NOTĂ DE FUNDAMENTARE

Secțiunea 1 Titlul proiectului **Hotărâre a Guvernului pentru reaprobarea Notei de fundamentare privind necesitatea și oportunitatea efectuării cheltuielilor aferente proiectului de investiții „*Sistem de alertă timpurie – SAT (Early warning system)*”**	
Secțiunea a 2-a Motivul emiterii actului	
2.1. Sursa proiectului	Prezentul proiect a fost elaborat la inițiativa Ministerului Afacerilor Interne prin Direcția Generală de Protecție Internă, în baza prevederilor Ordonanței de urgență de Guvernului nr. 30/2007 *privind organizarea și funcționarea Ministerului Afacerilor Interne*, aprobată cu modificări prin Legea nr. 15/2008, cu modificările și completările ulterioare, în scopul aprobării Notei de fundamentare privind necesitatea și oportunitatea efectuării cheltuielilor aferente proiectului „*Sistem de alertă timpurie – SAT (Early warning system)*”.
2.2. Descrierea situației actuale	În contextul derulării proiectului pentru operaționalizarea emiterii cărții electronice de identitate la nivelul Direcției Generale pentru Evidența Persoanelor, la nivelul Ministerului Afacerilor Interne s-a semnat Contractul de finanțare nr. 18441 din 29.08.2024 pentru proiectul de investiții „*Sistem de alertă timpurie – SAT (Early warning system)*“, în cadrul Planului Național de Redresare și Reziliență, Componenta 7 - Transformare digitală, investiția 8 - Cartea de identitate electronică și semnătura digitală calificată, Jalon 174 - Punerea în aplicare a măsurilor de sprijin pentru implementarea cărții de identitate electronice, Ministerul Afacerilor Interne prin Direcția Generală de Protecție Internă având calitatea de beneficiar. În considerarea prevederilor art. 42 alin. (1) lit. a) din Legea nr. 500/2002 *privind finanțele publice*, cu modificările și completările ulterioare, DGPI a transmis, spre aprobarea Guvernului, *Nota de fundamentare privind necesitatea și oportunitatea efectuării cheltuielilor aferente proiectului de investiții „Sistem de alertă timpurie – SAT (Early warning system)”,* aceasta fiind aprobată prin Hotărârea Guvernului nr. 361/2025, publicată în Monitorul Oficial al României, Partea I, nr. 328 din 11 aprilie 2025. Subsecvent, contractul de finanțare nr. 18441 din 29.08.2024 pentru proiectul de investiții *„Sistem de alertă timpurie – SAT (Early warning system)”* a fost modificat printr-o serie de notificări și acte adiționale, Notificarea nr. 1/19.12.2024, Notificarea nr. 2/30.05.2025, Actul adițional nr. 1/02.10.2025, Actul adițional nr. 2/23.06.2026, Notificarea nr. 3/29.07.2026, Actul adițional nr. 3/18.08.2026 și Actul adițional nr. 4/24.08.2026. Modificările relevante au avut în vedere următoarele: - actul adițional nr. 1/02.10.2025: actualizarea bugetului total al proiectului de investiții, în conformitate cu Legea nr. 141/2025 privind unele măsuri fiscal-bugetare, prin aplicarea la valoarea aprobată a proiectului de investiții a diferenței aferente modificării cotei de TVA, în cuantum de 1.788.576 lei; - actul adițional nr. 2/23.06.2026: modificarea perioadei de implementare a proiectului de investiții, de la data de 30.06.2026 la data de 25 august 2026. - actul adițional nr. 3/29.07.2026: modificarea perioadei de implementare a proiectului de investiții, până la data de 31.08.2026, inclusiv. - actul adițional nr. 4/24.08.2026: majorarea suplimentarea bugetului proiectului

	de investiții cu suma de 30.000.000,00 lei fără TVA (36.300.000,00 lei, cu TVA), pentru efectuarea de achiziții circumscrise componentei nr. 1. Astfel, valoarea totală actualizată a proiectului de investiții este de 144.509.562 lei iar valoarea totală rămasă de executat până la finalul perioadei de implementare, respectiv data de 31.08.2026, este de 58.616.959,71 lei. În forma aprobată, proiectul a urmărit realizarea unui singur Sistem de Alertă Timpurie, alcătuit din componente complementare care asigură automatizarea proceselor de colectare, validare și evaluare integrată a datelor și informațiilor multisursă, extinderea capacităților tehnice de detecție, monitorizare și analiză a evenimentelor de securitate, interoperabile cu Centrul Operațional de Securitate Cibernetică al MAI – CERT-INT, precum și funcțiile de back-up și disaster recovery. Rezultatul este circumscris indicatorului calitativ al Jalonului 174, respectiv „sistemul de alertă timpurie dezvoltat”, iar activitățile eligibile includ infrastructura hardware și software necesară evaluării integrate și predictive a datelor multisursă pentru anticiparea, prevenirea și contracararea amenințărilor și riscurilor tehnice și non-tehnice asociate ecosistemului CEI. Implementarea realizată până în prezent s-a desfășurat în conformitate cu graficul activităților și rezultatelor aprobate, iar indicatorii asumați vor fi atinși în termenul de implementare. Dezvoltarea propusă prin prezenta justificare nu are rolul de a remedia deficiențe ale rezultatelor deja obținute, nu înlocuiește componentele realizate și nu introduce un rezultat distinct, ci urmărește consolidarea dimensiunii calitative a aceluiași rezultat – R 1.1 Rezultat Componenta 1 – o soluție de automatizare, prin creșterea capacității de procesare, a vitezei și preciziei analizei, a scalabilității, rezilienței și continuității operaționale. Cu toate acestea, progresul tehnologic al inteligenței artificiale a dobândit recent un ritm extraordinar de accelerat, determinând o transformare structurală majoră a spațiului digital, caracterizată de o complexitate fără precedent a atacurilor cibernetice, precum și de creșterea exponențială a volumului de date generate și distribuite la nivel global, peste 65% din conținutul nou generat în spațiul cibernetic fiind produs automat de tehnologiile de inteligență artificială. Acest trend conduce la creșterea semnificativă a cantității de informații ce trebuie procesate și analizate rapid, fapt ce impune adaptarea continuă a infrastructurii informatice aferente instrumentelor analitice de volume mari de date, indispensabilă pentru asigurarea unui nivel ridicat de operativitate privind identificarea în timp util a amenințărilor de securitate emergente din mediul online. În acest context, a fost relevată nevoia stringentă de îmbunătățire calitativă a instrumentelor digitale propuse și realizate în cadrul proiectului Sistem de Alertă Timpurie pentru a fi capabile să mențină un nivel optim de prevenire și contracarare a amenințărilor hibride din spectrul cibernetic/informațional de natură a afecta ecosistemul digital al Cărții Electronice de Identitate (infrastructura de emitere, post emitere și accesare a serviciile electronice ale MAI). În etapa de implementare a proiectului SAT s-a constatat necesitatea recalibrării capabilităților dezvoltate prin Componenta 1, prin realizarea unei upgrade al infrastructuri destinate procesării directe și analizei imediate a volumelor mari de date și informații neclasificate provenite din spațiul cibernetic/informațional, complementar infrastructurii similare deja prevăzute în proiect pentru

	automatizarea proceselor de prelucrare, verificare și analiza multisursă a datelor și informațiilor clasificate. În forma aprobată a cererii de finanțare a proiectului SAT, reperele din componența acestui tip de infrastructură: - echipamente hardware și produse software asociate; - produse software cu tehnologie AI și hardware asociat, au fost dimensionate exclusiv pentru operaționalizarea capabilității sistemului de procesare și integrare a informațiilor clasificate, aceasta reprezentând infrastructura principală a Componentei 1 dedicată activităților complexe de evaluare a amenințărilor de securitate. Provocările de securitate menționate sunt determinate de intensificarea interferențelor informaționale și atacurilor cibernetice disruptive, acțiuni executate cu ajutorul unor instrumente malițioase bazate pe tehnologiile de inteligență artificială pentru exploatarea rapidă a vulnerabilităților infrastructurilor informatice. Corelativ, serviciile publice electronice ale MAI, reprezintă la rândul lor o țintă predilectă a interferențelor informaționale și atacurilor cibernetice, unul dintre scopurile urmărite fiind acela de alimentare constantă a neîncrederii și reticenței cetățenilor de a participa la tranziția către o societate modernă, digitalizată și debirocratizată. În acest sens, reliefăm precizările publice ale MAI din 28 octombrie 2025 și 26 martie 2026 referitoare la identificarea în spațiul public a unor informații false privind presupuse vulnerabilități ale sistemului CEI în scopul alimentării narațiunilor capabile să afecteze încrederea publică. Inteligența artificială a ajuns să reprezinte un instrument facil, la care atacatorii apelează frecvent în vederea automatizării activităților de creare imediată a unor rețele extinse de conturi neautentice (botnet), respectiv de fabricare și diseminare de conținut digital alterat cu scopul discreditării instituțiilor publice și serviciilor electronice oferite de acestea cetățenilor sau pentru realizarea unor acțiuni de inginerie socială în vederea obținerii facile a credențialelor de acces și compromiterii platformelor informatice ale administrației centrale și locale. Emergența și accelerarea exponențială a inteligenței artificiale (IA) au marcat trecerea de la amenințările digitale tradiționale la o nouă eră a războiului hibrid-cognitiv și cibernetic, fapt ce a determinat o reconfigurare radicală a securității globale. Dacă până recent securitatea cibernetică se baza pe protecția perimetrelor informatice împotriva unor coduri create manual, astăzi ne confruntăm cu amenințări dinamice, autonome și autoadaptative. Această transformare nu doar că a crescut complexitatea vectorilor de atac existenți, dar a generat categorii complet noi de vulnerabilități pe palierele informațional, tehnic și al serviciilor publice. Diferența fundamentală față de trecut constă în scara, viteza și precizia cu care un atac poate fi executat. Dacă un atac clasic necesita resurse umane substanțiale, analiză îndelungată și timp de execuție, IA permite automatizarea fiecărei etape a ciclului de atac (“Cyber Kill Chain”), reducând fereastra de reacție a defensivelor de la zile sau ore la microsecunde. Pe palierul informațional, explozia GenAI a determinat apariția unor amenințări noi și amplificarea celor existente cristalizând conceptul de război cognitiv de precizie. Operațiunile de influență tradiționale, bazate pe ferme de troli și mesaje rigide, aveau o eficiență limitată de factorul uman și de barierele lingvistice sau culturale. Astăzi, IA generativă și modelele lingvistice mari

	(LLM) permit crearea de conținut sintetic de o acuratețe absolută, eliminând erorile stilistice și adaptând discursul în funcție de amprenta psihologică a publicului-țintă. O amenințare complet nouă este reprezentată de falsificarea hiper-realistă a realității (Deepfake Audio/Video) utilizată ca armă tactică. Dacă în trecut manipularea imaginilor necesita tehnicieni video calificați și timp îndelungat, acum agenții autonomi pot genera în timp real clone vocale sau video ale liderilor și comandanților militari sau ale oficialilor publici. Acest lucru permite orchestrarea unor operațiuni de tip „false flag", capabile să genereze într-un timp foarte scurt revolte sociale sau erori de comandă strategică, respectiv o stare de teamă și neîncredere a cetățenilor în serviciile publice ale statului, înainte ca informația să poată fi verificată. Pe lângă apariția acestor noi vectori, complexitatea interferențelor existente a crescut exponențial prin automatizarea micro-targetării. Algoritmii de IA pot analiza simultan miliarde de date din amprentele digitale ale cetățenilor, identificând vulnerabilitățile emoționale ale fiecărui grup social. Mesajele manipulative nu mai sunt transmise la grămadă; ele sunt generate dinamic și livrate individualizat prin boți autonomi capabili să poarte conversații umane persuasive pe termen lung, fără a fi detectați de filtrele anti-spam sau anti-bot. Se trece de la poluarea informațională la eroziunea sistemică a încrederii. Atunci când cetățenii nu mai pot distinge o înregistrare autentică de una sintetică, însăși noțiunea de probă, adevăr public și proces democratic transparent devine vulnerabilă în fața intervențiilor externe. Pe palierul tehnic, IA a transformat fundamental peisajul atacurilor cibernetice, generând amenințări de o sofisticare nemaiîntâlnită. Principala provocare nouă este apariția malware-ului autonom și polimorf alimentat de IA. Spre deosebire de virușii tradiționali, care foloseau semnături de cod fixe ce puteau fi identificate de soluțiile antivirus, malware-ul avansat bazat pe IA își rescrie singur codul sursă în timp ce se propagă, învățând din comportamentul sistemelor defensive pe care le întâlnește. O altă provocare complet nouă o constituie atacurile orientate direct împotriva arhitecturilor de IA, cunoscute sub numele de "Data Poisoning" și „Prompt Injection/Adversarial Attacks". Prin alterarea subtilă a datelor pe care este antrenat un model sau prin introducerea unor instrucțiuni manipulative ascunse, atacatorii pot corupe capacitatea de decizie a unui sistem IA fără a lăsa urme în codul sursă tradițional, determinând sistemul să ia decizii catastrofale dar aparent legitime. În paralel, complexitatea atacurilor cibernetice existente a fost amplificată considerabil, tentativele de manipulare au trecut la campanii de "spear-phishing" hiper-personalizate. IA analizează stilul de scriere și generează mesaje identice ca stil, ton și context, crescând rata de penetrare a infrastructurilor critice. Integrarea IA în serviciile electronice publice pentru procesarea automată a cererilor, alocarea resurselor medicale sau gestionarea traficului urban introduce riscul "sabotajului algoritmic". Un atac cibernetic ce reușește să otrăvească datele de intrare poate forța un sistem public să ia decizii discriminatorii sau eronate la scară națională, blocând activitatea administrativă și generând daune financiare colosale. Instituțiile publice se confruntă cu o asimetrie gravă: în timp ce infractorii

	cibernetici adoptă rapid orice inovație IA pentru a ataca, administrațiile publice sunt încetinite de proceduri birocratice, bugete rigide și deficit de personal calificat. În lipsa unor sisteme de apărare bazate tot pe inteligență artificială, capabile să reacționeze autonom în timp real, infrastructura critică a serviciilor publice digitale rămâne expusă unor atacuri masive de tip Denial of Service (DoS) augmentat de IA sau ransomware polimorf. Progresul accelerat al IA a transformat interferențele informaționale într-o armă de dezbinare cognitivă în masă, iar atacurile cibernetice într-un război derulat la viteza procesoarelor. Pentru ca serviciile publice electronice să supraviețuiască acestui mediu ostil, este imperativă trecerea la arhitecturi de securitate bazate pe sisteme defensive de IA capabile să neutralizeze amenințările în timp real. Ca atare, reducerea vulnerabilităților de tip nou și contracararea amenințărilor emergente de securitate pot fi realizate doar prin implementarea unor soluții tehnologice de vârf și dezvoltarea capabilităților instituționale de răspuns, în special în domeniul inteligenței artificiale, pentru analiza în timp real a unor volume mari de date și facilitarea identificării unor pattern-uri utilizate în operațiunile informaționale sau atacurile cibernetice în scopul anticipării tehnicilor tacticilor și procedurilor ce vor fi utilizate de viitoarele campanii agresive. Aceste capabilități au potențialul de a crește nivelul de securitate și de a asigura continuitatea serviciilor esențiale, prin îmbunătățirea capacităților de detecție și răspuns a structurilor abilitate. Arhitectura actuală a sistemului de alertă timpurie include servicii în cloud de detecției și alertare timpurie a amenințărilor de securitate (asigurând funcționalități de colectare și procesare preliminară a datelor provenite din mediul online), în timp ce dezvoltarea calitativă a soluției are caracter de complementaritate și va permite recalibrarea printr-o capacitate on premise de analiză de volume mari de date în scopul accelerării componentei de evaluare a impactului și probabilității de materializare a amenințărilor de securitate detectate, respectiv de fundamentare a măsurilor de contracarare. Soluția hardware propusă are ca obiectiv implementarea unei infrastructuri IT scalabile, performante și securizate, destinată procesării intensive de date, aplicațiilor AI/ML, virtualizării, stocării de mare capacitate și conectivității de înaltă viteză. Aceasta integrează componente de ultimă generație, optimizate pentru performanță, redundanță și eficiență operațională. Beneficii și avantaje ale soluției descrise mai sus: - Performanță extremă pentru aplicații AI, HPC și virtualizare; - Scalabilitate modulară pentru procesare și stocare; - Redundanță și fiabilitate ridicată; - Securitate avansată și conformitate cu standarde internaționale; - Integrare facilă în infrastructuri existente; - Suport extins pentru 5 ani. Implementarea proiectului de investiții valorifică acordurile-cadru aflate în derulare la nivelul DGPI, prin încheierea contractelor subsecvente, numai după aprobarea modificării și parcurgerea verificărilor legale aplicabile. Livrarea, instalarea, configurarea, integrarea, testarea și recepția componentelor vor fi corelate cu arhitectura SAT și cu termenul maxim de finalizare de 31.08.2026. Bunurile, licențele și serviciile finanțate vor fi delimitate tehnic, contractual, patrimonial și contabil față de componentele deja realizate și față de orice activități complementare finanțate prin alte proiecte, pentru asigurarea trasabilității cheltuielilor și evitarea dublei finanțări. Ca atare, bugetul estimat de 30.000.000 de lei fără TVA (36.300.000,00 lei cu

	TVA) este destinat unui pachet integrat de achiziții format din echipamente hardware și produse software asociate, precum și din produse software cu tehnologie AI și hardware-ul necesar funcționării acestora. În concret, sunt avute în vedere resurse de calcul și stocare pentru volume mari de date, platforme și licențe de virtualizare și containerizare, baze de date analitice, componente software specializate pentru analiză semantică și corelare, infrastructură de comunicații securizate, licențe și servicii de instalare, configurare, integrare, testare și punere în funcțiune. Valoarea solicitată este astfel legată de categorii determinate de produse și servicii și nu reprezintă o rezervă bugetară generală. Majorarea alocării bugetare nu determină introducerea unor categorii noi de cheltuieli în proiect. Dezvoltarea propusă se încadrează integral în categoriile de cheltuieli existente și aprobate la nivelul proiectului, aferente achiziției de infrastructură hardware și software necesare evaluării integrate și predictive a datelor și informațiilor multisursă, precum și anticipării, prevenirii și contracarării amenințărilor și riscurilor tehnice și non-tehnice asociate ecosistemului CEI. Din această perspectivă, modificarea solicitată reprezintă o dezvoltare calitativă și o redimensionare funcțională a soluției aprobate, fără extinderea tipologiei cheltuielilor eligibile și fără introducerea unei activități, a unui rezultat sau a unui indicator cantitativ nou. Prelucrarea și evaluarea seturilor masive de date vizate de soluția propusă reprezintă fundamentul procesului analitic, fiind necesară asigurarea unei infrastructuri capabile să susțină atât procesarea de tip bază de date la scară foarte mare, cât și execuția algoritmilor de inteligență artificială în regim accelerat. Mecanismele de învățare adaptivă vor contribui la creșterea preciziei analizelor și la reducerea alertelor irelevante, permițând prioritizarea riscurilor cu impact asupra implementării serviciilor publice electronice. Această dezvoltare calitativă creează premisele asigurării sustenabilității pe termen lung a Sistemului de Alertă Timpurie, prin consolidarea unei capacități instituționale proprii, scalabile și adaptabile, capabile să susțină procesarea accelerată a volumelor mari de date, integrarea continuă a algoritmilor de inteligență artificială și perfecționarea mecanismelor de detecție, analiză și răspuns în raport cu evoluția amenințărilor cibernetice și informaționale, contribuind astfel la menținerea unui nivel ridicat de securitate, reziliență și continuitate a serviciilor publice electronice. În conformitate cu prevederile art. 10 lit. b) din OUG nr. 76/2016, Direcția Generală de Protecție Internă asigură coordonarea și controlul activităților pentru protecția informațiilor clasificate naționale, ale Organizației Tratatului Atlanticului de Nord și ale Uniunii Europene, precum și pentru securitatea cibernetică, la nivelul structurilor Ministerului Afacerilor Interne. Obiectivul investiției propuse de către DGPI vizează asigurarea unui nivel ridicat de încredere și siguranță pentru creșterea atractivității utilizării CEI și accesării serviciilor electronice publice. Sistemul reprezintă soluția de securitate optimă pentru asigurarea exploatării sistemelor utilizate în emiterea și punerea in circulație a CEI, precum și pentru utilizarea în mod neîntrerupt și în condiții de siguranță a serviciilor publice electronice furnizate de MAI. În acest fel, se vor crea premisele realizării în mod automat a colectării, procesării, validării și evaluării integrate a datelor și informațiilor multisursă pentru a anticipa, detecta, preveni și contracara amenințările și riscurile de securitate asociate cu emiterea și utilizarea CEI.

	Proiectul de investiții contribuie la consolidarea nivelului de securitate cibernetică și extinderea soluțiilor de securitate, inclusiv prin crearea și extinderea unor centre de securitate operaționale dedicate infrastructurii IT&C existentă la nivelul MAI pentru emiterea, managementul post-emitere al CEI și furnizarea celor 11 servicii publice electronice, facilitând interacțiunea digitală dintre entitățile publice/private și cetățeni, prin intermediul unei infrastructuri informatice sigure și reziliente. Integrarea tehnologiei de inteligență artificială (AI) va asigura o dinamică progresivă a sistemului de alertă timpurie a amenințărilor de securitate, care se îmbunătățește constant, crescând considerabil sustenabilitatea, adaptabilitatea și reziliența acestuia. În mod evident, capacitatea inteligenței artificiale de a analiza rapid volume mari de date reprezintă un avantaj tehnologic incomparabil față de metodele existente de automatizare a analizei și va conferi sistemului un caracter mult mai precis și eficient în timp. Prin realizarea acestui sistem, beneficiarul abordează provocările de securitate asociate celor 11 servicii publice electronice furnizate populației de către MAI, infrastructurii IT&C utilizată pentru emiterea și managementul post-emitere a CEI, precum și proceselor de autentificare/accesare a acestora de către utilizatorii persoane fizice sau juridice.
2.3. Schimbări preconizate	Prin demersul propus se solicită Guvernului ***reaprobarea Notei de fundamentare privind necesitatea și oportunitatea efectuării cheltuielilor aferente proiectului de investiții „Sistem de alertă timpurie – SAT (Early warning system)",*** în conformitate cu dispozițiile art. 42 alin. (2) din Legea nr. 500/2002 *privind finanțele publice*, cu modificările și completările ulterioare, în ceea ce privește: ➢ **actualizarea bugetului total al proiectului de investiții, în conformitate cu Legea nr. 141/2025 *privind unele măsuri fiscal-bugetare,* cu modificările și completările ulterioare, prin aplicarea la valoarea aprobată a proiectului de investiții a diferenței aferente modificării cotei de TVA, în cuantum de 1.788.576 lei și totodată majorarea valorii aferente proiectului de investiții, cu suma de 36.300.000,00 lei cu TVA** pentru Componenta 1 - *Automatizarea proceselor de colectare, validare și evaluare integrată a datelor și informațiilor multisursă necesare detecției și anticipării amenințărilor de securitate generate de tehnologiile emergente pe baza evaluărilor predictive complexe asociate emiterii și utilizării CEI pentru accesarea serviciilor publice electronice de către populație*, **rezultând o valoare totală actualizată de 144.509.562 lei;** ➢ **majorarea perioadei de implementare a proiectului de investiții**, prevăzută în Anexa la H.G. nr. 361/2025 (22 luni, dar nu mai târziu de 30 iunie 2026), **până la data de 31.08.2026, inclusiv;** ➢ **finanțarea proiectului de investiții din fonduri externe nerambursabile,** în cadrul *Planului național de redresare și reziliență, Componenta 7 - Transformare digitală, Investiția 8 - Cartea de identitate electronică și semnătura digitală, Jalon 174 - Punerea în aplicare a măsurilor de sprijin pentru implementarea cărții de identitate electronice*, și **de la bugetul de stat, prin bugetul Ministerului Afacerilor Interne, în limita sumelor aprobate anual cu această destinație, conform programelor de investiții publice aprobate potrivit legii.**
2.4. Alte informații	Având în vedere că valoarea totală a investiției prevăzute în Anexa la proiectul de hotărâre a Guvernului este de 144.510 mii lei, inclusiv TVA, este necesară ***reaprobarea Notei de fundamentare privind necesitatea și oportunitatea***

	efectuării cheltuielilor aferente proiectului de investiții „Sistem de alertă timpurie – SAT (Early warning system)”, în conformitate cu dispozițiile art. 42 alin. (2) din Legea nr. 500/2002 *privind finanțele publice*, cu modificările și completările ulterioare. În cadrul Planului Național de Redresare și Reziliență, Componenta 7 – Transformare digitală, Investiția 8 – Cartea de identitate electronică și semnătura digitală, Jalonul 174 – Punerea în aplicare a măsurilor de sprijin pentru implementarea cărții de identitate electronice, sunt finanțate proiectele „D4eID – Digitalizare pentru promovarea cărții de identitate electronice”, implementat de Direcția Generală pentru Comunicații și Tehnologia Informației și Direcția Informare și Relații Publice, în baza Deciziei de finanțare nr. 18440/29.08.2024, și „Sistem de alertă timpurie – SAT (Early warning system)”, finanțat în baza Contractului de finanțare nr. 18441/29.08.2024, cele două proiecte având caracter complementar. Resursele financiare necesare majorării bugetului proiectului „Sistem de alertă timpurie – SAT (Early warning system)” sunt asigurate prin diminuarea corespunzătoare a alocării aferente proiectului „D4eID – Digitalizare pentru promovarea cărții de identitate electronice”.
Secțiunea a 3-a Impactul socioeconomic	
3.1. Descrierea generală a beneficiilor şi costurilor estimate ca urmare a intrării în vigoare a actului normativ	
3.2. Impactul social	Proiectul propus contribuie la măsurile de sprijin finanțate pentru implementarea CEI prin crearea unei infrastructuri cu nivel ridicat de încredere și siguranță, necesară atât emiterii, punerii în circulație și asigurării funcționalității și disponibilității CEI, cât și a serviciilor accesate prin intermediul acesteia. Astfel, va fi implementat un sistem care să adreseze riscurile de securitate (tehnice și non tehnice), creând premisele facilitării interacțiunii digitale dintre entitățile publice/private și cetățeni. Acesta vine în completarea celorlalte două măsuri de sprijin (11 servicii publice online, cu un nivel de sofisticare de cel puțin „3”, respectiv o campanie de sensibilizare care să încurajeze utilizarea pe scară largă a cărții de identitate electronice și, implicit, a serviciilor publice electronice aferente acesteia) contribuind, astfel, la creșterea atractivității și utilizării CEI pe scară largă, în rândul populației.
3.3. Impactul asupra drepturilor şi libertăţilor fundamentale ale omului	
3.4. Impactul macroeconomic	
3.4.1. Impactul asupra economiei şi asupra principalilor indicatori macroeconomici	

3.4.2. Impactul asupra mediului concurenţial şi domeniul ajutoarelor de stat	
3.5. Impactul asupra mediului de afaceri	
3.6. Impactul asupra mediului înconjurător	
3.7. Evaluarea costurilor şi beneficiilor din perspectiva inovării şi digitalizării	
3.8. Evaluarea costurilor şi beneficiilor din perspectiva dezvoltării durabile	
3.9. Alte informaţii	

Secțiunea a 4-a
Impactul financiar asupra bugetului general consolidat, atât pe termen scurt, pentru anul curent, cât și pe termen lung (5 ani), inclusiv informaţii cu privire la cheltuieli şi venituri

mii lei

Indicatori	**Anul curent**	**Următorii 4 ani**				**Media pe 5 ani**
1	**2**	**3**	**4**	**5**	**6**	**7**
4.1. Modificări ale veniturilor bugetare, plus/minus, din care:						
a) bugetul de stat, din acesta:						
(i) impozit pe profit						
(ii) impozit pe venit						
b) bugete locale:						
(i) impozit pe profit						
c) bugetul asigurărilor sociale de stat:						
(i) contribuții de asigurări						
d) alte tipuri de venituri						
4.2. Modificări ale cheltuielilor bugetare, plus/minus, din care:						

a) buget de stat, din acesta:						
(i) cheltuieli de personal						
(ii) bunuri și servicii						
b) bugete locale:						
(i) cheltuieli de personal						
(ii) bunuri și servicii						
c) bugetul asigurărilor sociale de stat:						
(i) cheltuieli de personal						
(ii) bunuri și servicii						
d) alte tipuri de cheltuieli						
4.3. Impact financiar, plus/minus, din care:						
a) buget de stat						
b) bugete locale						
4.4. Propuneri pentru acoperirea creșterii cheltuielilor bugetare						
4.5. Propuneri pentru a compensa reducerea veniturilor bugetare						
4.6. Calcule detaliate privind fundamentarea modificărilor veniturilor și/sau cheltuielilor bugetare						
4.7.Prezentarea, în cazul proiectelor de acte normative a căror adoptare atrage majorarea cheltuielilor bugetare, a următoarelor documente: **a) fişa financiară prevăzută la art. 15 din Legea nr. 500/2002 privind finanţele publice, cu modificările şi completările ulterioare, însoţită de ipotezele şi metodologia de calcul utilizată;** **b) declaraţie conform căreia majorarea de cheltuială respectivă este compatibilă cu obiectivele şi priorităţile strategice**						

specificate în strategia fiscal-bugetară, cu legea bugetară anuală şi cu plafoanele de cheltuieli prezentate în strategia fiscal-bugetară.	
4.8. Alte informaţii	Finanțarea proiectului de investiții se realizează din fonduri externe nerambursabile, în cadrul Planului național de redresare și reziliență, Componenta 7 - Transformare digitală, Investiția 8 - Cartea de identitate electronică și semnătura digitală, Jalon 174 - Punerea în aplicare a măsurilor de sprijin pentru implementarea cărții de identitate electronice, și de la bugetul de stat, prin bugetul Ministerului Afacerilor Interne, în limita sumelor aprobate anual cu această destinație, conform programelor de investiții publice aprobate potrivit legii.
Secţiunea a 5-a Efectele proiectului asupra legislaţiei în vigoare	
5.1. Măsuri normative necesare pentru aplicarea prevederilor proiectului de act normativ: a) acte normative în vigoare ce vor fi modificate sau abrogate, ca urmare a intrării în vigoare a proiectului de act normativ; b) acte normative ce urmează a fi elaborate în vederea implementării noilor dispoziţii.	
5.2. Impactul asupra legislaţiei în domeniul achiziţiilor publice	
5.3. Conformitatea proiectului de act normativ cu legislația UE	
5.3.1. Măsuri normative necesare transpunerii directivelor UE	
5.3.2. Măsuri normative necesare aplicării actelor legislative UE	
5.4. Hotărâri ale Curții de Justiție a Uniunii Europene	
5.5 Alte acte normative şi/sau documente internaţionale din care decurg angajamente asumate	
5.6. Alte informaţii	
Secţiunea a 6-a Consultările efectuate în vederea elaborării proiectului	
6.1. Informaţii privind neaplicarea procedurii de participare la elaborarea actelor normative	
6.2. Informații privind procesul de consultare cu organizații neguvernamentale, institute de cercetare și alte organisme implicate	
6.3. Informaţii despre consultările organizate cu autorităţile administraţiei	

publice locale	
6.4. Informaţii privind puncte de vedere/opinii emise de organisme consultative constituite prin acte normative	
6.5. Informații privind avizarea de către: **a) Consiliul Legislativ** **b) Consiliul Suprem de Apărare a Țării** **c) Consiliul Economic și Social** **d) Consiliul Concurentei** **e) Curtea de Conturi**	
6.6. Alte informații	
Secțiunea a 7-a **Activități de informare publică privind elaborarea și implementarea proiectului**	
7.1. Informarea societății civile cu privire la elaborarea proiectului de act normativ	Proiectul are caracter individual, sens în care nu sunt incidente dispozițiile Legii nr. 52/2003 *privind transparența decizională în administrația publică.*
2. Informarea societății civile cu privire la eventualul impact asupra mediului in urma implementării proiectului de act normativ, precum si efectele asupra sănătății și securității cetățenilor sau diversității biologice	
Secțiunea a 8-a **Măsuri privind implementarea, monitorizarea şi evaluarea proiectului**	
8.1. Măsurile de punere în aplicare a proiectului	Implementarea măsurilor cuprinse în proiect se realizează de către Ministerul Afacerilor Interne, prin Direcția Generală de Protecție Internă
8.2. Alte informații	Proiectul se încadrează în situațiile prevăzute la art. 110 alin. (2) și (4) din Constituția României, republicată, iar soluțiile propuse prin acesta reprezintă acte de administrare a treburilor publice, care nu presupun o decizie de oportunitate și este necesar să fie emise de Guvern pentru asigurarea organizării executării legilor.

În considerarea celor prezentate, a fost elaborat **proiectul hotărârii Guvernului pentru reaprobarea Notei de fundamentare privind necesitatea și oportunitatea efectuării cheltuielilor aferente proiectului de investiții „Sistem de alertă timpurie – SAT (Early warning system)”,** pe care îl supunem Guvernului pentru adoptare.

VICEPRIM-MINISTRU,
MINISTRUL AFACERILOR INTERNE

MARIAN-CĂTĂLIN PREDOIU

AVIZAT:

MINISTRUL INVESTIȚIILOR ȘI PROIECTELOR EUROPENE

DRAGOȘ-NICOLAE PÎSLARU

MINISTRUL FINANȚELOR

ALEXANDRU NAZARE