAS. Documentul de analiză aprobat de către MSMPS în comun cu CNAM și CNAS va fi reperul pentru Acceptanța Finală, primând in fața oricărui alt document tehnic. Documentul de Analiză va fi întocmit de către Furnizor, cu implicarea specialiștilor Beneficiarului.	Am luat cunoștință și asumăm că primul livrabil va constitui Documentul de analiză, și va fi supus aprobării și acceptării de către MSMPS în comun cu CNAM și CNAS. Documentul de analiză aprobat de către MSMPS în comun cu CNAM și CNAS va fi reperul pentru Acceptanța Finală, primând in fața oricărui alt document tehnic. Documentul de Analiză va fi întocmit de către Furnizor, cu implicarea specialiștilor Beneficiarului. Ținând cont de solicitare de dezvoltare in termeni cat mai restrânși, contam pe o cooperare din partea tuturor părților implicate in oferirea si prezentarea informațiilor descrise exhaustiv necesare pentru elaborarea documentului de analiză in termeni cât mai restrânși.

Asumarea contextului dezvoltărilor software Contextul in care Furnizorul va desfășura serviciile contractate este următorul: • Beneficiarul deține dreptul de proprietate asupra codului aplicației. Orice operațiune de modificare a codului generează o noua versiune a aplicației pentru care dezvoltatorul [cel care efectuează modificarea] va oferi garanție completă. Beneficiarul își păstrează în continuare dreptul de proprietate asupra aplicației. Pentru o înțelegere clară, modificările funcționalităților existente sau noile dezvoltări ale aplicației se fac la cererea Beneficiarului. Beneficiarul nu intervine asupra codului aplicației, motiv pentru care răspunderea funcționării corecte a aplicației în timpul și după executarea modificărilor de cod aparține dezvoltatorului. Orice modificare asupra aplicației implică din partea dezvoltatorului obligația acordării garanției pentru întreg sistemul și nu doar pe modificările efectuate. • În același context este important de reținut faptul că eventualele incidente, disfuncționalități sau alterări de configurație care privesc buna funcționare a sistemelor se vor trata exclusiv cu furnizorul serviciilor și nu cu terțe persoane. Asumarea serviciilor din acest proiect implică acordarea garanției asupra sistemelor implicate. • Beneficiarul își păstrează dreptul de proprietate asupra aplicației indiferent de îmbunătățirile aduse acesteia pe parcursul desfășurării contractului. • În baza legislației sau a necesităților operaționale, Beneficiarul poate solicita Furnizorului modificări, sau funcționalități noi, iar Furnizorul trebuie sa fie pregătit în permanență să le implementeze rapid, fără a afecta funcționarea normală a sistemului. • În baza necesitaților operaționale, Beneficiarul poate solicita Furnizorului consultanță în formă de răspunsuri scrise la întrebările cu privire la sistemul dezvoltat, sau consultanță în formă de prezentări la oficiul Beneficiarul cu privire la întrebări specifice legate de sistemul dezvoltat. • Furnizorul este responsabil pentru eventualele incidente asupra sistemelor implicate generate pe	Asumăm cele expuse în compartimentul dat. Deasemenea noi suntem gata sa executăm orce modificare sau solicitare de la beneficiar, în baza condițiilor contractuale.

parcursul operațiunilor desfășurate de el, sau la recomandarea lui pe durata realizării de noi funcționalități. • Versiunile actualizate și funcționale ale sistemului intră automat în proprietatea Beneficiarului, iar furnizorul execută operațiunile tehnice asupra acestora pana la finalizarea contractului și acordă garanție asupra lor, în forma în care au fost predate. Cheltuielile generate de defecțiunile aplicației în perioada de garanție vor fi suportate de către Furnizor.	

Cerințe privind calitatea serviciilor **Mod de lucru. Modalități de intervenție** Toate componentele Portalului sunt găzduite în Cloud-ul guvernamental (M-Cloud). Accesul la serverele sistemului se face în mod securizat atât din interiorul centrului de date cât și din exterior. În timpul desfășurării operațiunilor de întreținere este important de păstrat o comunicare corectă între echipa Furnizorului și cea a beneficiarului. Experții Beneficiarului trebuie să înțeleagă terminologia tehnică specifică sistemelor informatice, nu doar pe cea specifică aplicației. Experiențele anterioare ale beneficiarului au demonstrat că unele situații pot fi tratate doar în condițiile implicării echipelor tehnice de la toate nivelurile sistemului în condițiile de menținere permanentă a calității și securității sistemului. Buna comunicare între echipele de suport este esențială în procesul de întreținere a sistemului și al asigurării unei bune experiențe a utilizatorilor sistemului. Toate operațiunile de acest fel se desfășoară în condiții de securitate cibernetica maximă, cu respectarea strictă a legislației în vigoare. Operațiunile de întreținere la nivelul aplicativ și de platformă software se desfășoară în mod securizat prin accesul experților din afara centrului de date. Situațiile mai simple, in special recomandări, pot fi tratate telefonic, sau prin email. Pot apărea însă și situații cu nivel sporit de complexitate sau risc, în care este necesara prezența on-site a echipelor de suport tehnic și comunicarea între managerii acestora devine obligatorie pentru succesul operațiunilor. Pe perioada contractului vor fi disponibile din partea Furnizorului următoarele modalități de intervenție în cazul incidentelor, dar și pentru operațiuni normale de întreținere: • Intervenție de la distanță [remote acces], securizată. Se vor respecta recomandările specialiștilor Centrului de Date al Cloud-uluii guvernamental; • Intervenții tehnice și recomandări telefonice, prin email, sau prin alte mijloace de comunicație electronică, inclusiv videoconferința;	Am făcut cunoștință cu acest capitol de cerințe și avind in vedere ca aplicatia este rulata pe MCloud ne vom conforma cu regulile impuse de MCloud. Toate adresarile vor fi raportate intr-un sistem de ticketing.

<table>
<tr><td>

- Intervenții on-site, în situațiile în care specialiștii centrului de date guvernamental apreciază că este necesară o astfel de abordare a situației.

</td><td></td></tr>
<tr><td>

Cerințe pentru Call Center

Prin ofertă, furnizorul serviciilor achiziționate de către Beneficiar asumă următoarele condiții minime de suport tehnic pe aplicație, la nivelul Call Center-ului:

- Disponibilitate Call Center prin email, telefon acordat la programul de lucru al beneficiarului;
- Modalități de asigurare a suportului; email, telefon, remote acces.

Obligații solicitate pentru Call Center în cazul unui incident la nivelul centrului de date:

- Personalul Call Center -ului va trebui să dispună permanent actualizată lista specialiștilor disponibili pentru intervenție;
- Personalul Call Center-ului trebuie să mențină legătura cu specialiștii (telefonică, email, sms) pe parcursul intervențiilor astfel încât utilizatorii să poată primi informații corecte privind starea de funcționare a sistemului;
- Call Center-ul nu va dirija utilizatorii către echipele de intervenție, ci va acționa ca punct unic de contact pe toată durata incidentului până la reintrarea sistemului în regim normal de operare.

</td><td>

Ne asumăm următoarele cerințe legate de Call Center:

Cerințe pentru Call Center

Prin ofertă, furnizorul serviciilor achiziționate de către Beneficiar asumă următoarele condiții minime de suport tehnic pe aplicație, la nivelul Call Center-ului:

- Disponibilitate Call Center prin email, telefon acordat la programul de lucru al beneficiarului;
- Modalități de asigurare a suportului; email, telefon, remote acces.

Obligații solicitate pentru Call Center în cazul unui incident la nivelul centrului de date:

- Personalul Call Center -ului va contacta personalul MCloud pentru a informa despre incidente legate de MCloud.

</td></tr>
<tr><td>

Timpi de intervenție [SLA]

Sistemul este conceput in scopul funcționarii corecte si continue. Intervențiile programate si durata acestora se agreează cu împreuna cu beneficiarul in urma consultării si agreării de către toate departamentele de suport. Serviciile interne pentru acest proiect sunt dimensionate pentru asigurarea unui nivel de disponibilitate la care trebuie sa se alinieze si serviciile achiziționate prin prezenta procedura. In situații de incident, timpii solicitați pentru operațiunile tehnice sunt următorii:

<table>
<tr><td>Timp de răspuns</td><td>2 ore</td></tr>
<tr><td>Timpi de intervenție pentru defecțiuni la nivelul serverelor sau alterarea configurației sistemului în Cloud-ul guvernamental (M-Cloud) cât și a componentelor majore ale sistemului.</td><td>2 ore</td></tr>
</table>

</td><td>

Asumăm timpii de intervenție pentru obiectele ce cad sub incidența garanției în conformitate cu subiectul contractului.

</td></tr>
</table>

Timpi de intervenție pentru acțiuni corective	8 ore	

Cerințe obligatorii privind experiența furnizorului Beneficiarul a identificat următoarele cerințe minime privind expertiza pe care trebuie să o aibă furnizorul: 1. Să demonstreze utilizarea în proiectele dezvoltate a serviciului guvernamental de autentificare și control MPass 2. 3. Să demonstreze utilizarea în proiectele dezvoltate a serviciului guvernamental de semnătură electronică MSign 4. 5. Să demonstreze utilizarea în proiectele dezvoltate a platformei guvernamentale de interoperabilitate MConnect 6.	Informația despre experiența furnizorului este anexată.

Cerințe obligatorii privind experiența personalului Beneficiarul a identificat următoarele cerințe minime privind expertiza pe care trebuie să o aibă echipa tehnica a furnizorului: **Expert - Manager de proiect** • Minim 5 ani experiență în managementul proiectelor în domeniul Tehnologii Informaționale si Comunicații; • Experiență în cel puțin 3 proiecte de implementare a unor soluții similare, în rolul de manager de proiect pentru toată durata proiectului; • Experiență de lucru de cel puțin 1 an în cadrul companiei Ofertantului sau a grupului din care aceasta face parte; • Experiența dobândită prin participarea în cel puțin 1 proiect la activități IT complexe privind infrastructura software și hardware din cadrul sistemelor informatice (se justifica prin documente semnate de beneficiari ex: recomandări); • Studii Superioare, deținerea unui Certificat emis de o instituție recunoscută la nivel internațional în domeniul managementului proiectelor (PMP sau PRINCE2 sau echivalent); • Cunoașterea limbii române este obligatorie. • Notă: În cazul în care oferta este depusă de o asociere, managerul de proiect trebuie să dispună de experiență în cadrul companiei lider al asocierii minim 1 an.	Informația despre echipă este anexată.

Specialist infrastructura sistem • Studii superioare TIC finalizate cu diploma de licență; • Competențe dovedite prin certificare în managementul serviciilor IT; • Experiența profesională generală in domeniul informatic de minim 10 ani; • Experiența dobândită prin participarea în cel puțin 3 proiecte la activități IT complexe privind infrastructura software și hardware din cadrul sistemelor informatice (se justifică prin documente semnate de beneficiari ex: recomandări, cel puțin o recomandare) •		
Specialist asigurare a calității în domeniul securității • Studii superioare finalizate cu diploma de licență in domeniul informatic; • Experiența profesională generală în domeniul informatic de minim 10 ani; • Competențe privind auditul securității sistemelor informatice, dovedite prin prezentarea unei certificări în domeniu emisă de autoritate publică competentă cu recunoaștere generală sau de către un organism de drept public sau privat autorizat. • Competențe privind auditarea sistemelor de management al calității, dovedite prin prezentarea unei certificări în domeniu emisă de autoritate publică competentă cu recunoaștere generală sau de către un organism de drept public sau privat autorizat.		

• Experiența dobândită prin participarea, în funcția de expert calitate, în cel puțin 3 proiecte informatice (se justifica prin documente semnate de beneficiari ex: recomandări, cel puțin o recomandare)	
Analist dezvoltare sistem informatic • Studii superioare finalizate cu diplomă de licență; • Experiența profesională generală în domeniul informatic de minim 5 ani; • Experiența dobândită prin participarea în calitate de specialist IT în cel puțin 3 proiecte de implementare a unui sistem informatic (se justifica prin documente semnate de beneficiari ex: recomandări, cel puțin o recomandare)	
Dezvoltator • Studii superioare finalizate cu diploma de licență în domeniul informatic; • Experiență conform CV de minim 5 ani in programarea aplicațiilor web și a bazelor de date cu următoarele tehnologii (Java, Spring React framework, Docker, Nginx, MySQL) • Experiența conform CV prin participarea în cel puțin 3 proiecte la activități tehnice asupra sistemelor informatice.	
Specialist baze de date • Studii superioare finalizate cu diploma de licență în domeniul informatic; • Experiență conform CV de minim 5 ani in programarea aplicațiilor web și a bazelor	

de date cu următoarele tehnologii (Java, Spring React framework, Docker, Nginx, MySQL) • Experiența conform CV prin participarea în cel puțin 3 proiecte la activități tehnice asupra sistemelor informatice. Notă: Ofertantul poate prezenta recomandare pe numele companiei, sau pe numele specialistului.	
Modalitatea de întocmire a ofertelor Toate cerințele din caietul de sarcini sunt minime și obligatorii, iar nerespectarea sau respectarea parțială a uneia dintre cerințe va duce automat la declararea ofertei ca fiind neconformă și, implicit, la descalificarea ei. Asumarea condițiilor în care se desfășoară proiectul și îndeplinirea cerințelor tehnice, de personal sau asupra modului de lucru pentru toate punctele precizate în capitolele documentației sunt condiții obligatorii și eliminatorii pentru conformitatea ofertelor și sunt totodată termeni considerați contractuali. Ofertantul va prezenta **Oferta tehnică** în care pentru toate cerințele ofertanții vor răspunde punct cu punct într-un tabel cu minim 2 coloane „Cerința" „Răspuns". Coloana răspuns va conține inclusiv durata de timp în zile necesare pentru dezvoltarea cerinței. **În cazul în care ofertantul nu prezintă Oferta tehnică oferta va fi declarată ca fiind neconformă și, implicit, la descalificarea ei.**	Am luat cunoștință
Criterii de evaluare **Condiții obligatorii ale ofertelor pentru calcularea punctajului** Pentru calcularea punctajului doar ofertele care îndeplinesc simultan condițiile: • îndeplinesc integral condițiile solicitate privind experiența ofertantului și pregătirea personalului; • răspund corect cerințelor Caietului de Sarcini.	Am luat cunoștință

Ofertele care nu îndeplinesc criteriile de mai sus sunt declarate neconforme și sunt descalificate. Tabelul de punctaj aplicat ofertelor selectate astfel are un punctaj maxim total de 100 de puncte	
ANEXE În scopul înțelegerii cât mai corecte a cerințelor Caietului de Sarcini, Beneficiarul aduce la cunoștința participanților la procedura de achiziție detaliile tehnice funcționale ale sistemelor informatice operaționale asupra cărora vor fi desfășurate operațiunile solicitate. Furnizorul va avea acces la codurile sursă ale componentelor deținute de către Beneficiarul și își va asuma toate riscurile ce decurg din modificarea acestora. Furnizorul serviciilor va documenta toate operațiunile de modificare a sistemului și le va prezenta Beneficiarului, acordând garanție pe întreg sistemul de la intrarea în regim de producție a sistemului.	Am luat cunoștință cu toate anexele din caietul de sarcini.

Aplicare a politicilor de securitate– 2600 cuvinte

Aplicarea politicile de securitate necesare sistemului se va face de către tot personalul implicat in proiect in conformitate cu legislația in vigoare. Sistemul prelucrează date cu

caracter personal si, asupra acestui tip de date, sunt emise acte normative speciale. De asemenea exista in domeniul informatic reguli de buna practica cat si standarde de securitate. Deținem o experiență vasta in prelucrarea informațiilor din baze de date de nivel național si ne sunt cunoscute modalitățile de aplicare a legislației, standardelor si regulilor de buna practica. Experții noștri au participat la proiecte importante in Republica Moldova, intre cele mai importante **proiecte precedente realizate pe teritoriul Republicii Moldova, enumeram:**

- ***„Servicii de creare a sub-sistemului Informațional E-Dosar din cadrul Programul Integrat de Gestionare a Dosarelor (PIGD) si extinderea acestuia cu funcționalități noi"***
- ***„Migrarea Sistemului Informațional Automatizat Asistenta Sociala din Republica Moldova in M-Cloud"***
- ***„Sistem Informațional Automatizat pentru Asistența Medicală Spitalicească (SIA AMS) - Sistem informațional automatizat de sănătate pentru instituțiile medico-sanitare spitalicești publice din Republica Moldova, găzduit în infrastructura de Cloud guvernamental"***

Politica de securitate aferenta tipului de date prelucrate va fi (re)adusă la cunoștința tuturor persoanelor responsabile de operarea datelor cu caracter personal, înaintea acordări accesului la operarea datelor cu caracter personal. Atât personalul medical cat si cel tehnic cunosc si se supun normelor de prelucrare a acestor date; totuși in cadrul proiectului vor exista iterații pe aceasta tema si se va tine cont de tipul informațiilor in ORICE activitate care presupune accesul la date.

Bunele practici si standardele de securitate impun ca datele cu caracter personal care fac obiectul prelucrării sa fie realizată cu respectarea următoarelor principii:

- Conformarea tuturor regulilor, impuse de MCloud, platformei guvernamentale care va asigura securitatea aplicației.
- Aplicarea bunelor practici pentru a evita "OWASP Top Ten Most Critical Web Application Vulnerabilities".
- Prelucrarea în mod corect și în conformitate cu prevederile legale.
- Asigurarea colectării unor date adecvate, pertinente și neexcesive în ceea ce privește scopul pentru care sunt colectate și/sau prelucrate ulterior.
- Asigurarea colectării unor date exacte și, dacă este necesar, actualizate. Datele inexacte sau incomplete din punct de vedere al scopului pentru care sunt colectate și ulterior prelucrate se șterg sau se rectifică.
- Colectarea în scopuri determinate, explicite și legitime, iar ulterior nu este admisă prelucrarea într-un mod incompatibil cu aceste scopuri.
- Excluderea accesului neautorizat la datele cu caracter personal existente.

- Preîntâmpinarea scurgerii de informații care conține date cu caracter personal, transmise prin canalele de legătură prin folosirea metodelor de cifrare a acestei informații.

- Preîntâmpinarea scurgerii de informații care conțin date cu caracter personal sau defecțiunilor în funcționarea soft-ului destinat operării cu date cu caracter personal este asigurata prin folosirea programelor licențiate, programelor antivirus, organizării sistemului de control al securității soft-ului.

- Preîntâmpinarea scurgerii de informații care conțin date cu caracter personal, este asigurată prin auditul intern al sistemelor informaționale, care se efectuează permanent.

- Stabilirea exactă a ordinii de acces la informația care conține date cu caracter personal in cadrul sistemelor informaționale și de evidență instituite atât pentru utilizatorii interni cât și pentru cei externi.

- Limitarea accesului personalului la datele cu caracter personal la nivelul minim de care aceștia au nevoie pentru desfășurarea activității. Acest lucru se realizează prin mecanismele de securitate ale sistemului.

Necesitatea înțelegerii politicilor de securitate necesare sistemului este o condiție obligatorie pentru:

- **Respectarea legislației;**
- **Succesul proiectului si sustenabilitatea acestuia pe termen lung;**
- **Încrederea cetățenilor si personalului care prelucrează datele personale;**
- **Siguranța datelor de importanta națională.**

Referințe utilizate:

- La 14.12.2010, prin Hotărârea Guvernului nr. 1123, au fost aprobate Cerințele faţă de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal, act normativ secundar care stabilește măsurile tehnice și organizatorice necesar a fi implementate de către deținătorii de date cu caracter personal în vederea asigurării securității, confidențialității și integrității datelor cu caracter personal, prelucrate în cadrul sistemelor informaționale de date cu caracter personal și/sau registrelor ţinute manual, în conformitate cu prevederile art. 14 al Legii cu privire la protecţia datelor cu caracter personal.
- **Legea** Nr.133 din 08.07.2011, ce are drept scop asigurarea protecţiei drepturilor şi libertăţilor fundamentale ale persoanei fizice în ceea ce priveşte prelucrarea datelor cu caracter personal, în special a dreptului la inviolabilitatea vieţii intime, familiale

şi private. O serie de paragrafe ale acestei legi sunt esentiale pentru intelegerea politicilor de securitate necesare:

Articolul 4. Caracteristica datelor cu caracter personal

(1) Datele cu caracter personal care fac obiectul prelucrării trebuie să fie:

a) prelucrate în mod corect şi conform prevederilor legii;

b) colectate în scopuri determinate, explicite şi legitime, iar ulterior să nu fie prelucrate într-un mod incompatibil cu aceste scopuri. Prelucrarea ulterioară a datelor cu caracter personal în scopuri statistice, de cercetare istorică sau ştiinţifică nu este considerată incompatibilă cu scopul colectării dacă se efectuează cu respectarea prevederilor prezentei legi, inclusiv privind notificarea către Centrul Naţional pentru Protecţia Datelor cu Caracter Personal, şi cu respectarea garanţiilor privind prelucrarea datelor cu caracter personal, prevăzute de normele ce reglementează activitatea statistică, cercetarea istorică şi cea ştiinţifică;

c) adecvate, pertinente şi neexcesive în ceea ce priveşte scopul pentru care sînt colectate şi/sau prelucrate ulterior;

d) exacte şi, dacă este necesar, actualizate. Datele inexacte sau incomplete din punctul de vedere al scopului pentru care sînt colectate şi ulterior prelucrate se şterg sau se rectifică;

e) stocate într-o formă care să permită identificarea subiecţilor datelor cu caracter personal pe o perioadă care nu va depăşi durata necesară atingerii scopurilor pentru care sînt colectate şi ulterior prelucrate. Stocarea datelor cu caracter personal pe o perioadă mai mare, în scopuri statistice, de cercetare istorică sau ştiinţifică, se va face cu respectarea garanţiilor privind prelucrarea datelor cu caracter personal, prevăzute de normele ce reglementează aceste domenii, şi numai pentru perioada necesară realizării acestor scopuri.

(2) Operatorii au obligaţia să respecte şi să asigure implementarea prevederilor alin. (1).

Articolul 5. Prelucrarea datelor cu caracter personal

(1) Prelucrarea datelor cu caracter personal se efectuează cu consimţământul subiectului datelor cu caracter personal.

(2) Consimţământul privind prelucrarea datelor cu caracter personal poate fi retras în orice moment de către subiectul datelor cu caracter personal. Retragerea consimţământului nu poate avea efect retroactiv.

(3) În cazul incapacităţii de exerciţu sau al capacităţii de exerciţiu limitate a subiectului datelor cu caracter personal, consimţământul privind prelucrarea datelor cu caracter personal se acordă, în formă scrisă, de către reprezentantul lui legal.

(4) În cazul decesului subiectului datelor cu caracter personal, consimţământul privind prelucrarea datelor sale se acordă, în formă scrisă, de către succesorii acestuia, dacă un astfel de consimţământ nu a fost dat de subiectul datelor cu caracter personal în timpul vieţii.

(5) Consimţământul subiectului datelor cu caracter personal nu este cerut în cazurile în care prelucrarea este necesară pentru:

a) executarea unui contract la care subiectul datelor cu caracter personal este parte sau pentru luarea unor măsuri înaintea încheierii contractului, la cererea acestuia;

b) îndeplinirea unei obligaţii care îi revine operatorului conform legii;

c) protejarea vieţii, integrităţii fizice sau a sănătăţii subiectului datelor cu caracter personal;

d) executarea sarcinilor de interes public sau care rezultă din exercitarea prerogativelor de autoritate publică cu care este învestit operatorul sau terţul căruia îi sînt dezvăluite datele cu caracter personal;

e) realizarea unui interes legitim al operatorului sau al terţului căruia îi sînt dezvăluite datele cu caracter personal, cu condiţia ca acest interes să nu prejudicieze interesele sau drepturile şi libertăţile fundamentale ale subiectului datelor cu caracter personal;

f) scopuri statistice, de cercetare istorică sau ştiinţifică, cu condiţia ca datele cu caracter personal să rămînă anonime pe toată durata prelucrării.

Articolul 6. Prelucrarea categoriilor speciale de date cu caracter personal

(1) Prelucrarea categoriilor speciale de date cu caracter personal este interzisă, cu excepţia cazurilor în care:

a) subiectul datelor cu caracter personal şi-a dat consimţământul. În cazul incapacităţii de exerciţu sau al capacităţii de exerciţiu limitate a subiectului datelor cu caracter personal, prelucrarea categoriilor speciale de date cu caracter personal se efectuează numai cu obţinerea consimţământului în formă scrisă al

reprezentantului lui legal;

b) prelucrarea este necesară pentru îndeplinirea obligaţiilor sau drepturilor specifice ale operatorului în domeniul dreptului muncii, cu respectarea garanţiilor prevăzute de lege şi ţinîndu-se cont de faptul că o eventuală dezvăluire către un terţ a datelor cu caracter personal prelucrate în acest scop poate fi efectuată numai dacă există o obligaţie legală a operatorului în acest sens;

c) prelucrarea este necesară pentru protecţia vieţii, integrităţii fizice sau a sănătăţii subiectului datelor cu caracter personal ori a altei persoane, în cazul în care subiectul datelor cu caracter personal se află în incapacitate fizică sau juridică de a-şi da consimţământul; (….)

Articolul 7. Prelucrarea datelor cu character personal privind starea de sănătate

(1) Prelucrarea datelor cu caracter personal privind starea de sănătate se permite, prin derogare de la prevederile art. 6, în cazul în care:

a) prelucrarea este necesară în scopuri de medicină preventivă, de stabilire a diagnosticelor medicale, de administrare a unor îngrijiri sau tratamente pentru subiectul datelor cu caracter personal sau de gestionare a serviciilor de sănătate care acţionează în interesul subiectului datelor cu caracter personal;

b) prelucrarea este necesară pentru protecţia sănătăţii publice.

(2) Cadrele medicale, instituţiile medico-sanitare şi personalul medical al acestora pot prelucra date cu caracter personal privind starea de sănătate fără autorizaţia Centrului Naţional pentru Protecţia Datelor cu Caracter Personal numai dacă prelucrarea este necesară pentru protejarea vieţii, integrităţii fizice sau a sănătăţii subiecţlor datelor cu caracter personal. Dacă scopurile menţionate se referă la alte persoane sau la societate în general, iar subiecţii datelor cu caracter personal nu şi-au dat consimţământul în scris şi în mod neechivoc, urmează să fie obţinută autorizaţia Centrului în modul stabilit de lege.

(3) Datele cu caracter personal privind starea de sănătate pot fi prelucrate în scopurile indicate la alin. (1) de către sau sub supravegherea unui cadru medical supus secretului profesional ori de către sau sub supravegherea unei alte persoane supuse unei obligaţii echivalente în ceea ce priveşte secretul profesional.

(4) Datele cu caracter personal privind starea de sănătate se colectează de la subiectul datelor cu caracter personal sau atunci cînd o astfel de prelucrare este necesară în conformitate cu alin. (1).

(….)

Articolul 9. Prelucrarea datelor cu caracter personal avînd funcţie de identificare

Prelucrarea numărului de identificare de stat (IDNP) al persoanei fizice, a amprentelor digitale sau a altor date cu caracter personal avînd o funcţie de identificare de aplicabilitate generală poate fi efectuată în următoarele condiţii:

a) subiectul datelor cu caracter personal şi-a dat consimţământul;

b) prelucrarea este prevăzută în mod expres de legislaţie.

(…..)

Articolul 11. Stocarea şi utilizarea datelor cu caracter personal la încheierea operaţiunilor de prelucrare

(1) Condiţiile şi termenele de stocare a datelor cu caracter personal se stabilesc de legislaţie ţinîndu-se cont de prevederile art. 4 alin. (1) lit. e). La expirarea termenului de stocare, datele cu caracter personal urmează a fi distruse în modul stabilit de lege.

(2) Datele cu caracter personal din registrele de stat, de la data încetării utilizării acestora, pot rămîne la păstrare primind statutul de document de arhivă.

(3) La încheierea operaţiunilor de prelucrare a datelor cu caracter personal, dacă subiectul acestor date nu şi-a dat consimţământul pentru o altă destinaţie sau pentru o prelucrare ulterioară, acestea vor fi:

a) distruse;

b) transferate unui alt operator, cu condiţia ca operatorul iniţial să garanteze faptul că prelucrările ulterioare au scopuri similare celor în care s-a făcut prelucrarea iniţială;

c) transformate în date anonime şi stocate exclusiv în scopuri statistice, de cercetare istorică sau ştiinţifică.

(4) După decesul subiectului datelor cu caracter personal, datele acestuia se pot utiliza, cu consimţământul succesorilor, în scop de arhivă sau în alte scopuri prevăzute de lege.

(....)

Articolul 19. Organul de control al prelucrărilor de date cu caracter personal

(1) Controlul asupra conformităţi prelucrării datelor cu caracter personal cu cerinţele prezentei legi se efectuează de către Centrul Naţional pentru Protecţia Datelor cu Caracter Personal (în continuare – Centru), care acţionează în condiţii de imparţialitate şi independenţă.

(2) Centrul este persoană juridică, dispune de ştampilă şi de antet cu imaginea Stemei de Stat a Republicii Moldova. Sediul permanent al Centrului se află în municipiul Chişinău.

(3) Regulamentul Centrului, structura şi personalul-limită ale acestuia se aprobă de Parlament.

(4) Bugetul Centrului se aprobă printr-o hotărîre a Parlamentului, după examinarea şi avizarea lui pozitivă în comisia parlamentară de profil.

(5) Parlamentul remite Guvernului bugetul aprobat al Centrului pentru a fi inclus în proiectul legii bugetului de stat pentru anul următor.

(...)

Articolul 29. Confidenţialitatea datelor cu caracter personal

(1) Operatorii şi terţii care au acces la datele cu caracter personal sînt obligaţi să asigure confidenţialitatea acestor date, cu excepţia cazurilor:

a) prelucrarea se referă la date făcute publice în mod voluntar şi manifest de către subiectul datelor cu caracter personal;

b) datele cu caracter personal au fost depersonalizate.

(2) Orice persoană care acţionează în numele, pe seama sau în alt mod sub autoritatea operatorului poate prelucra date cu caracter personal doar pe baza instrucţiunilor operatorului, cu excepţia cazului în care acţionează în temeiul unei obligaţii prevăzute de lege.

(3) Conducerea Centrului şi personalul acestuia sînt obligaţi să garanteze nedivulgarea secretului profesional în ceea ce priveşte informaţiile confidenţiale la care au acces, inclusiv după încetarea activităţii lor.

Articolul 30. Securitatea prelucrării datelor cu caracter personal

(1) La prelucrarea datelor cu caracter personal, operatorul este obligat să ia măsurile organizatorice şi tehnice necesare pentru protecţia datelor cu caracter personal împotriva distrugerii, modificării, blocării, copierii, răspîndirii, precum şi împotriva altor acţiuni ilicite, măsuri menite să asigure un nivel de securitate adecvat în ceea ce priveşte riscurile prezentate de prelucrare şi caracterul datelor prelucrate.

(2) În cazul în care prelucrarea datelor cu caracter personal este efectuată pe seama şi în numele operatorului, acesta va împuternici o persoană care va asigura respectarea garanţiilor referitoare la măsurile adecvate de securitate tehnică şi de organizare privind prelucrarea ce urmează să fie efectuată.

(3) Prelucrarea datelor cu caracter personal prin persoana împuternicită de către operator trebuie reglementată printr-un contract sau un alt act juridic care să asigure în special faptul că:

a) persoana împuternicită acţionează numai pe baza instrucţiunilor operatorului;

b) obligaţiile prevăzute la alin. (1) îi revin şi persoanei împuternicite.

(4) Cerinţele faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal se stabilesc de Guvern.

Articolul 31. Depersonalizarea datelor cu caracter personal

(1) În scopuri statistice, de cercetare istorică, ştiinţifică, sociologică, medicală, de documentare juridică, operatorul depersonalizează datele cu caracter personal prin retragerea din ele a părţii care permite identificarea persoanei fizice, transformîndu-le în date anonime, care nu pot fi asociate cu o persoană identificată sau identificabilă.

(2) În cazul depersonalizării, regimul de confidenţialitate stabilit pentru datele respective se anulează.

Concluzia necesității aplicării politicii de securitate necesară sistemului

Însăși **existenta** sistemului ar fi imposibila in lipsa aplicării politicii de securitate. Aplicarea acestei politici este obligatorie in orice faza a proiectului dar si nu numai, fiind extinsa chiar **si după încetarea oricărei prelucrări de date**. Întreg personalul care va avea acces la informațiile din sistem dar si cel managerial sau logistic înțeleg necesitatea aplicarea politicii de securitate. Ca si concluzie generala, sistemul deține informații care nu pot fi

accesate sau prelucrate decât in condițiile aplicării politicii de securitate cu referințele legislative in vigoare si însoțite de standardele de securitate dar si de bunele practici din domeniul informatic.