CAIET DE SARCINI

SPECIFICAȚIE TEHNICĂ

Servicii de mentenanța corectivă, preventivă și adaptivă a platformei guvernamentale de plăți electronice (MPay)

pentru perioada de 12 luni

1. CAIET DE SARCINI

1.1. Generalități

1.1.1. Abrevieri, Termeni și Definiții

1.1.1.1. Termeni și definiții

Banca Națională a Moldovei – autoritate publică, care reglementează și supraveghează activitatea prestatorilor de servicii de plată și gestionează SAPI (sistemul automatizat de plăți interbancare).

Posesorul MPay – I.P. Agenția de Guvernare Electronică (AGE, denumit în text și Beneficiar). AGE este responsabilă de implementarea, operarea, menținerea și dezvoltarea continuă a Serviciului Guvernamental de Plăți Electronice. AGE cooptează prestatori de servicii de plăți și integrează noi instrumente de plată în cadrul MPay și oferă servicii de încasare și restituire a plăților către prestatorii de servicii cu plată și servicii de distribuire a plăților către distribuitorii de plăți.

Administrator tehnic – I.P. Serviciul Tehnologia Informației și Securitate Cibernetică (STISC). STISC este responsabilă de administrarea tehnică și menținerea serviciului MPay, în conformitate cu prevederile Regulamentului privind administrarea tehnică și menținerea resurselor și sistemelor informaționale de stat, aprobat prin HG nr. 414/2018 cu privire la măsurile de consolidare a centrelor de date în sectorul public și de raționalizare a administrării sistemelor informaționale de stat.

Serviciul Guvernamental de Plăți Electronice (MPay), denumit și Serviciul MPay - componentă a platformei tehnologice guvernamentale comune, prin intermediul căreia este posibilă încasare, restituirea și distribuirea plăților de la bugetele componente ale bugetului public național.

Minister – Ministerul Finanțelor, împuternicit în sistemul automatizat de plăți interbancare (în continuare – SAPI) de către prestatorii de servicii de plată licențiați conform Legii nr. 114/2012 cu privire la serviciile de plată și moneda electronică (în calitate de participanți în SAPI) privind debitarea și/sau creditarea conturilor de decontare ale acestora deschise în SAPI, cu valoarea pachetelor de plăți încasate/distribuite/restituite prin serviciul MPay.

Prestator de servicii cu plată – persoanele juridice de drept public și persoanele juridice de drept privat care prestează servicii cu plată. Sunt asimilate prestatorilor de servicii cu plată, în sensul prezentului regulament, autoritățile/instituțiile publice împuternicite în temeiul legii să asigure colectarea impozitelor, taxelor, amenzilor, majorărilor de întârziere (penalităților) și altor plăți în CUT.

Prestator de servicii de plăți – se consideră astfel cum sunt determinați în conformitate cu cadrul normativ în domeniul serviciilor de plată și monedei electronice. Prestatorul de servicii de plată (de obicei bănci, Poșta Moldovei, prestatorii de terminale cash-in, monedă electronică) este responsabilă de încasarea sau distribuirea plăților, utilizând infrastructura proprie și cu informarea MPay.

Distribuitor de plăți – persoanele juridice de drept public în cadrul procesului de distribuire a prestațiilor sociale și altor plăți efectuate de la bugetele componente ale bugetului public național, precum și în cadrul plăților spre restituire din CUT și din conturile instituțiilor publice la autogestiune către persoanele fizice, cu excepția plăților salariale.

Prestator – agent economic care prestează servicii de suport, întreținere tehnică și mentenanță adaptivă a platformei Guvernamentale de Plăți Electronice în bază unui contract, încheiat între AGE și agent economic în bază desfășurării procedurii de achiziții publice.

notă de plată – document (date) în formă electronică emis de serviciul MPay în baza informației primare oferite de prestatorul de servicii cu plată, în temeiul căruia poate fi încasată plata pentru serviciile cu plată solicitate.

Rețeaua Telecomunicațională a Autorităților Administrației Publice – rețeaua de transport date destinată să asigură comunicarea între autoritățile publice din R. Moldova. Rețeaua este operată de I.P. Serviciul Tehnologia Informației și Securitate Cibernetică (STISC).

MCloud – Platforma tehnologică comună a Guvernului, dezvoltată în baza tehnologiilor de cloud computing.

Mentenanță adaptivă - constă în modificarea și/sau adaptarea/dezvoltarea sistemului informatic, aflat în exploatare în scopul asigurării eficienței, performanței si productivității acestuia, precum și adaptarea acestuia la cerințele tehnica-normative actuale.

MIA Plăți Instant - este un sistem de plăți interbancare în care tranzacțiile financiare electronice se realizează în timp real, disponibil 24/7, oferind beneficiarului plății acces imediat la mijloacele din cont transferate.

1.1.1.2. Abrevieri

AGE – I.P. Agenția de Guvernare Electronică;

BNM – Banca Națională a Moldovei;

MF – Ministerul Finanțelor;

STISC– I.P. Serviciul Tehnologia Informației și Securitate Cibernetică;

PP – Prestator de servicii de plată;

PS – Prestator de servicii cu plată;

DP – Distribuitor de plăți;

SGPE – Serviciul Guvernamental de Plăți Electronice

SAPI - Sistemul automatizat de plăţi interbancare

1.1.2. Modul de funcționare al MPay

Serviciul Guvernamental de Plăți Electronice MPay reprezintă infrastructura centrală de plăți a statului, prin intermediul căreia se realizează încasarea, restituirea și distribuirea

plăților către și de la bugetele componente ale bugetului public național. MPay funcționează ca un intermediar informațional și financiar neutru între prestatorii de servicii cu plată, distribuitorii de plăți, prestatorii de servicii de plată, Ministerul Finanțelor și persoane fizice și juridice, asigurând interoperabilitatea tuturor acestor actori într-un ecosistem unitar, securizat și trasabil.

Serviciul MPay este dezvoltat pe platforma .NET și rulează pe versiunea curentă Long-Term Support (LTS) a acesteia. Platforma acoperă un spectru larg de canale și instrumente de plată: plăți prin terminale bancare (POS), internet banking, mobile banking, terminale cash-in, Poșta Moldovei, e-Commerce, precum și plăți prin sistemul de decontare instantanee MIA Plăți Instant, disponibil 24/7. Serviciul MPay deține un rol central în implementarea Programului strategic de modernizare tehnologică a guvernării (HG nr. 710/2011) și a Strategiei de transformare digitală a Republicii Moldova pentru anii 2023–2030 (HG nr. 650/2023), constituind unul dintre pilonii digitalizării serviciilor publice cu plată.

1.1.2.1. Instituțional:

La realizarea plăților electronice în cadrul MPay participă următoarele instituții:

I.P. Agenția de Guvernare Electronică;

Ministerul Finanțelor;

Prestator de servicii de plată;

Prestator de servicii cu plată;

Distribuitor de plăți;

Banca Națională a Moldovei;

În figura 1 este prezentat cadrul instituțional pentru Serviciul Guvernamental de Plăți Electronice MPay.

Fig.1. Cadrul instituțional al infrastructurii guvernamentale de plăți electronice.

1.1.2.2. Fluxuri informaționale și financiare:

Fluxurile financiare din cadrul Serviciului MPay cuprind totalitatea operațiunilor de mișcare a mijloacelor bănești prin etapele tehnologice succesive, de la inițierea plății de către plătitor până la înregistrarea acesteia în conturile de destinație ale beneficiarilor de plăți.

Fluxurile financiare sunt însoțite în permanență de fluxuri informaționale corespondente, care asigură consistența, trasabilitatea și reconciliabilitatea fiecărei tranzacții. Mecanismul funcționează după cum urmează: Prestatorul de Servicii de Plată (PP) notifică Serviciul MPay cu privire la încasarea, restituirea sau distribuirea unei plăți; MPay validează și procesează notificarea, după care informează Prestatorul de Servicii cu Plată (PS) sau Distribuitorul de Plăți (DP) despre finalizarea tranzacției, închizând astfel ciclul informațional. Toate mesajele din cadrul acestor fluxuri sunt transportate prin canale criptate și conțin mecanisme criptografice de semnătură digitală care garantează autenticitatea, integritatea și non-repudierea acestora.

Fiecare mesaj din fluxul informațional include identificatorul instrumentului de plată utilizat la efectuarea tranzacției. Această informație servește atât la calcularea automată a comisioanelor datorate prestatorilor de servicii de plată conform cuantumurilor aprobate, cât și în scopuri de analiză statistică, raportare și audit financiar.

În figura 2 sunt prezentate fluxurile financiare și informaționale pentru încasare plăților prin Serviciul Guvernamental de Plăți Electronice MPay.

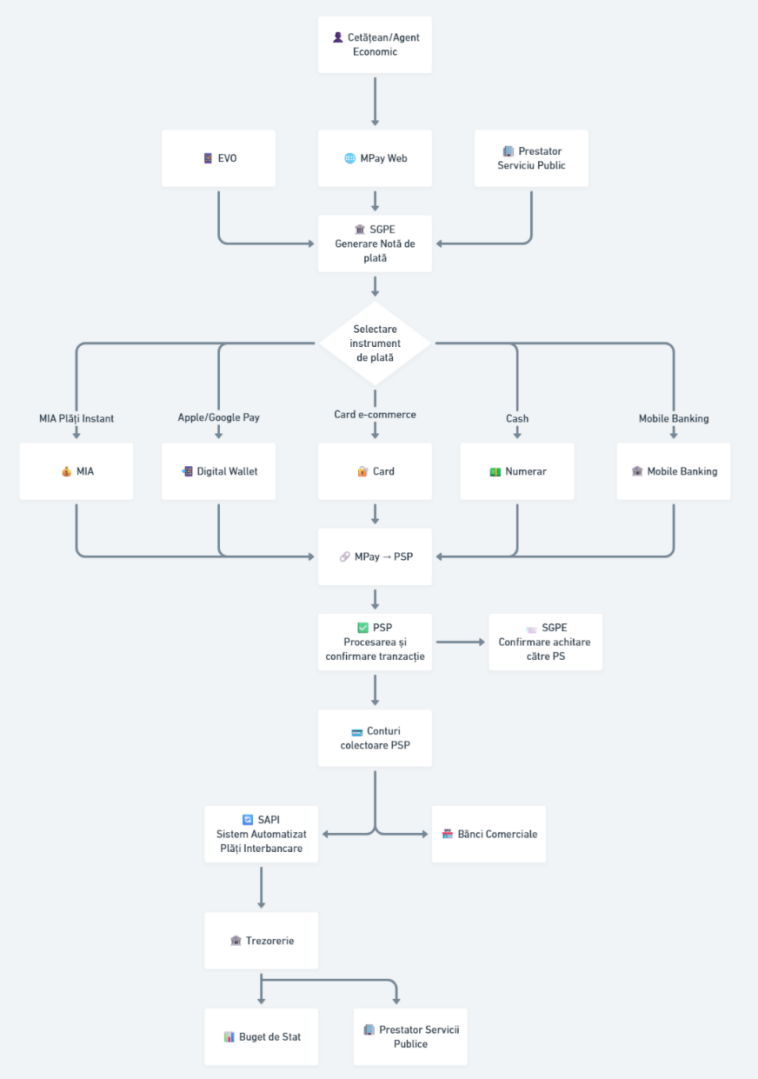

Fig.2. Fluxurile financiare și informaționale pentru încasarea plăților prin serviciul MPay.

În figura 3 sunt prezentate fluxurile financiare și informaționale pentru restituirea plăților prin Serviciul Guvernamental de Plăți Electronice MPay.

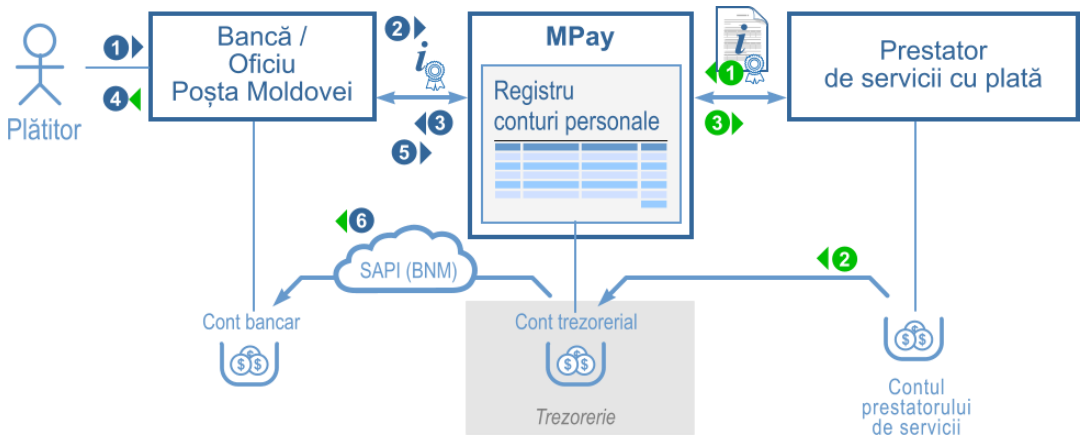

Fig.3. Fluxurile financiare și informaționale pentru restituirea plăților prin serviciul MPay.

În figura 4 sunt prezentate fluxurile financiare și informaționale pentru distribuirea plăților prin Serviciul Guvernamental de Plăți Electronice MPay.

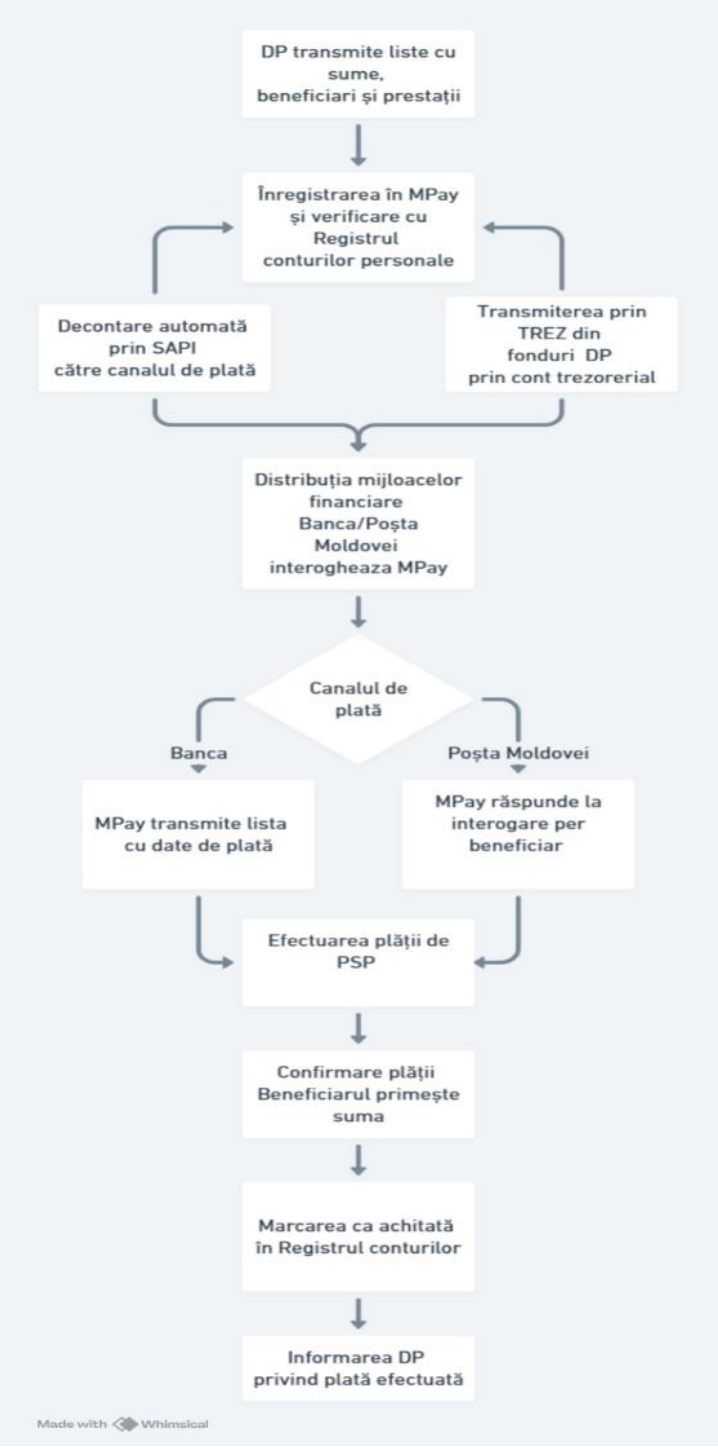

Fig.4. Fluxurile financiare și informaționale pentru distribuirea plăților prin serviciul MPay.

1.1.3. Obiectivele caietului de sarcini

Prezentul caiet de sarcini are ca obiect achiziția serviciilor de suport tehnic, întreținere și mentenanță — corectivă, preventivă și adaptivă — a platformei Guvernamentale de Plăți Electronice MPay, componenta back-office, pentru o perioadă de 12 luni. Scopul este asigurarea funcționării continue, securizate și performante a Serviciului MPay la parametrii de calitate stabiliți, în conformitate cu cerințele tehnice și operaționale descrise în prezentul document.

Prestatorul va primi acces la codul sursă al Serviciului MPay, deținut de Autoritatea Contractantă, și va prelua integral responsabilitatea tehnică pentru corectitudinea, stabilitatea și securitatea oricărei modificări operate asupra acestuia. Accesul la codul sursă se acordă exclusiv în scopul executării obligațiilor contractuale și este guvernat de clauzele de confidențialitate și proprietate intelectuală prevăzute la secțiunile 1.1.4 și 1.1.6.

Prin asumarea prezentului contract, Prestatorul acordă Beneficiarului o garanție asupra întregului Serviciu MPay pe o perioadă de minimum 12 luni de la încetarea contractului. Garanția devine activă de la data intrării în regim de producție a fiecărei modificări implementate de Prestator și se reînnoiește la fiecare intervenție ulterioară asupra sistemului. Prestatorul are obligația de a documenta exhaustiv toate intervențiile tehnice — modificări de cod, configurații, structuri de date, integrări — și de a prezenta această documentație Beneficiarului în forma și termenele stabilite prin contract.

1.1.4. Proprietatea intelectuală

Orice rapoarte și date precum diagrame, schițe, instrucțiuni, planuri, statistici, calcule, baze de date, cerințe tehnice, coduri sursă, design și înregistrări justificative ori materiale achiziționate, compilate ori elaborate de către Prestator sau de către personalul său salariat ori contractat în legătură cu executarea contractului, vor deveni proprietatea exclusivă a AGE, dacă nu se prevede altfel. Orice date stocate în cadrul bazelor de date aferente sistemului MPay sunt proprietatea AGE. Prestatorul nu va păstra copii ale acestor documente ori date şi nu le va utiliza în scopuri care nu au legătură cu contractul fără acordul scris prealabil al AGE.

Prestatorul nu va publica articole referitoare la obiectul contractului în scopuri publicitare sau alte scopuri, nu va face referire la acesta în cursul executării altor servicii pentru terți şi nu va divulga nicio informație furnizată de AGE, fără acordul scris prealabil al acestuia.

Orice rezultate ori drepturi, inclusiv drepturi de autor sau alte drepturi de proprietate intelectuală ori industrială, dobândite în executarea prezentului contract vor fi proprietatea exclusivă a AGE, care le va putea utiliza, publica, cesiona ori transfera în conformitate cu legislația în vigoare, fără limitare geografică ori de altă natură.

1.1.5. Referințe legale

Baza normativ-legislativă, care stă la baza Serviciului Guvernamental de Plăți Electronice MPay constituie legislația națională, tratatele internaționale şi recomandările europene şi internaționale în domeniu. Prevederile normative specifice MPay sunt reglementate de Hotărârea de Guvern nr. 712/2020 cu privire la serviciul guvernamental de plăți electronice (MPay).

1.1.6. Confidențialitate

În cadrul Serviciului MPay sunt operate, în funcție de natura tranzacțiilor și a participanților implicați, următoarele categorii de date protejate:

a) date cu caracter personal ale persoanelor fizice implicate în tranzacțiile de plată; b) date ce constituie secret comercial al participanților la Serviciul MPay; c) date ce constituie

secret fiscal, în conformitate cu legislația fiscală în vigoare; d) date ce constituie secret bancar, în conformitate cu legislația privind serviciile de plată și moneda electronică.

Pe durata executării contractului, precum și după încetarea acestuia, Prestatorul are obligația absolută de a asigura confidențialitatea tuturor datelor din categoriile enumerate mai sus, indiferent de suportul pe care se află (electronic, fizic sau alt format) și indiferent de modalitatea în care acestea au fost accesate. Prestatorul nu va divulga, transmite, copia sau utiliza aceste date în niciun alt scop decât cel strict necesar executării obligațiilor contractuale.

Prestatorul poate pune la dispoziție informații sau documente rezultate din executarea contractului exclusiv persoanelor din cadrul echipei sale care sunt direct implicate în prestarea serviciilor contractate și numai în măsura strict necesară îndeplinirii sarcinilor acestora. Fiecare astfel de persoană va fi obligată contractual față de Prestator la respectarea acelorași standarde de confidențialitate prevăzute în prezentul caiet de sarcini.

1.1.7. Protecția datelor cu caracter personal

În calitate de persoană împuternicită de operator, Prestatorul va prelucra date cu caracter personal strict în conformitate cu instrucțiunile documentate ale Beneficiarului (AGE, în calitate de operator) și cu prevederile legislației aplicabile, respectiv Legea nr. 133/2011 privind protecția datelor cu caracter personal și, începând cu data intrării sale în vigoare (23 august 2026), Legea nr. 195/2024 privind protecția datelor cu caracter personal, care transpune în dreptul național Regulamentul (UE) 2016/679 (GDPR). Prestatorul se obligă să adapteze procedurile și măsurile tehnico-organizatorice la cerințele noii legi anterior datei de 23 august 2026, fără costuri suplimentare pentru Beneficiar.

Prestatorul răspunde solidar cu Beneficiarul pentru orice prelucrare a datelor cu caracter personal efectuată la propria inițiativă, în afara instrucțiunilor Beneficiarului sau contrară principiilor de protecție a datelor cu caracter personal prevăzute de legislația în vigoare.

Prestatorul și angajații, subcontractorii sau colaboratorii acestuia nu vor divulga și nu vor oferi acces la datele cu caracter personal niciunei terțe părți, cu excepția cazurilor în care o asemenea divulgare este prevăzută expres în prezentul contract sau este impusă de lege. Această obligație se menține și după încetarea contractului, pe întreaga perioadă maximă de păstrare a datelor cu caracter personal prevăzută de legislația aplicabilă.

Pe durata contractului și ulterior, Prestatorul va implementa și menține măsuri tehnice și organizatorice adecvate pentru protecția datelor cu caracter personal prelucrate, în conformitate cu Cerințele față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale impuse de Legea nr. 195/2024 la data intrării acesteia în vigoare. Aceste măsuri vor viza cel puțin: controlul accesului la datele cu caracter personal, criptarea datelor în tranzit și în repaus, jurnalizarea accesărilor, și asigurarea integrității și disponibilității datelor.

Retenția și depersonalizarea datelor de tranzacție. Conform HG nr. 712/2020 privind Serviciul Guvernamental de Plăți Electronice MPay, informațiile privind tranzacțiile procesate

prin MPay se păstrează pe o perioadă de 10 ani de la data efectuării tranzacției. La împlinirea acestui termen, Prestatorul are obligația tehnică de a asigura depersonalizarea ireversibilă (pseudonimizarea sau anonimizarea tehnică) a tuturor datelor cu caracter personal asociate tranzacțiilor pentru care termenul de retenție a expirat, sau ștergerea definitivă a acestora, după caz, conform instrucțiunilor Beneficiarului și în conformitate cu politica de retenție agreată. Operațiunea de depersonalizare sau ștergere va fi documentată și raportată Beneficiarului, cu indicarea volumului de date procesate și a metodei utilizate. Nicio copie a datelor cu caracter personal supuse depersonalizării sau ștergerii nu va fi reținută de Prestator după executarea acestei operațiuni.

Prestatorul se obligă să notifice Beneficiarul în cel mult 4 ore de la depistarea oricărui eveniment sau incident de securitate care afectează ori poate afecta confidențialitatea, integritatea sau disponibilitatea datelor cu caracter personal prelucrate în cadrul Serviciului MPay. Notificarea va conține, în măsura posibilului: natura incidentului, categoriile și volumul estimat de date afectate, măsurile imediate întreprinse și acțiunile de remediere planificate. Ulterior, în termen de 72 de ore, Prestatorul va furniza un raport complet privind incidentul. Termenul de 72 de ore este aliniat cu obligația de notificare a Centrului Național pentru Protecția Datelor cu Caracter Personal, prevăzută de Legea nr. 195/2024.

1.1.8. Termen de prestare a serviciilor

Termenul de prestare a serviciilor face obiectul prezentului contract este de 12 luni calendaristice de la data semnării contractului de către ambele părți.

Contractul poate fi reziliat în mod unilateral de către Beneficiar în următoarele cazuri:

a) în cazul refuzului nejustificat al Prestatorului de a presta integral sau parțial serviciile prevăzute în prezentul contract, constatat în scris și neremediat în termen de 10 zile lucrătoare de la notificarea Beneficiarului;

b) cu notificarea prealabilă în scris a Prestatorului cu minimum 30 de zile calendaristice înainte de data rezilierii, în cazul în care finanțarea serviciilor din bugetul de stat este suspendată sau sistată din motive independente de voința Beneficiarului;

c) în cazul încălcării grave sau repetate de către Prestator a obligațiilor de confidențialitate, securitate a datelor sau protecție a datelor cu caracter personal prevăzute în prezentul contract, cu efect imediat de la data notificării scrise.

1.1.9. Penalități

Pentru nerespectarea nivelului minim de disponibilitate garantat pentru luna de raportare, din motive imputabile Prestatorului, acesta va datora Beneficiarului penalitățile calculate conform Tabelului de mai jos. Penalitățile se aplică exclusiv în cazul în care nerespectarea disponibilității este cauzată de factori aflați în zona de responsabilitate a Prestatorului, astfel cum este definită aceasta în secțiunea 2.3.

Penalitățile calculate conform Tabelului nr. 1 reprezintă penalități minime garantate și nu limitează dreptul Beneficiarului de a solicita despăgubiri suplimentare pentru prejudicii dovedite care depășesc valoarea penalităților aplicate.

Penalitățile vor fi calculate și comunicate Prestatorului în primele 5 zile lucrătoare ale lunii următoare perioadei de raportare, pe baza datelor din Sistemul de Service Desk și a raportului de disponibilitate lunară. Prestatorul are dreptul să conteste calculul penalităților în termen de 3 zile lucrătoare de la comunicare, cu prezentarea dovezilor tehnice relevante. În absența unei contestații în termen, penalitățile se consideră acceptate și vor fi reținute din factura lunară aferentă.

Tabelului nr. 1 - Penalități minime garantate

Disponibilitatea sistemului	**% de penalitate din costul lunar al serviciilor**
99,00% - 99,96 %	3%
98,00% - 98,99 %	5%
95,00% - 97,99 %	10%
90,00% - 94,9 %	25%
89,9% sau mai mic	2,5% pentru fiecare 1% al degradării disponibilității până la suma maximă de 25% din costul lunar mediu pe parcursul a ultimelor trei luni cu disponibilitatea minimă de 99,00 % al serviciilor.

Pentru crearea incidentelor de impact critic asupra funcționării serviciului MPay, comunicate imediat Prestatorului și neremediate în decurs de 12 ore, altele decât incidentele care afectează nivelul de disponibilitate minim pentru luna de raportare, Prestatorul va trebui să achite Beneficiarului o penalitate calculată în sumă de 5% din costul lunar al serviciilor.

Dacă incidentul critic asupra funcționării Serviciului MPay, produs din vina Prestatorului, este confirmat de Beneficiar ca având consecințe financiare sau operaționale grave asupra utilizatorilor Serviciului MPay și impune eforturi considerabile de remediere cu implicarea directă a utilizatorilor, ori afectează imaginea statului sau reputația Beneficiarului, penalitatea va fi de 15% din costul lunar al Serviciilor. Consecințele unui incident se consideră grave dacă îndeplinesc cel puțin unul dintre următoarele criterii, documentate de Beneficiar într-un raport detaliat transmis Prestatorului: necesită eforturi de remediere considerabile ce implică direct utilizatorii Serviciului MPay (de exemplu, reintroducerea datelor sau redirecționarea pachetelor de plăți); sau determină o scădere semnificativă a încrederii publice, evidențiată prin rapoarte de presă negative sau petiții primite de la utilizatorii Serviciului MPay.

1.2 Specificațiile serviciilor achiziționate

1.2.1 Generalități

Prezentul capitol stabilește cerințele tehnice și operaționale privind serviciile de suport, întreținere tehnică și mentenanță — corectivă, preventivă și adaptivă — pentru componenta

back-office a Serviciului MPay. Toate serviciile prestate în cadrul contractului trebuie să respecte integral cerințele descrise în continuare și să fie aliniate cu standardele și bunele practici din industrie, inclusiv cadrul ITIL v.3 pentru managementul serviciilor IT.

Perimetrul serviciilor acoperă exclusiv componenta back-office a Serviciului MPay, inclusiv interfețele API ale acesteia, bazele de date aferente, componentele de integrare cu sistemele externe (SAPI, MIA Plăți Instant, Trezorerie, sisteme ale participanților) și infrastructura aplicativă operată de Prestator în limitele responsabilității sale tehnice, astfel cum este definită în prezentul contract și coordonată cu Administratorul Tehnic (STISC).

1.2.2. Cerințe

Denumirea serviciilor	Caracteristicile tehnice/cerințele
Servicii de mentenanța corectivă și preventivă a platformei Guvernamentale de Plăți Electronice pentru component de back-office	1) Elaborarea, actualizarea și menținerea documentației tehnice a sistemului (arhitectură, proceduri operaționale, ghiduri de instalare, API documentation), cu prezentarea versiunii actualizate Beneficiarului la fiecare modificare semnificativă. 2) Oferirea suportului la instalarea, reinstalarea și configurarea inițială a sistemului și a modulelor acestuia conform documentației tehnice. 3) Oferirea suportului la instalarea și configurarea aplicațiilor adiționale necesare pentru rularea sistemului. 4) Menținerea platformei aplicative la cea mai recentă versiune Long-Term Support (LTS) a platformei .NET, inclusiv planificarea și executarea migrărilor de versiune coordonat cu Beneficiarul, în cadrul obligațiilor de mentenanță preventivă. 5) Aplicarea actualizărilor, patch-urilor de securitate și a înnoirilor pentru componentele de sistem, bibliotecile software (NuGet packages, dependențe terțe) și framework-urile utilizate, în termen de maximum 15 zile de la publicarea oficială a acestora. 6) Gestionarea și reînnoirea certificatelor digitale utilizate în cadrul Serviciului MPay (certificate SSL/TLS, certificate de semnătură digitală, certificate ale cheii publice ale participanților). 7) Monitorizarea performanței execuției interogărilor SQL, identificarea și optimizarea interogărilor cu timp de execuție ridicat, analiza

	planurilor de execuție și detectarea blocajelor (deadlocks), conform cerințelor detaliate în secțiunea 2.11. 8) Gestionarea indexurilor bazelor de date: monitorizarea fragmentării, reorganizarea și reconstruirea periodică a indexurilor, crearea de indexuri noi la identificarea degradărilor de performanță, eliminarea indexurilor redundante, conform cerințelor detaliate în secțiunea 2.11. 9) Actualizarea periodică a statisticilor bazelor de date și executarea lucrărilor de mentenanță: verificarea integrității (DBCC CHECKDB), gestionarea spațiului de stocare, arhivarea datelor istorice conform politicii de retenție agreate cu Beneficiarul conform cerințelor detaliate în secțiunea 2.11. 10) Monitorizarea proactivă continuă a disponibilității, performanței și securității componentelor Serviciului MPay (aplicație, baze de date, integrări externe), cu alertare automată la depășirea pragurilor agreate și notificarea imediată a Beneficiarului. 11) Oferirea suportului în asigurarea securității sistemului și confidențialității datelor pentru Serviciul MPay, inclusiv implementarea recomandărilor rezultate din auditurile de securitate și testele de penetrare. 12) Oferirea suportului la schimbul de date informațional între participanții MPay exclusiv în baza certificatelor cheii publice, asigurând autenticitatea și integritatea mesajelor. 13) Întreprinderea acțiunilor proactive de prevenire și a acțiunilor corective pentru funcționarea stabilă a sistemului, inclusiv identificarea și remedierea cauzelor rădăcină (root cause analysis) ale incidentelor repetitive. 14) Oferirea suportului la soluționarea incidentelor și solicitărilor conform nivelurilor de prioritate și SLA stabilite în prezentul caiet de sarcini, cu disponibilitate 24x7 pentru incidentele de prioritate Critică și Înaltă. 15) Analiza problemelor și propunerilor raportate, cu documentarea cauzei, soluției aplicate și măsurilor preventive în Sistemul de Service Desk.

	16) Înlăturarea operativă a erorilor de date, cu documentarea modificărilor efectuate la nivel de bază de date și notificarea Beneficiarului pentru fiecare intervenție directă asupra datelor de producție. 17) Consultarea și acordarea suportului tehnic necesar participanților noi care se conectează prin API la Serviciul MPay, inclusiv în cazul modificărilor de API, cu actualizarea corespunzătoare a ghidurilor tehnice de integrare. 18) Oferirea suportului la configurarea serviciilor și înregistrarea participanților (PP, PS, DP), inclusiv crearea și gestionarea conturilor de acces de diferite tipuri și niveluri de permisiuni. 19) Oferirea suportului în gestionarea funcționalului MIA Plăți Instant în cadrul Serviciului MPay. 20) Oferirea suportului la facilitarea reconcilierii datelor și soluționării divergențelor cu participarea PS, DP, PP și altor participanți ai Serviciului MPay. 21) Oferirea suportului la furnizarea mecanismelor de formare și prezentare a rapoartelor și a descifrărilor adiționale solicitate referitor la notele de plată, operațiuni și loguri, aferente rapoartelor existente. 22) Oferirea consultațiilor și instruirilor de specialitate Beneficiarului în exploatarea și administrarea sistemului, cu elaborarea materialelor de instruire și actualizarea acestora la fiecare modificare semnificativă a sistemului. 23) Prezentarea trimestrială a propunerilor de modernizare a aplicațiilor, serviciilor și bazelor de date aferente Serviciului MPay, cu estimarea efortului și beneficiilor așteptate. 24) Asigurarea asistenței tehnice necesare consumului de date (inclusiv date publice) din Serviciul MPay de către terți autorizați. 25) Depersonalizarea și ștergerea datelor cu caracter personal la expirarea termenului de retenție.
Servicii de mentenanță adaptivă	1) Mentenanța adaptivă cuprinde totalitatea activităților de modificare, extindere și evoluție a Serviciului MPay în scopul asigurării conformității continue cu cerințele funcționale, tehnice, legislative și

	de securitate. Spre deosebire de mentenanța corectivă (remediere erori) și cea preventivă (stabilitate și actualizări), mentenanța adaptivă răspunde nevoilor de schimbare generate de factori externi sau interni și se execută la solicitarea Beneficiarului sau la propunerea motivată a Prestatorului, cu aprobarea prealabilă a Beneficiarului. 2) Implementarea modificărilor funcționale solicitate de Beneficiar ca urmare a schimbărilor în procesele operaționale ale Serviciului MPay sau ale participanților săi (PS, DP, PP, BNM, MF). 3) Dezvoltarea și integrarea de noi funcționalități în back-office-ul MPay, inclusiv noi tipuri de rapoarte, fluxuri de procesare, mecanisme de notificare sau instrumente de administrare, conform specificațiilor agreate. 4) Adaptarea Serviciului MPay la cerințele și reglementările noi emise de autoritățile competente (BNM, Ministerul Finanțelor, alte autorități de reglementare), în termenele impuse de actele normative respective. 5) Implementarea modificărilor necesare pentru integrarea de noi participanți, instrumente de plată sau canale de încasare/distribuire în cadrul Serviciului MPay, inclusiv dezvoltarea sau extinderea interfețelor API aferente. 6) Adaptarea componentelor Serviciului MPay la modificările intervenite în sistemele externe cu care acesta se integrează (SAPI, MIA Plăți Instant, Trezorerie, sisteme ale prestatorilor de servicii de plată etc.). 7) Extinderea sau refactorizarea arhitecturii tehnice a Serviciului MPay în scopul îmbunătățirii performanței, scalabilității sau mentenabilității sistemului, la solicitarea sau cu acordul Beneficiarului. 8) Implementarea măsurilor tehnice necesare pentru conformarea Serviciului MPay la noile cerințe de securitate cibernetică, protecție a datelor cu caracter

	personal sau alte obligații legale aplicabile sistemelor informaționale de stat. 9) Actualizarea mecanismelor de autentificare, autorizare și audit al accesului la componentele Serviciului MPay, ca răspuns la evoluția standardelor de securitate sau la recomandările rezultate din auditurile externe.

Notă: Prestatorul va interacționa cu Administratorul tehnic (STISC) și va îndeplini dispozițiile acestuia coordonate cu Beneficiar, în scopul asigurării suportului și întreținerii tehnice a serviciului MPay – componenta de back-office. Interacțiunea se va asigura prin echipele de suport desemnate de părți.

2. Cerințe privind nivelul minim garantat al serviciilor prestate (SLA)

2.1. Scop

Prezentul capitol definește Cerințele privind Nivelul Minim Garantat al Serviciilor (în continuare — Cerințe SLA), care stabilesc standardele de calitate, disponibilitate și reactivitate pe care Prestatorul este obligat să le respecte pe durata întregului contract.

Cerințele SLA reglementează: nivelurile minime de disponibilitate și performanță ale Serviciului MPay; procesele de interacțiune operațională dintre Prestator și Beneficiar; responsabilitățile individuale ale fiecărei Părți în prestarea, monitorizarea și utilizarea serviciilor; mecanismele de raportare, escaladare și soluționare a incidentelor și solicitărilor.

Cerințele SLA constituie anexă la Contract, sunt parte integrantă a acestuia și au forță juridică egală cu clauzele contractuale. Ambele Părți sunt obligate să le respecte și să le aplice pe toată durata contractului.

Obiectivele principale ale acestor cerințe sunt:

- asigurarea disponibilității și accesibilității neîntrerupte a Serviciului MPay și a tuturor componentelor sale, la nivelurile agreate, pentru toți participanții autorizați;
- garantarea că incidentele, reclamațiile și solicitările de suport sunt adresate, prioritizate și soluționate cu celeritate, cu impact minim asupra continuității operaționale și reputației Serviciului MPay.

2.2. Abrevieri, termeni și definiții

*Rețeaua Telecomunicațională a Autorităților Administrației Publice (**RTAAP**)* — rețeaua de transport date destinată comunicării securizate între autoritățile publice din Republica Moldova, operată de STISC.

Orele de lucru — intervalul 08:00–20:00 în zilele lucrătoare, perioadă în care se înregistrează activitate operațională intensificată în cadrul Serviciului MPay și în care se aplică timpii de reacție și soluționare pentru solicitările de prioritate Medie și Joasă.

Disponibilitatea serviciului (AQS) — procentul de timp, calculat lunar, în care Serviciul MPay este accesibil și funcțional pentru utilizatorii autorizați, conform formulei: AQS = ((Timp total lunar − Timp de indisponibilitate imputabil Prestatorului) / Timp total lunar) × 100%.

Timp de indisponibilitate — orice perioadă în care Serviciul MPay sau o componentă critică a acestuia nu poate fi accesată sau utilizată conform funcționalității garantate, din cauze aflate în zona de responsabilitate a Prestatorului. Nu se includ în calculul indisponibilității: ferestrele de mentenanță planificate și agreate în prealabil cu Beneficiarul, indisponibilitățile cauzate de factori externi zonei de responsabilitate a Prestatorului (infrastructură STISC, SAPI, MIA Plăți Instant, rețele ale participanților).

Fereastră de mentenanță planificată — intervalul de timp notificat Beneficiarului cu minimum 48 de ore în avans, în care pot fi efectuate lucrări de mentenanță cu impact potențial asupra disponibilității, de regulă în afara orelor de vârf operaționale.

2.3. Nivelul de disponibilitate

Prestatorul este responsabil pentru asigurarea funcționării continue și stabile a Serviciului MPay în limitele zonei sale de responsabilitate tehnică, astfel cum este definită în prezentul contract.

Nivelul minim de disponibilitate lunară garantată (AQS) este stabilit la **99,97%**, calculat conform formulei definite la secțiunea 2.2. Nerespectarea acestui nivel atrage aplicarea penalităților prevăzute la secțiunea 1.1.9 și Tabelul nr. 1.

Serviciul MPay se consideră disponibil dacă, în perioada de referință, participanții autorizați pot accesa back-office-ul MPay, pot procesa tranzacții de încasare, restituire și distribuire, iar interfețele API ale sistemului răspund în parametrii de performanță stabiliți.

Prestatorul va implementa și opera un mecanism de monitorizare continuă (24x7) a disponibilității tuturor componentelor Serviciului MPay din zona sa de responsabilitate, cu alertare automată la orice degradare și cu jurnalizarea tuturor evenimentelor de indisponibilitate pentru calculul lunar al AQS.

2.4. Continuitate și restabilire

Prestatorul va elabora și va prezenta Beneficiarului, în termen de 15 zile de la semnarea contractului, un **Plan de Continuitate și Restabilire** pentru Serviciul MPay, care va fi revizuit anual sau ori de câte ori intervin modificări semnificative în arhitectura sistemului.

Planul va dimensiona și documenta cel puțin următorii indicatori:

- **RTO (Recovery Time Objective) = 15 minute** — timpul maxim admis de la depistarea sau comunicarea unui incident până la restabilirea completă a funcționalității Serviciului MPay în zona de responsabilitate a Prestatorului;
- **RPO (Recovery Point Objective) = 0 minute pentru tranzacții financiare** — nicio tranzacție financiară finalizată nu poate fi pierdută în urma unui incident; Prestatorul va asigura mecanisme de persistență și reluare a tranzacțiilor în curs;
- **MTD (Maximum Tolerable Downtime) = 4 ore** — durata maximă de întrerupere tolerată dincolo de care impactul devine critic și ireversibil pentru operațiunile Beneficiarului și ale participanților MPay.

În cazul în care restabilirea completă depășește RTO de 15 minute, Prestatorul va notifica Beneficiarul la intervale de maximum 30 de minute cu privire la stadiul remedierii, cauzele identificate și estimarea timpului de restabilire. La finalizarea incidentului, va elabora un raport post-incident în termen de 24 de ore.

Prestatorul este responsabil să solicite proactiv Beneficiarului resursele tehnice necesare la nivelul platformei MCloud pentru asigurarea indicatorilor de continuitate, coordonând toate solicitările cu Beneficiarul și STISC, cu respectarea restricțiilor tehnologice și a politicilor de utilizare rațională a resurselor.

În cazul pierderii de date, Prestatorul va coordona și va asigura suportul tehnic pentru restabilirea integrală a datelor din copiile de rezervă și din sursele externe relevante (SAPI, MIA Plăți Instant, sisteme ale PP), garantând consistența și integritatea datelor financiare după restabilire.

2.5. Nivelul serviciilor pentru mediul de testare

Prestatorul va configura, menține și actualiza un **mediu de testare dedicat** al Serviciului MPay, pe infrastructura pusă la dispoziție de AGE, destinat următoarelor scopuri: integrarea și testarea noilor participanți (PS, DP, PP) înainte de conectarea în producție; validarea noilor instrumente și modalități de plată ale prestatorilor de servicii de plată; testarea modificărilor și actualizărilor înainte de implementarea în producție.

Mediul de testare va fi funcțional echivalent cu mediul de producție din perspectiva configurației aplicative și a interfețelor API, pentru a garanta că testele efectuate reflectă comportamentul real al sistemului. Datele utilizate în mediul de testare vor fi exclusiv date anonimizate sau sintetice — nu se vor utiliza date reale de producție, inclusiv date cu caracter personal sau date financiare reale ale participanților.

Disponibilitatea mediului de testare va fi asigurată în baza principiului **„cel mai bun efort"** în zilele lucrătoare 08:00–20:00, fără garanții formale de SLA. Întreruperile planificate ale mediului de testare vor fi notificate Beneficiarului cu minimum 4 ore în avans.

2.6. Servicii de suport

2.6.1. Scopul serviciilor de suport

Prestatorul va furniza Beneficiarului servicii complete de suport tehnic pentru operarea back-office-ului MPay, acoperind întregul ciclu de viață al unui incident sau solicitare, de la înregistrare până la închidere și documentare.

Serviciile de suport vor include:

- diagnosticarea, prioritizarea și soluționarea incidentelor și problemelor tehnice apărute în cadrul Serviciului MPay, inclusiv a celor generate de erori software, vulnerabilități de securitate sau degradări de performanță;
- suport tehnic pentru soluționarea reclamațiilor și divergențelor financiare parvenite din partea participanților (PS, DP, PP) sau ale altor terți beneficiari ai Serviciului MPay;
- suport la conectarea tehnică a noilor participanți la Serviciul MPay (PS, DP, PP), inclusiv testarea integrării API și validarea fluxurilor financiare în mediul de testare înainte de activarea în producție;
- suport la reconcilierea datelor financiare și soluționarea discrepanțelor între sistemele participanților și Serviciul MPay.

2.6.2. Serviciul de suport MPay

Beneficiarul va desemna persoane responsabile pentru interacțiunea cu Serviciul de suport al Prestatorului. Prestatorul va desemna un Manager dedicat contractului MPay, care va fi punctul principal de contact pentru escaladări și comunicare operațională.

Serviciul de suport al Prestatorului va fi disponibil după cum urmează:

- Solicitări (prioritate Medie și Joasă): 08:00–20:00, zilele lucrătoare;
- Incidente (prioritate Critică și Înaltă): 24x7, inclusiv weekenduri și sărbători legale.

Prestatorul va asigura următoarele canale de înregistrare a solicitărilor și incidentelor:

- Portal web Service Desk — accesibil 24x7, cu autentificare securizată, disponibil atât pentru Beneficiar cât și pentru STISC;
- Linie telefonică dedicată — disponibilă 24x7 pentru incidente de prioritate Critică și Înaltă;
- Email dedicat — pentru solicitări de prioritate Medie și Joasă, în orele de lucru.

Toate solicitările și incidentele, indiferent de canalul de recepție, vor fi înregistrate obligatoriu în Sistemul de Service Desk în termen de maximum 15 minute de la recepționare. Fiecare ticket va conține: descrierea completă a problemei, prioritatea atribuită, persoana responsabilă din partea Prestatorului, istoricul complet al acțiunilor întreprinse și statusul curent. Beneficiarul și STISC vor avea acces permanent de citire la toate ticketele aferente contractului.

Prestatorul va menține în permanență minimum 2 ingineri de suport disponibili 24x7 pentru preluarea și soluționarea incidentelor de prioritate Critică, cu competențe tehnice acoperind toate componentele Serviciului MPay.

2.6.3. Nivelul serviciilor de suport

Nivelul serviciilor de suport este caracterizat prin doi indicatori principali:

- TR (Timp de Reacție) — intervalul de timp de la înregistrarea solicitării/incidentului până la momentul în care Prestatorul confirmă recepția, diagnostichează situația și comunică Beneficiarului acțiunile planificate pentru soluționare.
- TS (Timp de Soluționare) — intervalul de timp în care Prestatorul finalizează acțiunile din zona sa de responsabilitate pentru remedierea completă a incidentului sau executarea solicitării. TS poate fi extins, motivat, de comun acord cu Beneficiarul, exclusiv în cazul solicitărilor de prioritate Medie și Joasă și numai dacă extensia nu afectează operațiunile financiare ale zilei curente.

Timpii TR și TS se calculează din momentul înregistrării în Sistemul de Service Desk. Pentru incidentele raportate telefonic în afara orelor de lucru, TR se calculează din momentul apelului, nu din momentul înregistrării în sistem.

În funcție de acești parametri, toate notificările de incident vor fi prioritizate de Beneficiar, iar Prestatorul va gestiona, precum urmează în tabelul de mai jos:

Tabel 1 — Niveluri de serviciu pentru INCIDENTE

Prioritate	**Descriere**	**TR**	**TS**	**Forma de raportare**
Critică	Incident care a dus la indisponibilitatea completă a Serviciului MPay pentru majoritatea utilizatorilor sau participanților; sau incident de securitate cu impact imediat asupra integrității datelor financiare.	2 - 5 min	30 min – 1 oră	Telefon, Email, Service Desk
Înaltă	Incident care a dus la indisponibilitatea parțială a Serviciului MPay (număr limitat de utilizatori sau participanți afectați); sau existența unor riscuri majore de securitate care pot compromite funcționarea sau integritatea Serviciului MPay.	10 -15 min	2 ore	Telefon, Email, Service Desk
Medie	Evenimente care pot evolua spre indisponibilitate sau risc de securitate dacă nu sunt adresate; degradări de performanță fără impact imediat asupra tranzacțiilor.	2 - 4 ore	8 – 24 ore	Email, Service Desk

Joasă	Orice alt incident sau solicitare cu impact nesemnificativ și fără risc de escaladare.	1 zi lucrătoare	3 zile lucrătoare	Email, Service Desk

Toate solicitările de suport și solicitări vor fi prioritizate de Beneficiar, iar Prestatorul le va gestiona, precum urmează în tabelul de mai jos:

Tabel 2 — Niveluri de serviciu pentru SOLICITĂRI

Prioritate	**Descriere**	**TR**	**TS**	**Forma de raportare**
Critică	Necesitate operațională urgentă care, nerezolvată, duce la imposibilitatea procesării încasărilor, confirmărilor, debitărilor, distribuirilor sau restituirilor pentru mai mulți participanți PP/PS sau mai multe plăți simultan.	10 - 15 min	30 min – 1 oră	Telefon, Email, Servicedesk
Înaltă	Necesitate operațională care afectează un număr limitat de plăți sau un singur participant PP/PSP; sau riscuri majore care pot bloca procesarea unor plăți individuale prin Serviciul MPay.	15 – 25 min	2 ore	Telefon, Email, Servicedesk
Medie	Conectarea de noi participanți la Serviciul MPay; alte solicitări operaționale necesare închiderii zilei operaționale (SAPI, Trezorerie, MT103), cu condiția că executarea lor nu pune în pericol termenul de închidere.	2 - 4 ore	8 – 24 ore	Email, Servicedesk
Joasă	Orice altă solicitare operațională fără impact imediat asupra tranzacțiilor sau participanților.	1 zi lucrătoare	5 zile lucrătoare	Email, Servicedesk

2.6.4. Stabilirea priorității de soluționare a incidentelor

Prioritatea unui incident sau solicitări se determină prin combinarea a doi factori evaluați de Beneficiar la momentul înregistrării:

Gradul de urgență al incidentului	**Nivelul impactului incidentului**		
	Înalt	**Mediu**	**Redus**
Înalt	Critic	Înalt	Mediu

Mediu	Înalt	Mediu	Jos
Redus	Mediu	Jos	Jos

Beneficiarul are dreptul să reclasifice prioritatea unui incident în orice moment pe durata soluționării, cu notificarea imediată a Prestatorului. Prestatorul poate propune reclasificarea, dar decizia finală aparține Beneficiarului.

2.6.5. Evaluarea urgenței incidentului/solicitării

Gradul de urgență	**Descrierea gradului de urgență**
Înalt	Un incident/solicitare este calificată ca având gradul de urgență *Înalt* în unul sau mai multe din următoarele cazuri: • pagubele cresc sau vor crește extrem de rapid fără intervenție imediată; • există operațiuni absolut necesare continuității afacerii Beneficiarului care nu pot fi amânate; • riscuri legale majore sau de securitate a informației pot fi prevenite doar prin reacție imediată.
Mediu	Un incident/solicitare este calificată ca având gradul de urgență *Mediu* în unul sau mai multe din următoarele cazuri: • pagubele cresc treptat în timp; • există operațiuni importante care trebuie executate în cursul zilei; • reacția operativă poate preveni riscuri legale sau de securitate moderate.
Redus	Un incident/solicitare este calificată ca având gradul de urgență *Redus* în unul sau mai multe din următoarele cazuri: • pagubele nu cresc sau cresc neglijabil în timp; • nu există operațiuni imediate afectate; • riscurile legale și de securitate sunt nesemnificative sau inexistente.

2.6.6. Evaluarea impactului incidentului

Nivelul impactului	**Descrierea nivelului impactului**
Înalt	Un incident/solicitare este calificat (ă) ca având nivelul impactului *Înalt* în unul sau mai multe din următoarele cazuri: • activitățile-cheie ale Beneficiarului sunt sau vor fi întrerupte; • incidentul este vizibil din exteriorul organizației și afectează participanți externi, reputația sau imaginea Serviciului MPay; • există riscuri legale și financiare majore; • s-au produs sau se pot produce pierderi semnificative de date critice.

Mediu	Un incident/solicitare este calificat ca având nivelul impactului *Mediu* în unul sau mai multe din următoarele cazuri: • activitățile importante sunt desfășurate cu dificultate sau vor fi întrerupte; • incidentul afectează o parte din utilizatorii interni și un număr limitat de participanți externi; • există riscuri legale și financiare semnificative; • pierderile de date sunt nesemnificative.
Redus	Un incident/solicitare este calificat ca având nivelul impactului *Redus* în unul sau mai multe din următoarele cazuri: • doar activități interne nesemnificative sunt afectate; • incidentul nu este vizibil extern; nu există riscuri legale sau financiare imediate.

2.6.7. Suport la soluționarea incidentelor, erorilor și vulnerabilităților

Un incident aferent Serviciului MPay reprezintă orice eveniment — planificat sau neplanificat — care a dus sau ar fi putut duce la degradarea unuia sau mai multor parametri de calitate ai Serviciului MPay. Incidentele includ atât evenimentele sesizate de Beneficiar sau de participanți, cât și cele identificate proactiv de Prestator în cadrul activităților de monitorizare și mentenanță.

Parametrii de calitate ai Serviciului MPay susceptibili la incidente sunt:

Disponibilitatea — capacitatea Serviciului MPay și a componentelor sale de a recepta și procesa solicitările de inițiere, confirmare, restituire și distribuire a plăților, inclusiv capacitatea de a confirma către PSP plățile încasate de PP, în mod continuu și în parametrii SLA stabiliți.

Accesibilitatea — capacitatea Serviciului MPay de a fi accesat și utilizat de entitățile autorizate (PP, PS, DP și alte entități) din rețelele agreate, cu mijloacele de autentificare stabilite, cu accesul la funcționalitățile și datele corespunzătoare rolului fiecărei entități.

Performanța — capacitatea Serviciului MPay de a procesa cererile de servicii în limitele timpilor de răspuns stabiliți, fără degradare perceptibilă a vitezei sau calității procesării, inclusiv în perioadele de vârf operațional.

Securitatea — capacitatea Serviciului MPay de a asigura confidențialitatea, integritatea, disponibilitatea, autenticitatea și non-repudierea informațiilor și tranzacțiilor procesate, inclusiv protecția împotriva accesului neautorizat, a atacurilor cibernetice și a scurgerilor de date.

Prestatorul va gestiona, investiga și soluționa toate incidentele din zona sa de responsabilitate, documentând pentru fiecare incident: descrierea completă a simptomelor, cronologia evenimentelor, cauza rădăcină identificată (root cause), acțiunile de remediere

aplicate, măsurile preventive propuse și timpul de soluționare efectiv. Această informație va fi inclusă în **Raportul lunar de activitate** prezentat Beneficiarului și în **Raportul post-incident** elaborat în termen de 24 de ore de la închiderea oricărui incident de prioritate Critică sau Înaltă.

Toate incidentele, indiferent de sursa sesizării și de prioritate, vor fi înregistrate obligatoriu în Sistemul de Service Desk al Prestatorului. Prestatorul va înregistra inclusiv incidentele identificate proactiv în cadrul activităților proprii de monitorizare și mentenanță, chiar dacă acestea nu au fost sesizate de Beneficiar. Incidentele apărute în afara orelor de lucru vor fi preluate și gestionate activ de Prestator pentru prioritățile **Critică și Înaltă**; incidentele de prioritate Medie și Joasă apărute în afara orelor de lucru vor fi înregistrate și gestionate la reluarea programului.

Acordarea serviciilor de suport se va efectua în baza unui Regulament de Suport elaborat de Prestator pe baza cerințelor din prezentul caiet de sarcini și agreat de ambele Părți. Regulamentul va fi prezentat Beneficiarului în termen de 10 zile calendaristice de la data semnării contractului și va intra în vigoare după aprobarea scrisă a Beneficiarului. Regulamentul va fi revizuit anual sau ori de câte ori intervin modificări semnificative în procesele operaționale.

Regulamentul va acoperi obligatoriu următoarele aspecte:

Aspectul	**Descrierea**
Definiții și scopuri pentru serviciile de operare a mediului de testare și de producție	Definițiile complete pentru fiecare activitate de operare a mediului: instalare, implementare, monitorizare ordinară, mentenanță planificată — cu enumerarea activităților și responsabilităților aferente fiecărui mediu.
Criteriile serviciului de suport	Criteriile de notificare a Beneficiarului, perioadele și duratele lucrărilor de mentenanță planificată, ferestrele de mentenanță agreate — separat pentru mediul de testare și cel de producție.
Criterii de acordare și executare a fiecărui tip al serviciului de suport	Timpii de reacție (TR) și timpii de soluționare (TS) pentru fiecare tip de suport și nivel de prioritate, în conformitate cu Tabelele 1 și 2 din secțiunea 2.6.3.
Priorități	Criteriile de definire a priorităților pentru serviciile de operare și suport, pe baza matricei impact-urgență din secțiunea 2.6.4.
Regulile de categorizare a incidentelor, reclamațiilor și solicitărilor	Reguli clare pentru repartizarea automată și manuală a ticketelor către specialiștii responsabili, inclusiv regulile de escaladare și re-alocare.
Orarul de operare a serviciului de suport	Programul detaliat de lucru al serviciului de suport, inclusiv acoperirea 24x7 pentru incidente critice și înalte și acoperirea în orele de lucru pentru solicitări.
Procedurile de readresare	Procedurile de escaladare internă și externă a ticketelor nerezolvate în TR/TS, inclusiv pragurile de timp la care

	escaladarea devine obligatorie și persoanele de contact pentru fiecare nivel de escaladare.
Procedurile de prestare a serviciilor de suport de soluționare a incidentelor și a reclamațiilor	Flux complet: (1) Înregistrare; (2) Categorizare; (3) Prioritizare; (4) Diagnosticare inițială; (5) Readresare după caz; (6) Investigare și diagnosticare completă + Root Cause Analysis; (7) Rezolvare și restabilire; (8) Verificare post-remediere; (9) Închidere și documentare.
Procedura de executare a solicitărilor	Flux complet: (1) Înregistrare; (2) Categorizare; (3) Identificarea sursei și a contextului; (4) Prioritizare; (5) Readresare după caz; (6) Executare; (7) Validare cu Beneficiarul; (8) Închidere și documentare.
Gestionarea cunoștințelor (Knowledge Management)	Instrucțiunile de completare și menținere a bazei de cunoștințe (knowledge base) și a bazei de erori cunoscute (known errors database), inclusiv criteriile de publicare a articolelor noi și frecvența de revizuire.
Persoane responsabile din ambele părți	Desemnarea nominală a minimum 2 persoane responsabile din fiecare parte (Prestator și Beneficiar) pentru operare și suport, cu datele de contact și disponibilitatea acestora.
Canale de comunicare	Descrierea completă a canalelor utilizate pentru comunicarea incidentelor, reclamațiilor și solicitărilor (portal web, telefon, email, monitoring automat), cu indicarea canalului obligatoriu pentru fiecare prioritate.

2.7. Mentenanța adaptivă

Mentenanța adaptivă cuprinde totalitatea activităților de modificare, extindere și evoluție controlată a Serviciului MPay, executate ca răspuns la cerințe funcționale, tehnice, legislative sau de securitate noi, apărute pe durata contractului. Toate modificările, indiferent de amploare, vor fi gestionate printr-un proces formal de management al schimbărilor, agreat de ambele Părți, bazat pe bunele practici ITIL v.3 și adaptat specificului unui sistem financiar critic de stat.

2.7.1. Principii generale ale managementului modificărilor

Orice modificare la nivelul componentelor Serviciului MPay — cod sursă, configurații, structuri de baze de date, integrări externe, infrastructură aplicativă — va fi implementată exclusiv conform procesului descris în prezenta secțiune. Nicio modificare nu va fi aplicată în mediul de producție fără parcurgerea integrală a etapelor obligatorii și fără aprobarea prealabilă a Beneficiarului.

Modificările cu impact potențial semnificativ asupra disponibilității, performanței, securității sau integrității datelor Serviciului MPay vor fi supuse unui proces extins de evaluare

și autorizare, care include obligatoriu: testarea în mediul de testare, planul de implementare, planul de rollback și revizuirea post-implementare.

Toate intervențiile tehnice asupra Serviciului MPay — indiferent de natura lor (corective, preventive sau adaptive) — respectă următoarele principii obligatorii, de la care nu se admit derogări:

a) Livrare exclusiv prin pipeline CI/CD - Orice modificare la nivelul codului sursă, configurațiilor sau bazelor de date se livrează exclusiv prin pipeline-ul CI/CD lansat din repozitoriul pus la dispoziție de Beneficiar. Nu se acceptă intervenții manuale prin FTP, SCP sau copiere directă de fișiere în mediile de staging sau producție. Orice tentativă de intervenție manuală directă în mediul de producție, fără parcurgerea pipeline-ului aprobat, constituie încălcare gravă a contractului.

b) Build & Deploy prin template-uri standardizate - Procesul de compilare, testare și livrare (Build & Deploy) se realizează în mod obligatoriu și exclusiv prin utilizarea template-urilor de pipeline (Build) și template-urilor Helm pentru livrare și instalare, puse la dispoziție de Beneficiar. Prestatorul poate adapta aceste template-uri strict în limitele necesităților tehnice ale proiectului, cu obligația de a menține compatibilitatea cu standardele și structura stabilite de Beneficiar. Este strict interzisă utilizarea oricăror alte mecanisme, scripturi sau modalități alternative de compilare, livrare și desfășurare.

c) Gestionarea codului sursă în repozitoriul Beneficiarului - Codul sursă se livrează exclusiv în repozitoriul pus la dispoziție de Beneficiar, cu istoricul complet al commit-urilor și mesaje de commit descriptive, cu referință la ticketul din sistemul de Issue Tracking. Nu se acceptă livrarea prin arhive, stick USB sau orice altă modalitate alternativă. La finalizarea contractului, repozitoriul va conține istoricul integral al tuturor modificărilor efectuate pe durata contractului.

d) Calitatea livrărilor — coverage minim obligatoriu - Acceptanța oricărei livrări este condiționată de trecerea cu succes a tuturor testelor automate în pipeline, cu un **coverage minim de 80% pentru business logic**. Livrările care nu îndeplinesc acest prag vor fi respinse automat de pipeline și returnate Prestatorului pentru remediere, fără a fi considerate livrate.

e) Păstrarea arhitecturii originale - Arhitectura originală a sistemului stack tehnologic, pattern-uri de proiectare, structura de componente — se păstrează integral pe durata contractului. Orice modificare arhitecturală majoră (migrare framework, schimbarea arhitecturii monolith/microservices, rescrierea unor module majore) necesită reclasificarea solicitării, elaborarea unei evaluări separate de risc și aprobarea prealabilă scrisă a Beneficiarului, înainte de demararea oricărei activități.

f) Documentarea obligatorie a intervențiilor - Prestatorul va menține un **Registru al Modificărilor** actualizat în timp real în Sistemul de Service Desk, accesibil permanent Beneficiarului și STISC în regim de citire. Registrul va conține pentru fiecare modificare:

identificatorul unic, descrierea, tipul (corectivă/preventivă/adaptivă), statusul, datele de implementare planificate și efective, rezultatul revizuirii post-implementare și referința la documentația tehnică aferentă.

2.7.2. Procesul de management al modificărilor

Toate solicitările de modificare, indiferent de sursă, vor fi înregistrate în Sistemul de Service Desk și vor parcurge obligatoriu următoarele etape:

Etapa 1 — Înregistrarea solicitării de modificare Solicitarea poate fi inițiată de Beneficiar sau de Prestator în baza unei necesități identificate. Prestatorul va înregistra solicitarea în Service Desk cu descrierea problemei sau necesității, contextul tehnic și operațional, impactul estimat și urgența. Solicitările inițiate de Prestator vor fi supuse aprobării prealabile a Beneficiarului înainte de demararea oricărei activități.

Etapa 2 — Analiza și estimarea Prestatorul va examina solicitarea în termen de maximum 3 zile lucrătoare (pentru solicitări de complexitate medie) și va prezenta descrierea detaliată a soluției tehnice propuse, resursele necesare (om-ore pe roluri), planul de lucru estimat, riscurile identificate și măsurile de atenuare, dependențele față de sisteme externe și impactul asupra participanților MPay.

Etapa 3 — Aprobarea Beneficiarului Beneficiarul va comunica Prestatorului decizia sa (aprobare, respingere sau solicitare de clarificări) în termen de maximum 5 zile lucrătoare. Modificările pot fi aprobate, respinse sau returnate cu solicitare de revizuire. Nici o activitate de dezvoltare nu va fi demarată înainte de aprobarea Beneficiarului.

Etapa 4 — Planificarea După aprobarea Prestatorul va elabora: planul detaliat de implementare cu termene, planul de rollback cu pașii exacți de revenire la starea anterioară și criteriile de activare a acestuia, checklist-ul de implementare cu punctele critice de verificare pe parcursul și imediat după implementare — revizuit și validat de ambele Părți. Planificarea va stabili fereastra de implementare (preferabil în afara orelor de vârf operaționale) și va fi comunicată Beneficiarului cu minimum 48 de ore înainte.

Etapa 5 — Executarea dezvoltării Prestatorul va executa lucrările de dezvoltare conform planului aprobat, cu respectarea standardelor de cod, a politicilor de securitate și a arhitecturii Serviciului MPay. Toate modificările de cod vor fi gestionate în sistemul de versionare (repository) cu mesaje de commit descriptive și referința la ticketul din Service Desk.

Etapa 6 — Implementarea și acceptanța

a. Implementarea modificărilor în mediul de testare al Beneficiarului, cu notificarea acestuia și furnizarea instrucțiunilor de instalare;

b. Executarea testelor automate de regresie de către Prestator, în baza suitei de teste menținute și actualizate continuu, cu scopul de a demonstra că modificarea nu a degradat funcționalitățile existente;

c. Testarea de acceptanță funcțională de către Beneficiar, cu implicarea utilizatorilor operaționali ai Serviciului MPay, pe baza criteriilor de acceptanță definite;

d. Aprobarea implementării în producție de către Beneficiar, după finalizarea cu succes a testării de acceptanță;

e. Implementarea în mediul de producție conform ferestrei de mentenanță agreate, cu monitorizare activă în primele 2 ore post-implementare;

f. Revizuirea finală și acceptarea formală a modificării de către Beneficiar, cu închiderea ticketului în Service Desk și actualizarea Registrului Modificărilor.

Etapa 7 — Revizuirea post-implementare (Lessons Learned) În termen de 5 zile lucrătoare de la implementarea în producție, Prestatorul va elabora o notă de revizuire post-implementare care va documenta: dacă modificarea a atins obiectivele propuse, eventualele devieri față de plan, problemele întâmpinate și soluțiile aplicate, lecțiile învățate și propunerile de îmbunătățire a procesului.

2.8. Cerințe privind experiența Furnizorului și personalului echipei

Serviciile care fac obiectul prezentului contract vor fi prestate de o companie cu sediul sau reprezentanță legală în Republica Moldova, cu capacitate tehnică dovedită în mentenanța și dezvoltarea de sisteme informatice complexe, în special în sectorul financiar-guvernamental.

Cerințe obligatorii pentru companie:

- Minimum **5 (cinci) ani** de experiență continuă în implementarea și mentenanța de sisteme informatice similare pentru instituții guvernamentale, organizații neguvernamentale sau clienți din sectorul privat;
- Cel puțin **3 (trei) proiecte similare** finalizate cu succes, care să demonstreze capacitate în: mentenanța sistemelor informatice enterprise, implementarea interfețelor de schimb de date (API), migrarea și integrarea datelor cu resurse informaționale de stat — demonstrate prin scrisori de referință sau contracte relevante;
- Personalul propus va demonstra minimum **1 an de experiență** în cadrul companiei ofertante și implicare dovedită în cel puțin un proiect similar;
- Personalul cheie (Manager de Proiect) va fi capabil să comunice fluent în limbile **română și engleză**; cunoașterea limbii ruse constituie avantaj.

Compania va propune o echipă dedicată exclusiv contractului MPay, disponibilă pe toată durata acestuia. Înlocuirea oricărui membru al echipei cheie va fi notificată Beneficiarului cu minimum 15 zile lucrătoare în avans și va fi supusă aprobării scrise a acestuia. Înlocuitorul propus va îndeplini cel puțin cerințele minime ale rolului respectiv, iar perioada de tranziție va include minimum 10 zile lucrătoare de suprapunere documentată.

Echipa minimă obligatorie: Manager de Proiect, Senior Software Development Engineer, DevOps Engineer, Database Administrator, QA Engineer.

Cerințe minime pentru Echipa

Manager de Proiect	
Calificări și abilități	• Studii universitare în domeniul TI, economic sau management, confirmate prin diplomă de licență sau masterat. • Certificare în management de proiect (PMP, PRINCE2 sau echivalent) constituie avantaj. • Cunoașterea cadrului ITIL v.3 sau v.4 la nivel Foundation constituie avantaj. • Comunicare fluentă în română și engleză; rusa constituie avantaj.
Experiența profesională	• Minimum 7 (șapte) ani de experiență profesională în domeniul TI sau management de proiecte. • Minimum 3 (trei) proiecte gestionate cu succes în calitate de manager de proiect sau business analyst, în domeniul implementării sau mentenanței de sisteme informatice pentru sectorul public sau financiar-bancar, cu valoare contractuală demonstrabilă.
Responsabilități cheie în cadrul contractului	• Va fi punctul unic de contact al Prestatorului față de Beneficiar (AGE) și față de Administratorul Tehnic (STISC). • Asigură coordonarea operațională a echipei tehnice, respectarea SLA-urilor contractuale, elaborarea și prezentarea rapoartelor lunare de activitate, participarea la ședințele lunare de review și gestionarea procesului de escaladare. • Este contactabil în zilele lucrătoare 08:00–18:00 și disponibil pentru notificări în cazul incidentelor critice 24x7.
Senior Software Development Engineer	
Calificări și abilități	• Studii universitare în domeniul tehnologiei informației sau ingineriei software, confirmate prin diplomă. • Cunoștințe tehnice obligatorii demonstrate: platforma .NET (versiunea LTS curentă), ASP.NET MVC Core, Blazor, ADO.NET, SQL Server (interogări complexe, proceduri stocate, optimizare), REST API design și implementare, autentificare și autorizare (OAuth 2.0, certificate digitale, semnătură digitală). • Cunoașterea principiilor SOLID, a pattern-urilor de proiectare și a practicilor de clean code. • Experiență cu sisteme de versionare Git, cu strategii de branching (GitFlow sau echivalent) și cu procesele de code review. • Cunoașterea principiilor de securitate în dezvoltarea software (OWASP Top 10, input validation, protecție împotriva injection attacks). Experiență cu scrierea testelor automate unitare și de integrare, cu coverage minim 80% pentru business logic.
Experiența profesională	• Minimum 7 (șapte) ani de experiență în dezvoltarea software pe platforma .NET.

	• Minimum 3 (trei) proiecte similare finalizate în calitate de lider tehnic sau senior developer, pentru sisteme cu integrări complexe cu sisteme externe prin API. • Experiență dovedită în lucrul cu sisteme financiare sau de plăți electronice constituie avantaj major. • Cunoașterea specificului integrărilor cu sisteme guvernamentale (MConnect, SAPI, MIA Plăți Instant) constituie avantaj.
Responsabilități cheie în cadrul contractului	• Asigură implementarea tuturor modificărilor de cod conform principiilor din secțiunea 2.7.1; • Menține și actualizează suita de teste automate de regresie. • Răspunde de integritatea arhitecturală a sistemului și alertează Managerul de Proiect și Beneficiarul la orice solicitare cu potențial impact arhitectural major. • Asigură continuitatea tehnică prin documentarea detaliată a soluțiilor implementate și prin menținerea actualizată a documentației tehnice.
	DevOps Engineer
Calificări și abilități	• Studii universitare în domeniul tehnologiei informației, confirmate prin diplomă. • Cunoștințe tehnice obligatorii demonstrate: Azure DevOps (pipeline-uri CI/CD, artifact management, release management), Helm Charts (crearea și gestionarea template-urilor de livrare), Kubernetes (administrare clustere, deployment, troubleshooting), Windows Server și Linux (administrare, hardening), NGINX (configurare, load balancing, SSL termination), Docker și gestionarea imaginilor de container (inclusiv imagini minimizate Chiselled Ubuntu). • Cunoașterea principiilor de securitate a infrastructurii: gestiunea secretelor, rotirea certificatelor, hardening OS, principiul privilegiului minim. • Experiență cu sisteme de monitorizare și observabilitate (Prometheus, Grafana, ELK Stack sau echivalente).
Experiența profesională	• Minimum **5 (cinci) ani** de experiență în administrarea infrastructurilor și pipeline-urilor CI/CD pentru sisteme informatice complexe. • Minimum **2 (două) proiecte** similare în care a asigurat operarea infrastructurii DevOps pentru sisteme în producție cu cerințe de disponibilitate ridicată. • Experiență dovedită în implementarea și operarea pipeline-urilor CI/CD cu gates de calitate automate (teste, coverage, scanare de securitate).

Responsabilități cheie în cadrul contractului	• Administrează și menține pipeline-urile CI/CD ale Beneficiarului utilizate pentru livrarea Serviciului MPay. • Asigură că nicio livrare în producție nu se realizează în afara pipeline-ului aprobat. • Monitorizează continuu infrastructura aplicativă a Serviciului MPay și gestionează alertele de disponibilitate și performanță. • Execută lucrările planificate de mentenanță a infrastructurii în ferestrele agreate cu Beneficiarul. • Deține competențe de securitate cibernetică și răspunde de implementarea cerințelor tehnice de securitate
DataBase Administrator	
Calificări și abilități	• Studii universitare în domeniul tehnologiei informației, confirmate prin diplomă. • Cunoștințe tehnice obligatorii demonstrate: SQL Server (administrare instanțe, configurare, tuning), scrierea și optimizarea interogărilor SQL complexe, analiza și optimizarea planurilor de execuție (execution plans, Query Store), managementul indexurilor (fragmentare, REORGANIZE, REBUILD, statistici), proceduri stocate și funcții SQL, backup și restaurare (strategii full/differential/log, testarea restaurărilor), configurarea și monitorizarea SQL Server Agent jobs, gestionarea spațiului de stocare și capacity planning • Cunoașterea principiilor de securitate a bazelor de date: control acces, auditare, criptare date în repaus.î • Cunoașterea conceptelor de depersonalizare și anonimizare a datelor cu caracter personal în baze de date relaționale.
Experiența profesională	• Minimum **7 (șapte) ani** de experiență în administrarea bazelor de date SQL Server în medii de producție cu volum ridicat de tranzacții. • Minimum **2 (două) proiecte** similare în care a ocupat rolul de DBA principal pentru sisteme informatice integrate cu tranzacții financiare sau date sensibile. • Experiență dovedită în optimizarea performanței bazelor de date cu volume mari de date istorice.
Responsabilități cheie în cadrul contractului	• Execută integral activitățile de mentenanță a bazelor de date descrise în secțiunea 2.11: gestionarea indexurilor, actualizarea statisticilor, monitorizarea performanței interogărilor, verificări de integritate, capacity planning. • Implementează și operează mecanismul tehnic de depersonalizare a datelor cu caracter personal la expirarea termenului de retenție. • Asigură integritatea datelor pe durata migrărilor de schemă și a intervențiilor de mentenanță adaptivă. • Testează săptămânal integritatea backup-urilor prin restaurări în mediul de testare și raportează orice eșec al job-urilor automate.

QA Tester	
Calificări și abilități	• Studii superioare tehnice sau universitare în domeniul tehnologiei informației, confirmate prin diplomă. • Cunoștințe tehnice obligatorii demonstrate: elaborarea și menținerea suitelor de teste automate (unit tests, integration tests, regression tests) pe platforma .NET, cu instrumente de tip xUnit, NUnit sau MSTest; măsurarea și raportarea code coverage cu instrumente integrate în pipeline CI/CD; elaborarea planurilor de testare, a cazurilor de test și a rapoartelor de testare; testare API (REST) cu instrumente de tip Postman, RestSharp sau echivalente; testare de performanță și load testing cu instrumente de tip k6, JMeter sau echivalente; identificarea, documentarea și urmărirea defectelor în sistemul de Issue Tracking al Beneficiarului. • Experiență cu testarea sistemelor financiare sau de plăți — verificarea consistenței tranzacțiilor, reconcilierii și rapoartelor financiare — constituie avantaj major.
Experiența profesională	• Minimum **3 (trei) ani** de experiență în testarea calitativă a sistemelor informatice complexe, cu accent pe testare automatizată. • Minimum **2 (două) proiecte** similare în care a contribuit la implementarea sau menținerea unei suite de teste automate pentru un sistem informatic integrat în producție, cu demonstrarea atingerii unui coverage de minimum 80% pentru business logic. • Experiență în testarea integrărilor API cu sisteme externe. Experiență în elaborarea testelor de acceptanță funcțională cu implicarea utilizatorilor finali.
Responsabilități cheie în cadrul contractului	• Menține și actualizează continuu suita de teste automate de regresie a Serviciului MPay, asigurând că orice modificare de cod este însoțită de teste actualizate sau noi, cu menținerea coverage-ului minim de 80% pentru business logic. • Elaborează și execută planurile de testare pentru fiecare modificare de mentenanță adaptivă, inclusiv testele de integrare cu sistemele externe. • Efectuează periodic teste de performanță și load testing pentru a valida că modificările nu degradează capacitatea de procesare a Serviciului MPay în perioadele de vârf.

2.9. Auditări externe

Beneficiarul are dreptul să solicite auditări externe independente ale Prestatorului în orice moment pe durata contractului, fără obligația de a justifica decizia. Obiectivele auditurilor pot include:

- verificarea că Prestatorul menține capacitatea tehnică și organizatorică necesară prestării serviciilor la nivelul agreat prin SLA;

- evaluarea adecvării și eficacității Planului de Gestiune a Riscurilor de Securitate al Prestatorului;
- verificarea conformității cu cerințele de protecție a datelor cu caracter personal și cu obligațiile de confidențialitate din prezentul contract;
- evaluarea maturității proceselor de management al modificărilor, incidentelor și continuității serviciului.

Costurile auditorului extern sunt suportate de Beneficiar. Prestatorul este obligat să coopereze integral cu auditorii desemnați: va pune la dispoziție documentația solicitată, va asigura accesul la sediile și sistemele relevante, va aloca personalul necesar pentru interviuri și demonstrații de proceduri, în termenele stabilite de Beneficiar.

Suplimentar, la solicitarea motivată a Beneficiarului, Prestatorul va comanda și va prezenta Beneficiarului o opinie de audit independent (echivalent SOC 2 Type II sau ISAE 3402, înlocuitor al standardului SAS 70 care nu mai este în vigoare din 2011), emisă de un auditor terț calificat, privind capacitatea Prestatorului de a presta serviciile la nivelul agreat. Costurile acestui audit sunt suportate de Prestator.

2.10. Suport la soluționarea reclamaților și divergențelor

În cazul reclamațiilor și divergențelor privind tranzacțiile procesate prin Serviciul MPay — inclusiv discrepanțe financiare, plăți neconfirmate, restituiri contestate sau erori de distribuire — Prestatorul va desemna specialiști tehnici cu competențe complete în arhitectura și funcționarea Serviciului MPay, care vor colabora activ cu Beneficiarul și cu participanții implicați pentru clarificarea și soluționarea situației.

Soluționarea reclamațiilor și divergențelor se va realiza conform unui termen rezonabil agreat de Părți la momentul sesizării, dar nu mai târziu de 10 zile lucrătoare de la data înregistrării formale a reclamației, cu posibilitate de prelungire motivată, cu acordul Beneficiarului. Toate reclamațiile și acțiunile întreprinse vor fi documentate în Sistemul de Service Desk.

2.11. Mentenanța bazelor de date

Administratorul de baze de date (DBA) din cadrul echipei Prestatorului are responsabilitatea de a asigura performanța, integritatea și disponibilitatea bazelor de date aferente Serviciului MPay. În acest sens, Prestatorul va executa în mod regulat, conform unui plan agreat cu Beneficiarul, următoarele activități de mentenanță a bazelor de date:

a) Gestionarea și optimizarea indexurilor: Prestatorul va monitoriza permanent starea indexurilor din bazele de date ale Serviciului MPay. Activitățile includ: analiza fragmentării indexurilor existente, reorganizarea (REORGANIZE) indexurilor cu fragmentare moderată (între 10% și 30%), reconstruirea (REBUILD) indexurilor cu fragmentare ridicată (peste 30%), crearea de indexuri noi la identificarea interogărilor cu performanță degradată, eliminarea indexurilor neutilizate sau redundante care consumă resurse nejustificat, și documentarea tuturor operațiunilor efectuate. Reindexarea completă a tabelelor critice va fi planificată în afara

orelor de vârf operaționale, cu notificarea prealabilă a Beneficiarului cu minimum 24 ore înainte.

b) Actualizarea statisticilor: Prestatorul va asigura actualizarea periodică a statisticilor bazelor de date (UPDATE STATISTICS) pentru toate tabelele și indexurile relevante, cu o frecvență stabilită în funcție de volumul de date și rata de modificare a acestora. Actualizarea statisticilor va fi executată automat prin job-uri planificate, iar Prestatorul va monitoriza și ajusta frecvența acestora în funcție de comportamentul Query Optimizer-ului și de degradările de performanță identificate. Raportul lunar de mentenanță va include situația actualizărilor de statistici efectuate.

c) Monitorizarea performanței execuției interogărilor: Prestatorul va implementa și opera un mecanism continuu de monitorizare a performanței execuției interogărilor SQL (query execution monitoring), utilizând instrumente de tip Query Store, Extended Events sau echivalente. Activitățile includ: identificarea interogărilor cu timp de execuție ridicat (long-running queries), analiza planurilor de execuție (execution plans) și identificarea regresiilor de plan, detectarea blocajelor (deadlocks) și a situațiilor de așteptare excesivă (wait statistics), optimizarea interogărilor critice pentru tranzacțiile financiare ale Serviciului MPay, și raportarea lunară a indicatorilor de performanță ai bazei de date.

d) Lucrări periodice de mentenanță a bazei de date: Prestatorul va executa periodic lucrări de mentenanță care includ: verificarea integrității fizice și logice a bazelor de date (DBCC CHECKDB sau echivalent), gestionarea și monitorizarea spațiului de stocare (creștere fișiere de date și log, alertare proactivă la praguri de utilizare), arhivarea și curățarea datelor istorice conform politicii de retenție agreate cu Beneficiarul, managementul fragmentării tabelelor (heap fragmentation), monitorizarea și optimizarea utilizării memoriei buffer pool, și revizuirea periodică a configurației instanței SQL Server pentru alinierea la cele mai bune practici de securitate și performanță. Toate lucrările de mentenanță vor fi documentate și raportate lunar Beneficiarului, cu indicarea duratei, impactului și rezultatelor obținute.

2.12. Transfer de cunoștințe și management al ieșirii din contract

Transferul de cunoștințe reprezintă o obligație contractuală esențială, menită să garanteze că Serviciul MPay poate fi operat, menținut și dezvoltat în continuare fără întrerupere, indiferent de schimbările intervenite în relația contractuală. Această obligație se activează în două situații: la finalul contractului și la înlocuirea oricărui membru cheie al echipei Prestatorului pe durata contractului.

Cu minimum 60 de zile calendaristice înainte de expirarea contractului — sau imediat după notificarea de reziliere anticipată — Prestatorul va iniția procesul formal de transfer, care va parcurge obligatoriu următoarele etape:

Etapa 1 — Audit și inventariere (zilele 1–10): Prestatorul va elabora și prezenta Beneficiarului un inventar complet al tuturor elementelor supuse transferului: module de cod și versiunile curente, documentație tehnică și funcțională, configurații de mediu, integrări

active, conturi de acces și credențiale, certificate digitale și chei criptografice, job-uri automate, proceduri operaționale și runbook-uri, baza de cunoștințe din Service Desk.

Etapa 2 — Livrarea documentației (zilele 1–30): Prestatorul va actualiza și preda Beneficiarului documentația completă a Serviciului MPay, care va include: arhitectura tehnică actualizată cu toate modificările implementate pe durata contractului, diagramele de flux pentru toate procesele operaționale cheie, manualele de administrare și operare a back-office-ului, ghidurile de instalare și configurare a tuturor componentelor, documentația API actualizată, procedurile de backup și restaurare, și planul de continuitate actualizat.

Etapa 3 — Predarea codului sursă și acceselor (zilele 1–15): Prestatorul va preda Beneficiarului codul sursă complet și actualizat, cu istoricul integral al modificărilor din sistemul de versionare. Predarea credențialelor de acces, certificatelor digitale și cheilor criptografice se va realiza printr-un proces securizat agreat cu Beneficiarul, cu schimbarea obligatorie a tuturor parolelor și secretelor după confirmare.

Etapa 4 — Sesiuni de instruire (zilele 15–45): Prestatorul va organiza sesiuni de instruire cu durata minimă de 10 zile lucrătoare pentru echipa tehnică a Beneficiarului sau a noului prestator, acoperind: arhitectura și componentele sistemului, procedurile operaționale zilnice, managementul incidentelor și procedurile de escaladare, administrarea bazelor de date, gestionarea integrărilor cu sistemele externe, și procedurile de backup și restaurare.

Etapa 5 — Perioada shadow (zilele 31–60): Prestatorul va lucra în paralel cu echipa timp de minimum 30 de zile calendaristice, asigurând transferul know-how-ului operațional prin participarea comună la rezolvarea incidentelor, executarea modificărilor și operațiunile de mentenanță. Pe durata perioadei shadow, responsabilitatea operațională se transferă treptat către echipa preluatoare, conform unui plan de tranziție agreat.

Nerespectarea obligațiilor de transfer de cunoștințe în termenele stabilite atrage penalități contractuale de 1% din valoarea lunară a contractului pentru fiecare zi de întârziere și poate conduce la reținerea garanției de bună execuție.

2.13. Cerințe de securitate cibernetică

Accesul Prestatorului și al personalului său la orice componentă a Serviciului MPay — cod sursă, baze de date, medii de testare și producție, sisteme de monitorizare — va respecta obligatoriu principiul privilegiului minim: fiecare persoană va avea acces exclusiv la resursele strict necesare îndeplinirii atribuțiilor sale.

Remedierea vulnerabilităților de securitate identificate, cu respectarea următoarelor termene maxime de la publicarea oficială în bazele de date CVE:

Severitate	**Termen maxim de remediere**
Critică (CVSS ≥ 9.0)	7 zile calendaristice
Înaltă (CVSS 7.0–8.9)	15 zile calendaristice

Medie și joasă	30 zile calendaristice

Prestatorul va implementa și opera un proces continuu de identificare și remediere a vulnerabilităților de securitate, care va include: scanarea lunară a dependențelor software (biblioteci, pachete NuGet, framework-uri) cu instrumente automatizate de tip SCA (Software Composition Analysis); monitorizarea notificărilor CVE (Common Vulnerabilities and Exposures) pentru toate componentele utilizate; aplicarea patch-urilor de securitate pentru vulnerabilități critice (CVSS ≥ 9.0) în maximum 7 zile calendaristice de la publicarea oficială; aplicarea patch-urilor pentru vulnerabilități înalte (CVSS 7.0–8.9) în maximum 15 zile calendaristice. Actualizarea dependențelor software (pachete NuGet, biblioteci terțe, middleware) și a imaginilor de container ca răspuns la notificări CVE sau la modificări de compatibilitate. Prestatorul va utiliza imagini minimizate (pentru .NET: Chiselled Ubuntu) și va furniza Beneficiarului, la fiecare release, un SBOM actualizat (Software Bill of Materials) în format CycloneDX sau SPDX, care să ateste compoziția completă a dependențelor livrate.

La fiecare release livrat în mediul de producție, Prestatorul va furniza Beneficiarului un **SBOM (Software Bill of Materials)** actualizat, în format standardizat CycloneDX sau SPDX, care va documenta complet: toate dependențele directe și tranzitive ale aplicației, versiunile exacte utilizate, licențele aferente și statusul de securitate față de bazele de date CVE cunoscute la data livrării. SBOM-ul va fi arhivat de Beneficiar și va constitui documentul de referință pentru auditurile de securitate și pentru verificarea conformității la transferul de contract.

Actualizarea platformei .NET la versiunea Long-Term Support (LTS) curentă, planificată și executată coordonat cu Beneficiarul, ca răspuns la încheierea ciclului de suport al versiunii în uz. Această activitate constituie obligație de mentenanță preventivă și se execută fără costuri suplimentare față de contractul de bază.

Prestatorul va efectua semestrial sau la orice modificare majoră de arhitectură test de penetrare (penetration testing) al componentelor Serviciului MPay din zona sa de responsabilitate, realizat de un specialist intern certificat (OSCP, CEH sau echivalent) sau de o terță parte independentă. Raportul complet al testului va fi prezentat Beneficiarului în termen de 5 zile de la finalizarea testului. Toate vulnerabilitățile vor fi remediate conform tabelului de mai sus în maximum 30 de zile de la identificare, cu confirmare tehnică prezentată Beneficiarului.

Suplimentar, la orice modificare majoră de arhitectură sau la conectarea unui nou tip de participant, Prestatorul va efectua o evaluare de securitate (security review) înainte de implementarea în producție.

Toate datele financiare și cu caracter personal vor fi criptate în tranzit (TLS 1.2 minimum, recomandat TLS 1.3) și în repaus. Prestatorul va menține o politică documentată de clasificare a datelor și va asigura că angajații săi accesează exclusiv categoriile de date necesare rolului lor. Orice export sau copiere de date din mediul de producție în scop de diagnostic sau testare va fi autorizat în scris de Beneficiar și va utiliza exclusiv date anonimizate.

La identificarea oricărui incident de securitate cibernetică, Prestatorul va notifica Beneficiarul în maximum 4 ore, conform obligației din secțiunea 1.1.7. În termen de 72 de ore, va prezenta un raport complet cu: natura și amploarea incidentului, datele și sistemele afectate, cronologia evenimentelor, măsurile imediate aplicate și planul de remediere pe termen scurt și lung. Prestatorul va coopera integral cu autoritățile competente (CERT-MD, CNPDCP) în cazul incidentelor cu impact asupra datelor personale sau infrastructurii critice.

Prestatorul se va conforma cerințelor de securitate prevăzute de HG nr. 1123/2010, Legea nr. 195/2024 privind protecția datelor cu caracter personal (de la data intrării în vigoare — 23 august 2026), reglementărilor BNM aplicabile sistemelor de plată, și oricăror cerințe de securitate emise de STISC în calitate de Administrator Tehnic al Serviciului MPay.

2.14. Raportare lunară și guvernanță

Prestatorul va prezenta Beneficiarului un Raport lunar de activitate până cel târziu în a 5-a zi lucrătoare a lunii următoare perioadei de raportare. Raportul va fi structurat obligatoriu pe următoarele secțiuni:

1. Disponibilitate și SLA — indicatorul AQS lunar calculat conform metodologiei din secțiunea 2.2, cu detalii despre toate perioadele de indisponibilitate înregistrate (dată, durată, cauză, rezoluție), ferestrele de mentenanță executate și calculul penalităților aplicabile dacă este cazul.

2. Managementul incidentelor — numărul total de incidente înregistrate, distribuit pe priorități (Critică / Înaltă / Medie / Joasă); timp mediu de reacție (TR efectiv) și timp mediu de soluționare (TS efectiv) per prioritate, comparate cu valorile SLA contractuale; numărul de incidente soluționate în SLA vs. depășiri; incidentele repetitive identificate și măsurile de prevenție propuse.

3. Managementul solicitărilor — numărul total de solicitări procesate, distribuit pe priorități; TR și TS medii per prioritate comparate cu SLA; solicitări în așteptare la sfârșitul perioadei de raportare cu justificare.

4. Mentenanță și modificări — lista modificărilor implementate în perioada de raportare cu referința în Registrul Modificărilor; statusul lucrărilor de mentenanță a bazelor de date (indexuri, statistici, DBCC); statusul actualizărilor de securitate și patch-urilor aplicate; modificările planificate pentru luna următoare.

5. Securitate — statusul patch management (vulnerabilități identificate, remediate, în lucru); incidente de securitate înregistrate dacă există; statusul certificatelor digitale (cu alertă pentru cele care expiră în următoarele 60 de zile).

6. Performanța bazelor de date — indicatori cheie de performanță BD: timp mediu de răspuns al interogărilor critice, număr de deadlocks, utilizarea spațiului de stocare și tendința de creștere, statusul job-urilor automate de mentenanță.

7. Riscuri și propuneri — riscurile tehnice și operaționale identificate în perioada de raportare, cu nivelul de severitate și măsurile de atenuare propuse; propuneri de îmbunătățire sau modernizare a componentelor Serviciului MPay.

Raportul va fi transmis în format electronic (PDF și Excel pentru datele cantitative) și va fi însoțit de un rezumat executiv de maximum o pagină, destinat managementului Beneficiarului.

Pentru orice incident de prioritate Critică sau Înaltă, Prestatorul va elabora un Raport post-incident în termen de 24 de ore de la închiderea incidentului, conținând: cronologia detaliată, cauza rădăcină (root cause analysis), impactul asupra tranzacțiilor și participanților, acțiunile de remediere aplicate și măsurile preventive pentru evitarea recurenței.

Prestatorul va participa lunar la o ședință de review operațional cu reprezentanții Beneficiarului și, după caz, STISC. Ședința va avea loc în primele 10 zile lucrătoare ale lunii, după prezentarea raportului lunar. Agenda standard va include: analiza raportului lunar, discutarea incidentelor semnificative și a măsurilor preventive, planificarea modificărilor pentru luna următoare, escaladarea problemelor nerezolvate și decizii privind prioritizarea activităților. Prestatorul va distribui minuta ședinței în termen de 2 zile lucrătoare de la desfășurare.

Prestatorul va prezenta trimestrial un Raport de capacitate, care va include: tendințele de creștere a volumelor de tranzacții și impactul estimat asupra performanței sistemului, prognoza de utilizare a resurselor de stocare și procesare pentru următoarele 6 luni, și recomandările privind necesarul de resurse suplimentare — pentru a permite Beneficiarului să planifice bugetar și tehnic din timp.

Prestatorul va prezenta anual un Raport de securitate, care va consolida: rezultatele testelor de penetrare, statusul conformității cu cerințele de securitate din secțiunea 2.13, evoluția indicatorilor de securitate pe parcursul anului și planul de îmbunătățire a posturii de securitate pentru anul următor.