ANNEX VI*[[1]](#footnote-1)* Template of a programme for the AMIF, the ISF and the BMVI – Article 16(3)

**PROGRAMUL NAȚIONAL**

**FONDUL SECURITATE INTERNĂ 2021-2027**

|  |  |
| --- | --- |
| CCI number |  |
| Title in English | [255 CHARACTERS[[2]](#footnote-2)]  NATIONAL PROGRAMME INTERNAL SECURITY FUND |
| Title in the national language | [255] PROGRAMUL NAȚIONAL FONDUL SECURITATE INTERNĂ |
| Version | DRAFT 1 |
| First Year | 2021 |
| Last Year | 2027 |
| Eligible from | 1 IANUARIE 2021 |
| Eligible until | 31 DECEMBRIE 2029 |
| Commission Decision Number |  |
| Commission Decision Date |  |
| Member State amending decision number |  |
| Member State amending decision  entry into force date |  |

1. **Programme strategy: main challenges and policy responses**

*Reference: Article 17(3)(a) )(ii bis), (iii), (iv) and (vii) and CPR*

|  |
| --- |
| *This section explains how the programme will address the main challenges identified at the national level based on local, regional and national needs assessments and/or strategies. It provides an overview of the state of implementation of relevant EU acquis and the progress achieved on EU action plans, and describes how the Fund will support their development through the programming period.*  *Text field [15 000]* |

În linii generale, în România, fenomenul de **criminalitate organizată** se menține la cote ridicate, grupuri de interese continuând să se implice în activități economice ilegale de mare amploare. România reprezintă, de asemenea, predominant, un spațiu de tranzit pentru **migrația ilegală** şi pentru rutele **traficului internațional de droguri** de mare risc, grupări de criminalitate organizată autohtone implicându-se preponderent pe palierul de intermediere sau sprijin.

Europol, în evaluarea amenințărilor de criminalitate organizată întreprinsă la nivelul agențiilor de aplicare a legii din cadrul UE, document denumit, „E.U. Serious and Organised Crime Treath Assesment 2017” arăta că: ”*Mai mult de o treime din grupările de criminalitate organizată sunt implicate în producerea traficarea și distribuția drogurilor. Alte activități infracționale importante includ furturile, migrația ilegală, traficul de persoane și criminalitatea economică*.” Studiul reprezintă documentul ce stă la baza conceptului Policy Cycle și la planificarea strategiilor și activităților pentru combaterea criminalității organizate în spațiul European.

Fondul va aborda principalele provocări și domenii de acțiune identificate pe baza documentelor strategice naționale și europene, aferente fiecărui domeniu în parte, detaliate în cele ce urmează.

**Criminalitatea informatică** se situează pe o tendință ascendentă, aspect identificat în proiectul Strategiei Naționale de Apărare a Țării 2020 – 2024, tot mai multe grupări autohtone specializându-se în activități ilicite din această sferă cum ar fi: compromitere de ATM-uri și POS-uri, clonări de carduri, acces neautorizat în sisteme informatice, interceptarea ilegală de date informatice, postare de anunțuri fictive pe site-uri de comerț intens accesate, infectarea sistemelor informatice cu ransomware, preluarea sub control de resurse informatice pentru minarea de monede virtuale, dar şi utilizarea sau exploatarea criptomonedelor pentru derularea de operațiuni ilicite din zona economică.

Tendințele și factorii de risc identificați în domeniul criminalității informatice pentru următoarea perioada vizează, în principal:

- Apariția unor noi moduri de operare, devenite, din punct de vedere tehnic, din ce în ce mai complexe, incluzând majoritatea infracțiunilor din sfera criminalității organizate;

- Folosirea facilităților oferite de dezvoltarea tehnologica (dispozitive performanțe, aplicații de criptare a comunicațiilor, utilizarea cripto-monedelor) în vederea disimulării/anonimizării accesului la internet, ascunderea identității reale a autorilor, în contrapondere cu accesul dificil/redus al autorităților de aplicare a legii la astfel de tehnologii;

- Existența elementelor de extraneitate, existența de rețele specializate doar în anumite genuri de activități infracționale, gradul ridicat de mobilitate grupărilor transnaționale de criminalitate informatică, atât în interiorul UE cât și în afara spațiului UE;

- Utilizarea de servicii de genul **Crime as a service – CaaS**, accesul facil la astfel de servicii și Darknet pentru persoane/autori care nu au nevoie de cunoștințe tehnice avansate pentru a se implica în infracțiuni informatice;

- Creșterea numărului de cazuri privind **atacurile informatice** de tip ransomware, acest gen de atacuri sunt tot mai mult orientate spre atacuri mult mai profitabile din punct de vedere financiar și pot provoca pagube economice majore, pe fondul existenței de rețele informatice și calculatoare fără măsuri de siguranța sau cu măsuri de siguranța învechite;

- Creșterea numărului de infracțiuni cu carduri bancare săvârșite pe teritoriul României şi al celor comise în străinătate de cetățenii români, prin confecționarea şi folosirea echipamentelor de **skimming/fraudarea tranzacţiilor efectuate la ATM-uri şi POS-uri** sau sau utilizarea de noi moduri de operare care vizează compromiterea securității informatice a ATM -urilor sau chiar declanșarea unor atacuri informatice care vizează rețelele informatice ale instituțiilor bancare în scopul sustragerii de sume importante de bani;

- Creșterea numărului de accesări neautorizate ale adreselor de poştă electronică ale persoanelor private, instituțiilor publice sau întreprinderilor private, în scopul săvârșirii de fraude informatice, creșterea numărului de cazuri de **fraude de tip BEC** (Business Email Compromise), în urma cărora sunt fraudate companii din România;

- Dezvoltarea de legături infracționale între grupările infracționale organizate și entități statale sau non statale și inițiere de atacuri informatice asupra instituțiilor private și de stat, sau asupra infrastructurilor informatice critice, în vederea obținerii de date informatice confidențiale, sau producerea de pagube majore - criminalitatea informatică ca forma de manifestare a războiului hibrid, inclusiv **cyber-terorism**

- Utilizarea monedei virtuale în tranzacțiile financiare, în activități de **spălare a banilo**r și disimularea provenienței produsului financiar ilicit, raportat la posibilitățile reduse de investigare a autorităților de aplicare a legii;

- Trendul ascendent al **pornografiei infantile prin sisteme informatice**. Se observă o creștere a numărului de cazuri generate de accesului facil la tehnologie atât al infractorilor cat și al victimelor (în special în cazul auto producerii de material pornografic), dar și apariția noilor moduri de operare – livestreaming, crearea de grupuri închise, dedicate prin intermediul diferitelor aplicații de social media (Instagram, Telegram, WhatsApp) ;

În contextul **transpunerii Directivei NIS** (Directiva UE 2016/1148) este preconizată o creștere a nivelului de sesizări cu privire la incidente de securitate cibernetică, raportate de către furnizorii și operatorii de servicii digitale din cele 7 sectoare de activitate economică, printre care: piețe online, motoare de căutare online și servicii de claud computing. Aceste incidente pot periclita grav securitatea în mediul online la nivelul statelor membre UE.

**Traficul de persoane** a înregistrat o creștere în ultima perioada, în contextul fluxului de migrație înregistrat în UE având ca sursă principală de proveniență regiunile afectate de conflictele militare din Orientul Mijlociu, Asia și Africa Subsahariană. Totodată, s-au dezvoltat și o serie de mutații în tiparul de derulare a acestui tip de infracțiune, cu implicații pentru situația României. Un exemplu este dat de reprofilarea unor rețele infracționale transnaționale, specializate în contrabanda cu produse din tutun sau traficul de produse contrafăcute, pe activități de trafic de migranți și, în unele cazuri, de trafic de persoane pentru exploatarea sexuală sau prin muncă.

Acțiunile de combatere a traficului de persoane vor fi complementare acțiunilor de **prevenire** a acestui fenomen, în conformitate cu prevederile Directivei 36/2011 *privind prevenirea și combaterea traficului de persoane și protejarea victimelor acestuia.* România a notificat transpunerea în termen a prevederilor Directivei 36/2011 iar activitățile de prevenire, combatere și asistență a victimelor se desfășoară în conformitate cu prevederile acesteia. În perioada 2014 – 2020, un accent deosebit s-a pus pe adoptarea unor măsuri de descurajare și reducere a cererii care favorizează toate formele de exploatare și pe măsuri de reducere a riscului ca oamenii să devină victime ale traficului de persoane.

Și în domeniul **protecției martorilor** România intenționează sa înregistreze progrese și își propune să răspundă provocărilor legate de operaționalizarea pachetului de interoperabilitate ce presupune asocierea datelor biometrice cu cele personale. În acest context, schimbarea identității martorilor protejați nu va mai fi suficientă pentru protejarea martorilor întrucât parametrii faciali (necesari componentei facial recognition), datele digital-palmare (amprente) precum și orice alte informații similare sunt asociate datelor cu caracter personal.

Printre direcțiile de acțiune prevăzute în Strategia Națională de Apărare a Țării 2020 - 2024 se numără și **dezvoltarea cooperării internaționale** atât în formatele de cooperare regională (Convenţia de cooperare poliţienească din Europa de Sud-Est, Asociația Șefilor de Poliție din Europa de Sud-Est), cât şi în cele din cadrul UE (EUROPOL, Agenţia FRONTEX), în vederea combaterii criminalității organizate transnaționale.

Totodată, România va continua să participe în cadrul Proiectului **EMPACT,** în viitorul ciclu de politici 2021-2024, susținând dezvoltarea structurilor de combatere a criminalității organizate.

În contextul transpunerii în legislația din România a prevederilor articolelor 14 și 16 din cadrul Directivei 2019/713 privind **combaterea fraudelor şi a contrafacerii** în legătură cu mijloacele de plată fără numerar, structurile de combatere a criminalității informatice vor fi implicate în soluționarea cât mai urgentă a cererilor de asistență și cooperare în domeniul combaterii fraudelor cu instrumente de plata electronică, sosite prin punctele de contact 24/7, prevăzute în art. 14 din Directiva, și totodată vor fi implicate în soluționarea plângerilor transmise de victimele acestui gen de infracțiuni conform art. 16 din aceeași Directiva.

În domeniul **interoperabilității / schimbului de informații,** Fondul va aborda principalele provocări și domenii de acțiune identificate pe baza *Masterplan-ului pentru implementarea noii arhitecturi a sistemelor de informații pentru securitate și frontieră*. Totodată, în România se va pune în continuare accent pe implementarea Directivei 681/2016 privind utilizarea datelor din registrul cu numele pasagerilor (PNR). România a înregistrat progrese semnificative, finanțarea FSI 2014 – 2020 fiind utilizată pentru modernizarea soluției informatice, creșterii numărul de transportatori aerieni care transmit date PNR și realizării unei soluții de Disaster Recovery.

Conform Raportului de țară România 2019 - **Semestrul European** 2019, **corupția** rămâne o problemă majoră și împiedică mediul de afaceri. Corupția, precum și nepotismul sunt identificate ca *obstacole în calea activității în România de 85% și respectiv 82% dintre întreprinderi (medii UE: 37%, respectiv 38%). Poziția României cu privire la indicatorul de incidență a corupției din Indicele Global al Competitivității din 2018 stagnează, clasându-se printre ultimele din UE, însă unele regiuni au înregistrat progrese semnificative pozitive în ultimii ani.* În acest context, activitățile de prevenire și combatere a corupției se numără printre prioritățile orizontale ale politicilor UE, identificate ca atare în Strategia Națională Anticorupție. România va face și în continuare eforturi care se înscriu în politicile UE de prevenire și reducere a corupției și menținerea unui cadru de integritate.

Directiva 2008/114/CE privind identificarea și desemnarea **infrastructurilor critice europene** și evaluarea necesității de îmbunătățire a protecției acestora este transpusa în legislația românească prin OUG nr. 98/2010 și Legea nr. 18/2011. Astfel, România va continua eforturile pentru implementarea Directivei 2008/114/CE, punând accent pe obligația de a pune în aplicare un mecanism de comunicare adecvat între autoritatea competentă a statului membru și ofițerul de legătură pentru securitate, sau echivalentul acestuia, în scopul schimbului de informații relevante privind riscurile și amenințările identificate în legătură cu infrastructura critică europeană respectivă.

O altă obligație asupra căreia România își va concentra eforturile este aceea conform căreia fiecare SM va prezenta COMi la fiecare doi ani un raport de sinteză cu date generale privind tipurile de riscuri, amenințări și puncte vulnerabile întâmpinate în fiecare dintre sectoarele ICE în care a fost desemnată o ICE în temeiul articolului 4 al Directivei și care se află pe teritoriul său.

**Ameninţările teroriste** la adresa României nu au atins caracterul de iminenţă, riscurile teroriste fiind conexate preponderent evoluțiilor externe de securitate.

Deși cei implicați în activități de risc pe profil AT sunt cu precădere cetățeni străini, cu un profil radical, adepți ai jihadului global, se remarcă un trend ascendent al (auto)radicalizării și implicării în activități generatoare de riscuri de securitate și în cazul unor cetățeni români convertiți.

În România, în ultimii ani, **radicalizarea** a cunoscut un trend constant ascendent, reţinând atenţia procesele de radicalizare identificate în rândul:

- minorilor/ tinerilor - categorie vulnerabilă pe fondul, atât al vârstei fragede ce reprezintă un factor important în procesul de radicalizare, cât și al prezenţei ridicate a subiectului terorism în mass-media şi a atractivităţii acestuia pentru tinerii aflaţi într-o etapă "a căutărilor", a stabilirii propriei identităţi;

- unor persoane care au executat pedepse privative de libertate, fiind evidențiată înclinația acestora spre violenţă;

În prezent, **acțiunile extremist - violente** și radicalizarea evidențiază o accelerare a trecerii din planul declarativ în cel acțional, fiind caracterizate de:

- atacuri individuale;

- parcurgerea unui proces rapid de radicalizare - depăşirea accelerată a stadiului declarativ şi trecerea la acţiune a indivizilor radicalizaţi, fie sub un imbold personal, fie sub îndrumarea unor elemente radicale cu care se află în contact;

- orientarea către ținte soft, dar cu un puternic impact emoțional;

- spontaneitatea și imprevizibilitatea momentului declanşării unor acte violente;

- utilizarea unor tehnici și metode de comitere a atentatelor facile și simpliste utilizând arme albe sau de foc.

Printre provocările identificate în plan național, ce vizează extremismul și radicalizarea se numără:

-­ creșterea exponenţială a utilizării mediului online și a social-media (cu accent pe rețelele criptate), accesul facil şi în „timp real” la conţinut extremist şi terorist, în paralel cu insuficiența instrumentelor legislative adecvate pentru limitarea propagării acestui tip de mesaje;

- linia relativă de demarcaţie între propaganda cu tente extremiste/ radicale şi dreptul la liberă exprimare sau între teribilismul specific vârstei și al activismului social,respectiv eficienţa scăzută a unor metode coercitive (precum cenzurarea sau închiderea unui blog, site ori cont de pe o reţea de socializare. În cazul blocării conturilor online utilizate de extremiști, aceștia își creează noi profiluri în cadrul cărora derulează activități similare, concomitent cu accentuarea radicalizării și adoptarea unor măsuri contrainformative suplimentare);

- cunoaşterea insuficientă a evoluţiilor/indicatorilor relevanţi de (auto)radicalizare care se manifestă la nivel individual limitează implicit capacitatea autorităţilor competente de a interveni preventiv, pentru a preîntâmpina şi înlătura premisele de parcurgere a tuturor etapelor de radicalizare ale persoanelor vulnerabile şi care au intrat în contact cu ideologia extremistă;

- lipsa unor programe de pregătire, la nivelul societăţii, care să permită identificarea corectă a radicalizării islamice la cât mai multe nivele (combătând xenofobia şi alte prejudecăţi) şi crearea unor mecanisme de (re)inserţie socială ca soluţii de protejare sau extragere a individului de sub influenţa ideologiei radicale/ extremiste.

România va avea în vedere asigurarea complementarității și sinergiilor cu obiectivele politicii de coeziune, conform prevederilor Acordului de Parteneriat 2021 – 2027. Astfel, se va asigura corelarea și sincronizarea intervențiilor finanțate prin FSI cu cele din cele 8 fonduri structurale, pe domenii cum ar fi protecția victimelor sau securitatea cibernetică.

1. **Specific objectives**

*(repeated for each specific objective other than technical assistance )*

*Reference: Article 17(2) and 17(4)*

## 2.1. Title of the specific objective [300] Sporirea schimburilor de informații dintre și în cadrul autorităților de aplicare a legii și al altor autorități competente și organisme ale Uniunii, precum și cu țările terțe și organizațiile internaționale, și sporirea capacităților aferente ale statelor membre.

**2.1.1. Description of a specific objective**

|  |
| --- |
| *This section describes, for each specific objective, the initial situation, main challenges and proposes responses supported by the Fund. It describes which implementation measures are addressed with the support of the Fund; it provides an indicative list of actions within the scope of Articles 3 and 4 of the AMIF, ISF or BMVI Regulations.*  *In particular: For operating support, it provides a justification in line with Article 15[[3]](#footnote-3)of the ISF Regulation, Articles 15 and 16 of the BMVI Regulation or Artic-le 18 of the AMIF Regulation. It includes an indicative list of beneficiaries with their statutory responsibilities, main tasks to be supported.*  *Planned use of financial instruments, if applicable.*  *Text field (16 000 characters)* |

În ultima perioadă, România a contribuit semnificativ la îmbunătățirea capacității de **schimb de informații**, inclusiv cu sprijinul finanțărilor externe nerambursabile. Printre exemple se numără dezvoltarea **Unității Naționale de Informații privind Pasagerii**, extinderea rețelei **SIENA** și modernizarea **AFIS.**

În ceea ce privește **AFIS,** în perioada următoare sistemul va beneficia de finanțare prin intermediul Mecanismului Financiar Norvegian. Astfel, sistemul va urma să îndeplinească toate cerințele stabilite prin Regulamentele UE nr. 817/2019 și 818/2019 privind stabilirea unui cadru pentru interoperabilitatea între sistemele de informații ale UE în domeniul frontierelor și vizelor și cele în domeniul cooperării polițienești și judiciare, azil și migrație. În vederea asigurării interoperabilității AFIS cu EURODAC, SIS, VIS, dar și cu viitoarele sisteme informatice EES și ECRIS-TCN, sistemul AFIS va avea capacitatea de a prelucra și exportă noile tipuri de fișiere NIST care conțin date dactiloscopice. În plus, odată cu modernizarea sistemului și introducerea posibilității de furnizare a fișierelor tip NIST, se va asigura operaționalizarea schimbului de date dactiloscopice cu FBI, cu țările membre ale organizației PCC SEE, cu Web Interpol Services for Data Management (WISDM), dar și cu statele membre în context Prüm.

**SIENA** reprezintă o rețea de comunicare securizată care asigură accesul unităților de poliție la rețeaua Europol și implicit la aplicaţiile şi bazele de date puse la dispoziţie prin intermediul acestora. La nivelul anului 2014, SIENA era implementată la nivelul a 12 autorități de aplicare a legii de la nivel național, Poliția Română prin Unitatea Națională Europol reprezentând punctul de prezență al SIENA în România. Prin intermediul FSI 2014 – 2020, rețeaua SIENA a fost extinsă către cele 42 de unități teritoriale ale României.

Directiva (UE) 681/2016 privind utilizarea datelor din **registrul cu numele pasagerilor (PNR)** pentru prevenirea, depistarea, investigarea și urmărirea penală a infracțiunilor de terorism și a infracțiunilor grave a fost transpusă în România prin Legea 284/2018. Dezvoltarea Unității Naționale de Informații privind Pasagerii (UNIP) a beneficiat de finanțare prin FSI 2014-2020 în vederea îmbunătățirii schimbului de informații. Astfel, va fi modernizată soluția informatică, va crește numărul de transportatori aerieni care transmit date PNR și va fi realizată o soluție de Disaster Recovery, concomitent cu pregătirea personalului.

Se remarcă o tendință de creștere a nevoilor de prelucrare a datelor PNR, luând în considerare și faptul că numărul de pasageri care folosesc frontierele aeriene ale României a crescut semnificativ în ultimii ani (2016 – 14,2 mil.; 2017 – 17,2 mil.; 2018 – 18,6 mil; 2019 – 20,2 mil ), situație care va genera nevoia de optimizare a soluției informatice actuale sau dezvoltarea/implementarea unei noi soluții informatice.

Totodată, a crescut și numărul de infracțiuni aflate în competența Poliției de Frontieră raportat la valoarea adăugată a activității de targeting în prevenirea și combaterea infracțiunilor de terorism, a infracțiunilor grave și a amenințărilor la adresa siguranței naționale, actuala soluție informatică având limitări în aplicarea/implementarea conceptului de targeting raportat la modalitățile concrete de creare/implementare/adaptare/monitorizare și actualizare a profilurilor de risc, coroborat cu aspecte privind recepția datelor PNR și asigurarea calității acestora.

România va acorda și în viitor o atenție sporită **gestionării sistemelor europene de informaţii.** Astfel, pentru respectarea angajamentului asumat la nivel european de a implementa la timp noua arhitectură a sistemelor europene de informații, a fost constituit un Comitet de coordonare a noii arhitecturi a sistemelor europene de informații pentru frontieră şi securitate, ce funcționează în cadrul Ministerului Afacerilor Interne. În acest scop, România a elaborat un document programatic și de monitorizare a implementării tuturor sistemelor- Masterplan- care contine toate măsurile avute în vedere pentru reușita acestui obiectiv.

Totodată, în conformitate cu direcția de acțiune 2.3. aferentă obiectivul strategic nr. 2 din Strategia națională de **protecție a infrastructurilor critice** aprobată prin HG nr. 718/2011, se prevede punerea în aplicare la nivel național a unui mecanism de comunicare adecvat între autoritățile naționale responsabile și ofițerii de legătură pentru securitate sau echivalenții acestora, în scopul eficientizării schimbului de informații relevante privind riscurile și amenințările identificate în legătură cu infrastructurile critice respective.

În domeniul **armelor de foc,** avansul tehnologic al ultimilor ani a avut un impact decisiv asupra dezvoltării mijloacelor și metodelor de identificare a acestora, în prezent fiind gestionate și stocate date privind arma, muniția, fabricantul, deținătorul etc. Pe viitor, aceste informații pot fi valorificate în schițarea unui istoric al tranzacțiilor și al deținătorilor, detectarea rutelor de traficare și a tendințelor de procurare (de ex. arme reactivate, arme cu gaze convertite în arme de foc, arme de foc provenite din zonele de conflict militar etc), concomitent fiind disponibile date despre părțile componente ale armei sau muniției utilizate. Totodată, informațiile obținute despre arme furate, pierdute sau mijloace de probă vor face obiectul unor semnalări în Sistemul de Informații Schengen, aceasta fiind si una dintre prioritățile identificate în fișa de țară a României.

În timp ce aplicația **iARMS** verifică dacă o armă este raportată ca sustrasă/traficată/introdusă prin contrabandă, într-un anumit stat, prin utilizarea unui sistem automat de identificare balistică a armei după urmele de tragere create pe gloanțe și tuburile trase, precum și realizarea schimbului internațional de date balistice, se va putea verifica dacă arma traficată a fost folosită la fapte în spațiul național și/sau european, venind în completarea activității investigative.

Activitatea de **schimb de date genetice** se va intensifica semnificativ în contextul Directivei 93/2011, a Deciziei 2008/615/JAI, Deciziei 2008/616/JAI, Regulamentului 2018/1862 și Deciziei 905/2009 privind acreditarea furnizorilor de servicii de expertiză criminalistică care efectuează activități de laborator. În același context, numărul crescut al profilurilor genetice obținute vor face în continuare obiectul schimbului de date genetice, realizat prin intermediul mecanismelor de cooperare internațională (Tratatul Prum), aducând beneficii sporite la nivel național și european. Toate aceste demersuri vor necesita susținere prin consolidarea capacității operaționale în domeniul realizării analizelor genetice.

Potențialul **atacurilor CBRN** este subliniat în mod vizibil în propaganda teroristă, presa jihadistă exprimându-și intențiile de a comite atacuri CBRN și distribuind – prin intermediul diferitor platforme de comunicare socială – posibile tactici de atac și ținte. În acest context, se impune consolidarea relațiilor de colaborare și intensificarea relațiilor de cooperare printr-un schimb eficient și operativ de date și informații cu statele din zona balcanică, prin prisma relațiilor dezvoltate anterior cu structuri similare în domeniu. Totodată, este necesară asigurarea unei identificări și a unei caracterizări rapide, precum și a unor mecanisme rapide de punere în comun a probelor obținute din atacuri CBRN, aspecte ce vor fi realizate prin dezvoltarea capabilităților laboratorului institutului național de criminalistică. Concomitent, laboratorul trebuie conectat la baza **EBDS** a Europol pentru asigurarea sinergiei în domeniul schimbului de informații și al consolidării capacității Statelor Membre în domeniul intervențiilor în situații de criză

În prezent, pe teritoriul României sunt comercializate o mare parte din bunurile provenite din săvârșirea de infracțiuni în spațiul european. În acest context se consideră benefică realizarea unei platforme online destinată cetățenilor și organelor judiciare naționale și din statele membre UE, în vederea verificării **provenienței licite a bunurilor** achiziționate. Platforma ar putea fi alimentată cu informații despre bunuri furate cert individualizate, prin categorie și serie/număr, de către organele judiciare ca urmare a înregistrării sesizărilor cu privire la comiterea unor fapte penale. Realizarea platformei ar permite accesarea acesteia de către cetățeni, în condiții de siguranță.

**Pornografia infantilă** prin sisteme informatice înregistrează un trend ascendent, fiind identificată ca prioritate și în fișa de țară a României. Se poate observa o creștere a numărului de cazuri, datorită accesului facil la tehnologie atât al infractorilor cât și al victimelor (în special în cazul auto producerii de material pornografic). Informațiile primite indică puternic creșterea activității online de către cei care caută materiale pentru abuzuri asupra copiilor. Aceasta este în concordanță cu postările în forumuri dedicate de către infractori primind oportunități de a interacționa cu copiii care sunt în această perioadă mai vulnerabili din cauza izolării, mai puțin supravegheați și cu expunere online mai mare.

În prezent, datele legate de cauzele din domeniul **criminalității informatice** sunt descentralizate, existând de foarte multe ori sincope în a înțelege fenomenul în totalitate, la nivel național, astfel încât este necesară consolidarea schimbului de date și informații între autoritățile de aplicare a legii din România.

În ceea ce ce privește **infracțiunile cu instrumente de plată electronică,** acestea se afla la un nivel stabil, utilizarea frauduloasă a datelor cardurilor bancare fiind în creștere datorită creșterii numărului de utilizatori și lipsei de prevenție din partea utilizatorilor. Se poate anticipa o creștere a acestui gen de fapte, în special în zona fraudelor cu instrumente de plată electronică online, accentuată în actualul context COVID 19, de utilizarea cardurilor bancare la achiziționarea de bunuri și servicii în mediul online și utilizarea cardurilor pentru plata produselor și serviciilor la POS. Utilizarea tot mai frecventă în mediul online a cardurilor bancare, sugerată chiar de reprezentanții sistemului bancar ca măsură anti COVID va atrage cu certitudine atenția grupărilor infracționale care vor încerca prin diverse metode sa compromit aceste facilități de plată.

Totodată se poate observa o mutație în aceasta zona infracțională, în sensul că membrii grupărilor infracționale specializate în infracțiuni cu instrumente de plata se pot orienta spre zona atacurilor de tip ATM malware sau BlackBox attacks împotriva bancomatelor, măsură în care, acest mod de operare devine tot mai accesibil.

În domeniul **fraudelor informatice** se înregistrează o diversificare a modurilor de operare, acestea urmărind tot mai mult utilizarea tehnologiei digitale și a oportunităților oferite de internet. Campaniile de phishing, din ce în ce mai diverse și sofisticate, ofertele de produse și servicii la prețuri avantajoase, promovate în mediul online, sub diverse forme: site-uri false, site-uri de scam, rețele de socializare, campanii de email, sunt cateva din formele de manifestare ale fraudelor în mediul online. Important de remarcat este faptul că o parte din aceste fraude vizează victime cu potențial finaciar, în special companii private sau instituții de stat. O creștere majoră atât la nivel național cât și internațional se referă la cazurile de tip BEC (Business Email Compromise ) în care grupările infracționale transnaționale organizate reușesc să compromită modul de desfășurare a afacerilor între partenerii de afaceri, de cele mai multe ori aflați în țări diferite, obțin informații confidențiale relevante, și astfel reușesc să obțină importante sume de bani, sume care ulterior sunt transferate în conturi din țări unde cooperarea internațională este deficitară.

Important de menționat este și faptul că structura centrală de combatere a criminalității informatice din cadrul Poliției Române este implicată în gestionarea cererilor de asistență și a cererilor de conservare de date informatice transmise prin intermediul **rețelei de puncte de contact 24/7** organizată în baza Convenției privind combaterea criminalității informatice de la Budapesta cât și în cadrul Rețelei G7 24/7 High Tech Crime Network.

**Utilizarea cryptomonedelor,** ca metodă de spălare a sumelor de bani provenite din activități din sfera criminalității informatice rămâne în continuare o provocare pentru structurile de aplicare a legii, pe fondul utilizării din ce în ce mai mult a acestui mod de plată.

Pandemia COVID 19 are impact și asupra operațiunilor **Darkweb**. Anumite bunuri ilicite vor deveni mai scumpe, deoarece piețele sursă devin indisponibile, iar vânzătorii activi pe Darkweb oferă aceste produse speciale pentru COVID19 la reduceri.

Astfel, Programul Național FSI al României va finanța următoarele măsuri de implementare:

1. asigurarea aplicării uniforme a acquis-ului Uniunii în domeniul securității prin sprijinirea schimbului de informații;

2. instituirea, adaptarea și menținerea unor sisteme și rețele TIC la nivel național și la nivelul Uniunii, relevante pentru securitate, inclusiv asigurarea interoperabilității acestora, și elaborarea unor instrumente adecvate pentru remedierea lacunelor identificate;

3. sporirea utilizării active a instrumentelor, a sistemelor și a bazelor de date de la nivelul Uniunii și de la nivel național care susțin schimbul de informații relevante pentru securitate, asigurându-se alimentarea acestora cu date de înaltă calitate;

4. sprijinirea măsurilor de la nivel național și de la nivelul Uniunii care sunt relevante pentru punerea în aplicare a obiectivelor specifice prevăzute la articolul 3 alineatul (2) litera (a) din Regulament

Acțiunile avute în vedere în cadrul PN FSI sunt, în principal, următoarele:

• sisteme și rețele TIC care contribuie la realizarea obiectivelor prezentului regulament, formarea cu privire la utilizarea acestor sisteme, testarea și îmbunătățirea interoperabilității și a calității datelor acestor sisteme;

• monitorizarea punerii în aplicare, în statele membre, a legislației Uniunii și a obiectivelor strategice ale Uniunii în domeniul sistemelor de informații privind securitatea;

• sprijin pentru crearea de rețele tematice sau transversale ale unităților naționale specializate în vederea îmbunătățirii încrederii reciproce, a schimbului și a diseminării de competențe și cunoștințe, de informații, de experiență și de bune practici, precum și a punerii în comun a resurselor și a expertizei în cadrul unor centre de excelență comune;

• educația și formarea personalului și a experților din cadrul autorităților de aplicare a legii, al autorităților judiciare și al agențiilor administrative relevante, ținând seama de nevoile operaționale și de analizele riscurilor;

• cooperarea cu sectorul privat cu scopul de a consolida încrederea și a îmbunătăți coordonarea, planificarea de contingență, precum și schimbul și diseminarea de informații și bune practici între actorii din sectorul public și privat, inclusiv în ceea ce privește protecția spațiilor publice și a infrastructurii critice;

• acțiuni care permit comunităților să elaboreze abordări și politici de prevenire locale, precum și acțiuni de sensibilizare și comunicare, în rândul părților interesate și al publicului larg, cu privire la politicile de securitate ale Uniunii;

• echipamente, mijloace de transport, sisteme de comunicații și facilități [...] relevante pentru securitate;

SPRIJIN OPERAȚIONAL: În temeiul art. 15 România va solicita sprijin operațional pentru întreținerea și asigurarea asistentei tehnice a sistemelor și rețelelor TIC de la nivelul Uniunii și de la nivel național, care contribuie la realizarea obiectivelor Regulamentului.

Beneficiari:

Poliția Română care, în conformitate cu Legea nr. 218/2002, republicată, este instituția specializată a statului, care exercită atribuții privind apărarea drepturilor și libertăților fundamentale ale persoanei, a proprietății private și publice, prevenirea și descoperirea infracțiunilor (....).

Poliția de Frontieră Română care este instituția în cadrul careia, în baza Legii nr 284/2018 de transpunere a Directivei 681/2016, funcționează Unitatea Națională de Informații privind Pasagerii.

## 2.2. Title of the specific objective [300] Intensificarea operațiunilor comune transfrontaliere dintre și în cadrul autorităților de aplicare a legii și al altor autorități competente în ceea ce privește toate formele de criminalitate, în special terorismul și criminalitatea gravă și organizată cu o dimensiune transfrontalieră

**2.2.1. Description of a specific objective**

|  |
| --- |
| *This section describes, for each specific objective, the initial situation, main challenges and proposes responses supported by the Fund. It describes which implementation measures are addressed with the support of the Fund; it provides an indicative list of actions within the scope of Articles 3 and 4 of the AMIF, ISF or BMVI Regulations.*  *In particular: For operating support, it provides a justification in line with Article 15[[4]](#footnote-4)of the ISF Regulation, Articles 15 and 16 of the BMVI Regulation or Artic-le 18 of the AMIF Regulation. It includes an indicative list of beneficiaries with their statutory responsibilities, main tasks to be supported.*  *Planned use of financial instruments, if applicable.*  *Text field (16 000 characters)* |

Poliția Română este un membru activ în cadrul EUROPOL, participând în cadrul parteneriatului şi cooperării internaționale între autoritățile române, Comisia Europeană şi **EUROPOL**, pe mai multe paliere circumscrise **priorităților EMPACT,** aceasta fiind și una dintre prioritățile stabilite pentru România prin fișa de țară, în cadrul Obiectivului Specific 2.

Anual, Poliția Română derulează, în medie, 50 de **operațiuni comune transfrontaliere,** cele mai multe dintre acestea vizând combaterea traficului de persoane, dar și a criminalității informatice, traficului de droguri sau combaterea spălării banilor. Doar în domeniul combaterii traficului de droguri, în perioada 2014-2020 au fost efectuate peste 200 de livrări supravegheate.

În cadrul Ciclului de Politici UE 2018-2022 România și-a asumat roluri de **Driver** (*prioritatea cybercrime, sub-prioritatea Non cash Paymenty Fraud*), **Codriver** (*prioritatea Traffiking in Human Beings și prioritatea Cybercrime, subprioritatea Empact Cyber attacks against Information Systems*) sau **Action Leader** (în cadrul tuturor priorităților).

Combaterea fenomenelor infracționale / moduri de operare, care afectează interesele statelor membre UE, pot fi realizate în mod unitar, integrat, pe mai multe domenii infracționale, în cadrul **JAD-urilor**.

De asemenea, în fiecare an România se implică activ, cu eforturi și rezultate notabile, în derularea activităților aferente zilelor comune de acțiune la nivel European - **JAD THB,** dedicate prevenirii și combaterii traficului de persoane.

În instrumentarea cauzelor penale în domeniul traficului de persoane pe plan internațional, România a cooperat cu autoritățile corespondente din ţările de destinaţie, sub egida EUROJUST, în cadrul unor **Joint Investigation Team - JIT** (echipe comune de anchetă), fiind înregistrat un progres semnificativ în ultimii ani.

Astfel, dacă în anul 2010 exista un singur **JIT** pe linia traficului de persoane, până în prezent ofițerii din cadrul structurilor de combatere a traficului de persoane au fost implicați în 61 de astfel de investigații comune cu state europene precum Marea Britanie, Germania, Spania, Belgia, Cehia, Danemarca, Elveția, Franța, Italia, Norvegia, în această perioadă, aflându-se în lucru un număr de 25 JIT-uri.

În cadrul E.U. Serious and Organised Crime Treath Assesment 2017, transportul bunurilor legale a fost identificat ca o componentă esențială pentru grupările infracționale în **transportul bunurilor ilegale**. Transportul rapid al bunurilor legale între țări terțe EU și piețele de desfacere s-au intensificat în volum și viteză ceea ce face imposibil un control adecvat. Posibilitățile clasice de control al mijloacelor de transport internațional în România sunt limitate și ineficiente, procentul descoperirilor de bunuri ilegale pe baza analizelor de risc și a controalelor raportat la alte țări din U.E. fiind unul mic.

Datele disponibile din **„European drug market report 2019”** indică faptul că, în general, disponibilitatea **drogurilor** în Europa rămâne pe toate tipurile de droguri. Piața europeană a drogurilor se caracterizează tot mai mult prin faptul că populația are acces la o varietate de droguri de mare puritate și cu potență ridicată care, în termeni reali, sunt de obicei fie echivalente ca preț fie mai ieftine decât în urmă cu zece ani. Utilizarea heroinei și a altor opioide încă reprezintă cea mai mare parte a riscurilor asociate consumului de droguri.

Piața drogurilor rămâne principala sursă de venituri pentru **grupările de criminalitate organizată**. Valoarea minimă a pieței drogurilor a fost estimată pentru anul 2017 la 30 miliarde de euro din care traficul de canabis reprezintă 39%, cocaina 31%, heroina 25% iar drogurile sintetice 5%.

**Ruta balcanică,** așa cum se subliniază și în documentul de țară, rămâne principalul coridor de intrare a heroinei în UE, în timp ce Balcanii de Vest par să rămână o sursă importantă de origine pentru canabisul vegetal confiscat. De asemenea, UE pare să fie din ce în ce mai utilizată ca zonă de tranzit pentru anumite droguri, cum ar fi cocaina, destinată altor piețe, iar drogurile cu potență ridicată precum opioidele sintetice sunt comercializate din ce în ce mai mult online și expediate prin poștă. În concluzie, fenomenul traficului de drogurilor devine din ce în ce mai global iar piața drogurilor din România este puternic interconectată la tendințele europene. Luând în considerarea rutele comerciale ce tranzitează România traficul de droguri are un canal logistic creat care este exploatat de către grupările de criminalitate organizată. Pentru a putea destructura rețelele de trafic de droguri ce acționează global și pentru a avea un real impact asupra pieței drogurilor, anumite măsuri concrete trebuie întreprinse pentru a întrerupe acest flux, așa cum se indica și în fișa de țară a României. În proiectul de strategie Europeană antidrog pentru perioada 2020- 2025 se prevăd obiective strategice esențiale pentru destructurarea grupărilor ce acționează global. Unul din acestea este **creșterea capacității de detecție a cantităților mari de droguri, precursori și pre-precursori.** Acest obiectiv va fi transpus și în strategia națională antidrog pentru perioada 2021-2025 și îi va fi acordată o atenție sporită în cadrul PN FSI.

Având în vedere faptul că în ultimii ani grupările de **criminalitate organizată** sunt tot mai active pe mai multe genuri de criminalitate (organizații policriminale) fiind interesate de a se interconecta în circuitele legale comerciale și astfel de a avea permanent acces la infrastructuri economice din mai multe state europene exista riscul ca în viitor să se observe o dezvoltare a unor astfel de infrastructuri criminale. În această situație, menținerea și continuarea parteneriatelor operative prin organizarea **echipelor comune de genul JAD și J-CAT** ar crea premisele creșterii posibilităților de investigare, dar și a creșterii numărului de organizații criminale identificate și care operează în mai multe state europene și pe mai multe domenii infracționale, pe modelul oferirii de servicii de tipul crime as a service.

Prin intermediul **Cybercrime Action Taskforce (J-CAT)** Poliția Română reușește să schimbe într-un mod facil date și informații privind spețe complexe din aria criminalității informatice, participarea în cadrul J-CAT permițând consolidarea poziției în cadrul programului **EMPACT,** schimbul rapid de informații în cadrul echipelor de anchetă și detașarea de experți în cauze complexe de criminalitate informatica transfrontalieră.

România acționează, de asemenea, pe următoarele paliere de combatere a criminalității transfrontaliere:

- Asistența judiciară și polițienească internațională pentru combaterea infracțiunilor grupurilor organizate de criminalitate itinerantă care comit infracțiuni contra patrimoniului;

- Combaterea traficului internațional cu autovehicule;

- Combaterea traficului ilicit cu bunuri culturale mobile;

- Depistarea, prinderea și predarea/extrădarea persoanelor urmărite la nivel european/internațional.

Numai în anul 2019, Direcția de Investigații Criminale a efectuat 28 de delegări în vederea soluționării unor **ordine europene de anchetă** sau **cereri de comisie rogatorie internațională** formulate de autoritățile străine. Activitățile în aceste cereri de asistență judiciară internațională au constat în principal în: efectuarea de percheziții domiciliare, efectuarea de audieri de suspecţi/inculpaţi şi martori, punerea în executare de MEA, verificări şi identificări de persoane, investigaţii, identificări profile genetice (comparări formule ADN), interceptări convorbiri telefonice, listinguri apeluri şi comunicări telefonice și/sau efectuarea de filaje.

Astfel, Programul Național FSI al României va finanța următoarele măsuri de implementare:

1. intensificarea operațiilor de asigurare a respectării legii între statele membre, inclusiv, atunci când este cazul, în colaborare cu alți actori relevanți, în special pentru a se facilita și a se îmbunătăți utilizarea echipelor comune de anchetă, a patrulelor comune, a urmăririlor transfrontaliere, a supravegherii discrete și a altor mecanisme de cooperare operațională în cadrul ciclului de politici ale UE [...], punând accentul în special pe operațiile transfrontaliere;

2. îmbunătățirea coordonării și a cooperării între autoritățile de aplicare a legii și alte autorități competente în statele membre și între acestea, precum și cu alți actori relevanți, de exemplu prin intermediul rețelelor de unități naționale specializate, al rețelelor și structurilor de cooperare ale Uniunii și al centrelor Uniunii;

3. îmbunătățirea cooperării interinstituționale [...] la nivelul Uniunii între [...] statele membre [...] și organele, oficiile și agențiile relevante ale Uniunii [...], precum și la nivel național între autoritățile naționale ale fiecărui stat membru.

Acțiunile avute în vedere în cadrul PN FSI sunt, în principal, următoarele:

• sisteme și rețele TIC care contribuie la realizarea obiectivelor prezentului regulament, formarea cu privire la utilizarea acestor sisteme, testarea și îmbunătățirea interoperabilității și a calității datelor acestor sisteme;

• acțiuni operaționale în cadrul ciclului de politici ale UE;

• acțiuni care sprijină răspunsul eficace și coordonat la criză prin asigurarea unei legături între capacitățile sectoriale existente, centrele de expertiză și centrele de conștientizare cu privire la o anumită situație, inclusiv centrele pentru sănătate, protecție civilă și combaterea terorismului;

• sprijin pentru crearea de rețele tematice sau transversale ale unităților naționale specializate în vederea îmbunătățirii încrederii reciproce, a schimbului și a diseminării de competențe și cunoștințe, de informații, de experiență și de bune practici, precum și a punerii în comun a resurselor și a expertizei în cadrul unor centre de excelență comune;

• educația și formarea personalului și a experților din cadrul autorităților de aplicare a legii, al autorităților judiciare și al agențiilor administrative relevante, ținând seama de nevoile operaționale și de analizele riscurilor, [...] în cooperare cu CEPOL și, atunci când este cazul, cu Rețeaua Europeană de Formare Judiciară;

• acțiuni care permit comunităților să elaboreze abordări și politici de prevenire locale, precum și acțiuni de sensibilizare și comunicare, în rândul părților interesate și al publicului larg, cu privire la politicile de securitate ale Uniunii;

• echipamente, mijloace de transport, sisteme de comunicații și facilități [...] relevante pentru securitate;

• costurile cu personalul implicat în acțiunile sprijinite de fond sau acțiuni care necesită implicarea personalului din motive tehnice sau din motive legate de securitate.

SPRIJIN OPERAȚIONAL: În temeiul art. 15 România va solicita sprijin operațional pentru întreținerea echipamentelor tehnice sau a mijloacelor de transport utilizate pentru acțiuni în domeniul prevenirii, al detectării și al investigarii criminalității grave și organizate cu dimensiune transfrontalieră.

Beneficiari:

Inspectoratul General al Poliției Române (IGPR) care, în conformitate cu Legea nr. 218/2002, republicată, este instituția specializată a statului, care exercită atribuții privind apărarea drepturilor și libertăților fundamentale ale persoanei, a proprietății private și publice, prevenirea și descoperirea infracțiunilor (....).

## 2.3. Title of the specific objective [300] Sprijinirea eforturilor de consolidare a capacităților în ceea ce privește combaterea și prevenirea criminalității și a terorismului, inclusiv prin cooperarea sporită dintre autoritățile publice și toți actorii relevanți.

**2.3.1. Description of a specific objective**

|  |
| --- |
| *This section describes, for each specific objective, the initial situation, main challenges and proposes responses supported by the Fund. It describes which implementation measures are addressed with the support of the Fund; it provides an indicative list of actions within the scope of Articles 3 and 4 of the AMIF, ISF or BMVI Regulations.*  *In particular: For operating support, it provides a justification in line with Article 15[[5]](#footnote-5)of the ISF Regulation, Articles 15 and 16 of the BMVI Regulation or Artic-le 18 of the AMIF Regulation. It includes an indicative list of beneficiaries with their statutory responsibilities, main tasks to be supported.*  *Planned use of financial instruments, if applicable.*  *AMIF only: resettlement and solidarity shall be presented separately.*  *Text field (16 000 characters)* |

Pentru a asigura eficiența acțiunilor de **prevenire și combatere a criminalității și terorismului** este nevoie de conjugarea, cumulativa, a doi factori: o buna **capacitate instituțională,** cu personal suficient și dotări corespunzătoare alături de o bună **pregătire a personalului.**

Finanțarea oferită prin FSI în cadrul prezentului obiectiv specific va acționa pe ambele paliere, în toate domeniile eligibile, așa cum sunt identificate și în Fișa de țară a României. Protecția cetățenilor și a infrastructurilor critice, protecția martorilor, prevenirea radicalizării, combaterea criminalității informatice, a drogurilor, a criminalității organizate, a traficului de ființe umane sau de migranți și lupta anticorupție se vor bucura de finanțare atât în vederea creșterii capacității administrative, cât și a instruirii personalului. Desigur, acordarea finanțării va urmări cu prioritate rezolvarea problemelor identificate în urma unor analize instituționale riguroase și descrise, pe scurt, mai jos.

**Criminalitatea informatică,** identificată ca și prioritate și în fișa de țară a României, va fi una din principalele provocări căreia instituțiile aflate în luptă cu criminalitatea vor trebui să-i facă faţă în anii următori.

Doar o mică parte din faptele penale comise prin utilizarea sistemelor informatice ajung să fie reclamate și astfel aduse la cunoștința organelor judiciare, fiind dificil de obținut o privire de ansamblu asupra amplorii și evoluției fenomenului.

Lupta împotriva acestei criminalității va implica şi **sectorul privat,** acesta fiind detentorul tuturor probelor digitale necesare investigațiilor penale. Sectorul privat este primul care observă noile trenduri infracționale în acest domeniu, deține cunoștințe și poate fi implicat și în pregătirea specialiștilor din cadrul Poliției și autorităților judiciare, toate acesta în contextul COVID 19, în care cetățenii și companiile private sunt îndemnate să folosească serviciile de internet ca alternativa la serviciile fizice.

Una dintre problemele identificate este aceea că, în prezent, cooperarea cu furnizorii de servicii IT este destul de greoaie, solicitările din partea autorităților fiind transmise în format letric prin serviciul poştal. Acest fapt îngreunează de multe ori activitatea operativă şi întârzie desfășurarea activităților în dosarele penale.

În domeniul **combaterii pornografiei infantile** prin sisteme informatice se impune întărirea reacției autorităților de aplicare a legii, așa cum prevede și Strategia UE 2020 în domeniul combaterii abuzurilor împotriva copiilor, mai ales în contextul actual al pandemiei de COVID 19, în care atât copii, cât și abuzatorii, petrec din ce în ce mai mult timp în mediul online. Așa cum se menționează și în fișa de țară a României, se impune dezvoltarea structurilor naționale specializate în combaterea pornografiei infantile prin sisteme informatice și de prevenire a acestui gen infracțional. Măsurile de dezvoltare avute în vedere vizează: asigurarea cu echipamente necesare desfășurării investigațiilor, dezvoltarea de capabilități naționale în domeniul identificării victimelor și investigațiilor sub acoperire în mediul online și de infiltrare în rețelele online de pornografie infantilă, precum și participarea la inițiativele de cooperare internațională în acest domeniu atât la nivel EUROPOL EC3 cât și la nivel INTERPOL – ICSE.

Pandemia globală a COVID-19 a crescut și riscul de **criminalitate informatică.** Infractorii au folosit criza medicală pentru a efectua atacuri de inginerie socială, anume e-mailuri de tip **phishing** prin campanii de spam și încercări direcționate cum ar fi compromiterea e-mailurilor de afaceri (BEC).

Pe fondul noilor tendințe în materie de comitere a infracțiunilor, a modurilor avansate de operare folosite de infractori, a particularităților speciale ale noilor tipuri de urme și/sau altor mijloace materiale de probă descoperite în arealul infracțional, **activitatea de cercetare la fața locului** a devenit una dintre principalele precondiții pentru furnizarea unui probatoriu valid și relevant. Mai mult, numărul intervențiilor criminalistice este în continua creștere, în anul 2019 fiind realizate aproximativ 200.000 de astfel de intervenții.

Apariția acestor noi condiții în care trebuie analizate un volum mare al diferitelor tipuri de urme la locul faptei, precum și revizuirea procedurilor de cercetare și a bunelor practici stabilite împreună cu specialiști criminaliști din UE, impun utilizarea unor echipamente, tehnici și mijloace mobile moderne, care să răspundă în mod prompt, eficient și profesionist nevoilor actuale.

**Lupta împotriva traficului de persoane**, identificată ca și prioritate în fișa de țară a României, necesită o abordare coordonată, multidisciplinară, care să implice toţi factorii de decizie cu atribuții în acest domeniu și care sa abordeze atât latura preventivă, cât și cea de combatere a fenomenului.

Mobilitatea şi specializarea continuă a grupărilor criminale impune creșterea capacității de culegere cu operativitate de date privind traficul de persoane din spaţiile şi zonele de comitere, de transmiterea cu celeritate a informațiilor către beneficiari şi/sau parteneri si de facilitare a accesului echipelor multi-disciplinare de investigare în zonele de acţiune ale grupărilor criminale.

Activitățile de **prevenire a traficului de persoane** vor corespunde priorităților Directivei 36/2011 și vor consta în adoptarea unor măsuri de descurajare și reducere a cererii care favorizează toate formele de exploatare, precum și măsuri de reducere a riscului ca oamenii să devină victime ale traficului de persoane.

În România, funcționează încă din anul 2003 Oficiul Național pentru **Protecția Martorilor,** înregistrând, în medie, un coeficient anual de creștere cu 1,6 al persoanelor incluse în program. În același context, numărul activităților efectuate de Oficiu pentru atingerea obiectivelor programelor de protecția martorilor din alte state a crescut cu peste 20% în ultimii 3 ani.

Una dintre problemele întâmpinate o reprezintă dificultatea în gestiunea integrată a datelor și informațiilor operaționale cu incidență în managementul martorilor protejați prin prisma atât a volumului mare de date și informații, cât și a complexității și varietății surselor de date.

O altă problemă o reprezintă necesitatea unei mai bune corelări a datelor administrative cu informațiile operaționale, precum și monitorizarea în format letric a îndeplinirii obligațiilor martorilor protejați materializate în protocolul de protecție și schema de sprijin, fiind necesară gestiunea electronică a datelor pentru implementarea unor mecanisme informatice de tipul: activity planning (calendar, resurse, acțiuni propuse vs. efectiv realizate) și early warning.

Directiva PNR și regulamentele ETIAS și cele referitoare la pachetul interoperabilitate prevăd asocierea datelor biometrice cu cele personale. În acest mod, schimbarea identității nu va mai fi suficientă pentru protejarea martorilor întrucât parametrii faciali (necesari componentei facial recognition), datele digito-palmare (amprente) precum și orice alte informații similare sunt asociate datelor cu caracter personal. Astfel, în scenariul în care o persoană călătorește cu identitatea reală cărei îi sunt corelate datele biometrice, în cazul în care va intra în programul de protecție a martorilor și i se schimbă identitatea (deci numai datele cu caracter personal) și se prezintă la punctele de trecere a frontierei, noile sisteme informatice vor genera o alertă conform cărei datele personale nu se potrivesc cu cele biometrice.

România va urmări și în continuare îmbunătățirea capacității de a asigura un **nivel înalt de securitate la frontiera externă a UE,** precum și adoptarea şi implementarea politicilor comune în domeniu. De aceea este necesară continuarea eforturilor de utilizare a unor mecanisme eficiente de gestiune a resurselor umane, în vederea dezvoltării competenţelor şi abilităţilor personalului, continuarea sau dezvoltarea unor noi relații de cooperare cu structuri similare din ţările UE, de cooperare la Marea Neagră, dar şi cu diverse organisme şi organizaţii internaţionale cu atribuţii în domeniul managementului frontierei şi combaterii criminalității transfrontaliere (FRONTEX, EUROPOL, CEPOL, EUBAM, SELEC ș.a.).

În domeniul **protecției infrastructurilor critice,** Directiva 2008/114/CE a fost transpusă în legislația națională prin OUG 98/2010. Astfel, în România funcționează Centrul național de coordonare a protecției infrastructurilor critice care are responsabilitatea de a implementa un mecanism de comunicare și avertizare timpurie destinat asigurării managementului integrat al protecției ICN/ICE, cu rolul de sistem național securizat de informare în domeniul protecției ICN/ICE.

Acesta va asigura cadrul unitar al schimbului de informații privind incidente, amenințări, vulnerabilități și riscuri identificate în legătură cu aceste tipuri de infrastructuri, necesare atât în procesul de prevenție și combatere a riscurilor și amenințărilor, cât și pentru diminuarea impactului generat de incapacitatea de a menține serviciile esențiale furnizate de acestea.

În domeniul luptei **anticorupție,** așa cum se menționează și în fișa de țară, România va continua sa ofere un răspuns aplicat al solicitărilor UE formulate prin intermediul Raportul MCV care prevede ca “infracțiunile de corupție să poată fi investigate și sancționate în mod eficace, cu respectarea deplină a drepturilor fundamentale, iar cetățenii să poată avea încredere în independența sistemului judiciar”. În acest sens, Comisia sugerează “crearea unui sistem mai robust de măsuri de supraveghere tehnică utilizate de organele de urmărire penală”.

În prezent, fenomenul **radicalizării și terorismul** își găsesc inspirația într-o paletă vastă de ideologii, fiind contemporani unui trend ascendent al popularității curentelor extremiste, în rândul tinerilor, preponderent ale celor de extremă dreapta și extremist-islamice, concretizate în acțiuni violente sau acte teroriste.

Pornind de la personalitatea în formare a tinerilor, entităţile teroriste au creat și diseminat în spațiul virtual mesaje axate pe nevoile comune ale publicului țintă vizat, respectiv: apartenența, recunoașterea, identitatea. Astfel, chiar dacă în decurs de mai puțin de un an Daesh și-a pierdut atât liderul, cât și teritoriile controlate din Siria și Irak, acțiunile teroriste comise în numele organizației continuă să existe, urmare a impactului procesului propagandistic multiplicat în spaţiul online.

Mediul virtual reprezintă mai mult decât oricând principala platformă unde adepții diverselor organizații/ mișcări radicale se reunesc, interacționează, se inspiră, conspiră și se activează pentru a comite acțiuni teroriste, combaterea extremismului on line fiind și una dintre prioritățile din Fișa de țară a României.

Măsurile preventive adoptate de Serviciul Român de informaţii, în cooperare cu partenerii instituţionali din cadrul Sistemului Naţional de Prevenire şi Combatere a Terorismului au permis menţinerea nivelului actual de alertă teroristă (Albastru-Precaut).

Evoluţia ameninţărilor teroriste la adresa României au fost influenţată de:

- manifestări din spaţiile cu problematică teroristă activă;

- evoluţiile recente ale jihadului global ce au inclus teritoriul naţional pe harta ţintelor;

- percepţii punctuale privind posibilitatea comiterii cu uşurinţă a unor acţiuni teroriste în România.

România își va concentra și în continuare eforturile în vederea apărării intereselor naționale de securitate și va urmări dezvoltarea capabilităților de pregătire a autorității naționale în domeniul prevenirii și combaterii terorismului în vederea eficientizării modului de răspuns sincronizat dintre structurile cu specializări diferite care execută misiunile de intervenție antiteroristă / contrateroristă.

Astfel, Programul Național FSI al României va finanța următoarele măsuri de implementare:

1. intensificarea activităților de formare, a exercițiilor, a învățării reciproce, a programelor de schimb specializate și a schimbului de bune practici în materie de aplicare a legii, inclusiv în țările terțe și împreună cu acestea și cu alți actori relevanți;

2. exploatarea sinergiilor prin punerea în comun a resurselor și a cunoștințelor statelor membre și ale altor actori relevanți, inclusiv ale societății civile, de exemplu prin crearea unor centre de excelență comune, prin conceperea unor evaluări comune ale riscurilor sau prin crearea unor centre comune de sprijin operațional pentru operațiile desfășurate în comun;

3. promovarea și elaborarea unor măsuri, garanții, mecanisme și bune practici pentru identificarea rapidă, protejarea și sprijinirea martorilor, a denunțătorilor și a victimelor infracționalității, precum și crearea în acest scop a unor parteneriate între autoritățile publice și alți actori relevanți;

4. achiziționarea de echipamente relevante și instituirea sau modernizarea unor centre de formare specializată și a [...] infrastructurii relevante pentru securitate, în scopul îmbunătățirii gradului de pregătire, a rezilienței, a nivelului de conștientizare al publicului și a răspunsului adecvat la amenințările la adresa securității.

Acțiunile avute în vedere în cadrul PN FSI sunt, în principal, următoarele:

• sisteme și rețele TIC care contribuie la realizarea obiectivelor prezentului regulament, formarea cu privire la utilizarea acestor sisteme, testarea și îmbunătățirea interoperabilității și a calității datelor acestor sisteme;

• acțiuni care sprijină răspunsul eficace și coordonat la criză prin asigurarea unei legături între capacitățile sectoriale existente, centrele de expertiză și centrele de conștientizare cu privire la o anumită situație, inclusiv centrele pentru sănătate, protecție civilă și combaterea terorismului;

• proiecte care dezvoltă metode inovatoare sau utilizează noi tehnologii care ar putea fi transferate către alte state membre, în special proiecte care au drept obiectiv testarea și validarea rezultatelor proiectelor de cercetare în domeniul securității finanțate de Uniune;

• sprijin pentru crearea de rețele tematice sau transversale ale unităților naționale specializate în vederea îmbunătățirii încrederii reciproce, a schimbului și a diseminării de competențe și cunoștințe, de informații, de experiență și de bune practici, precum și a punerii în comun a resurselor și a expertizei în cadrul unor centre de excelență comune;

• educația și formarea personalului și a experților din cadrul autorităților de aplicare a legii, al autorităților judiciare și al agențiilor administrative relevante, ținând seama de nevoile operaționale și de analizele riscurilor, [...] în cooperare cu CEPOL și, atunci când este cazul, cu Rețeaua Europeană de Formare Judiciară;

• cooperarea cu sectorul privat cu scopul de a consolida încrederea și a îmbunătăți coordonarea, planificarea de contingență, precum și schimbul și diseminarea de informații și bune practici între actorii din sectorul public și privat, inclusiv în ceea ce privește protecția spațiilor publice și a infrastructurii critice;

• acțiuni care permit comunităților să elaboreze abordări și politici de prevenire locale, precum și acțiuni de sensibilizare și comunicare, în rândul părților interesate și al publicului larg, cu privire la politicile de securitate ale Uniunii;

• echipamente, mijloace de transport, sisteme de comunicații și facilități [...] relevante pentru securitate;

**SPRIJIN OPERAȚIONAL**: În temeiul art. 15 România va solicita sprijin operațional pentru întreținerea echipamentelor tehnice sau a mijloacelor de transport utilizate pentru acțiuni în domeniul prevenirii, al detectării și al investigării criminalității grave și organizate cu dimensiune transfrontalieră.

Beneficiari: Inspectoratul General al Poliției Române, care, în conformitate cu Legea nr. 218/2002, republicată, este instituția specializată a statului, care exercită atribuții privind apărarea drepturilor și libertăților fundamentale ale persoanei, a proprietății private și publice, prevenirea și descoperirea infracțiunilor (....).

### 

### *URMĂTOARELE SECȚIUNI VOR FI COMPLETATE ULTERIOR.*

**2.1.2 Indicators**

*Reference: Article 17(4)(e) CPR*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Table 1: Output indicators** | | | | | |
| **Specific objective** | **ID [5]** | **Indicator [255]** | **Measurement unit** | **Milestone (2024)** | **Target (2029)** |
|  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Table 2: Result indicators** | | | | | | | | | |
| **Specific objective** | **ID [5]** | **Indicator [255]** | **Measurement unit** | **Baseline or reference value** | **Reference year** | **Target (2029)** | ***[Measurement unit for target][[6]](#footnote-6)*** | **Source of data [200]** | **Comments [200]** |
|  |  |  |  |  |  |  |  |  |  |

**2.1.3 Indicative breakdown of the programme resources (EU) by type of intervention**

*Reference: Article 17(5) CPR and Article 12(15) of the BMVI Regulation or Article 12(9) ISF Regulation or Article 13(9) AMIF Regulation*

|  |  |  |  |
| --- | --- | --- | --- |
| **Table 3** | | | |
| **Specific objective** | **Type of intervention** | **Code** | **Indicative amount (Euro)** |
|  |  |  |  |

***2.1.4* Technical assistance**

*Reference: Article 17(3)(e); Article 30(5) CPR; Article 32 CPR; Article 89 CPR;*

|  |
| --- |
| *Text field [5 000] (Technical assistance pursuant to Article 30(5) CPR)* |
| *Text field [3000] (Technical assistance pursuant to Article 32 CPR)* |

|  |  |  |
| --- | --- | --- |
| **Table *4*** | | |
| **Type of intervention** | **Code** | **Indicative amount (Euro)** |
|  |  |  |

1. **Financial plan**

*Reference: Article 17(3)(f)*

**3.1. Financial appropriations by year**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Table *5*: *Financial appropriations by year*** | | | | | | | | |
| **Fund** | **2021** | **2022** | **2023** | **2024** | **2025** | **2026** | **2027** | **Total** |
|  |  |  |  |  |  |  |  |  |

**3.2 Total financial allocations**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Table *6:* *Total financial allocations by fund and national contribution*** | | | | | | | | |
| **Specific objective** | **Type of action** | **Basis for calculation EU support (total or public)** | ***~~EU~~ Union* contribution (a)** | **National contribution (b)=(c)+(d)** | **Indicative breakdown of national contribution** | | **Total**  **e=(a)+(b)** | **Co-financing rate (f)=(a)/(e)** |
| **public (c )** | **private (d)** |
| Specific objective 1 | *Actions co-financed in line with Article 11(1) of ISF or BMVI Regulation or Article 12(1) of AMIF Regulation* |  |  |  |  |  |  |  |
|  | *Actions co-financed in line with Article 11(2) of ISF or BMVI Regulation or Article 12(2) of AMIF Regulation* |  |  |  |  |  |  |  |
|  | *Actions co-financed in line with Article 11(3) of ISF or BMVI Regulation or Article 12(3) of AMIF Regulation* |  |  |  |  |  |  |  |
|  | *Actions co-financed in line with Article 11(4) of ISF or BMVI Regulation (excluding Special Transit Scheme) or Article 12(4) of AMIF Regulation* |  |  |  |  |  |  |  |
|  | *Actions co-financed in line with Article 11(4) of BMVI Regulation (Special Transit Scheme)* |  |  |  |  |  |  |  |
|  | *Actions co-financed in line with Article 11(5) of ISF or BMVI Regulation or Article 12(5) of AMIF Regulation* |  |  |  |  |  |  |  |
|  | *Actions co-financed in line with Article 16 of AMIF Regulation* |  |  |  |  |  |  |  |
|  | *Actions co-financed in line with Article 17 of AMIF Regulation* |  |  |  |  |  |  |  |
| Total for SO 1 |  |  |  |  |  |  |  |  |
| SO 2 | *Actions co-financed in line with Article 11(1) of ISF or BMVI Regulation or Article 12(1) of AMIF Regulation* |  |  |  |  |  |  |  |
|  | *Actions co-financed in line with Article 11(2) of ISF or BMVI Regulation or Article 12(2) of AMIF Regulation* |  |  |  |  |  |  |  |
|  | *Actions co-financed in line with Article 11(3) of ISF or BMVI Regulation or Article 12(3) of AMIF Regulation* |  |  |  |  |  |  |  |
|  | *Actions co-financed in line with Article 11(4) of ISF or BMVI Regulation* |  |  |  |  |  |  |  |
|  | *Actions co-financed in line with Article 11(5) of ISF or BMVI Regulation or Article 12(5) AMIF Regulation* |  |  |  |  |  |  |  |
| Total for SO 2 |  |  |  |  |  |  |  |  |
| SO 3 | *Actions co-financed in line with Article 11(1) of ISF Regulation or Article 12(1) of AMIF Regulation* |  |  |  |  |  |  |  |
|  | *Actions co-financed in line with Article 11(2) of ISF Regulation or Article 12(2) of AMIF Regulation* |  |  |  |  |  |  |  |
|  | *Actions co-financed in line with Article 11(3) of ISF Regulation or Article 12(3) of AMIF Regulation* |  |  |  |  |  |  |  |
|  | *Actions co-financed in line with Article 11(4) of ISF Regulation or Article 12(4) of AMIF Regulation* |  |  |  |  |  |  |  |
|  | *Actions co-financed in line with Article 11(5) of ISF Regulation or Article 12(5) of AMIF Regulation* |  |  |  |  |  |  |  |
| Total for SO 3 |  |  |  |  |  |  |  |  |
| TA *pursuant to Article 30(5) CPR* |  |  |  |  |  |  |  |  |
| TA *pursuant to Article 32 CPR* |  |  |  |  |  |  |  |  |
| Grand total |  |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Table 8 [AMIF only]** | **Number of persons per year** | | | | | | | |
| **Category** | **2021** | **2022** | **2023** | **2024** | **2025** | **2026** | **2027** |
| Resettlement |  |  |  |  |  |  |  |
| Humanitarian admission |  |  |  |  |  |  |  |
| [other categories] |  |  |  |  |  |  |  |

***[*Table 8 Transfers between shared management funds\**]***

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *Receiving fund / instrument*  *Transferring fund /*  *instrument* | *AMIF* | *ISF* | *BMVI* | *ERDF* | *ESF+* | *CF* | *EMFF* | *Total* |
| *AMIF* |  |  |  |  |  |  |  |  |
| *ISF* |  |  |  |  |  |  |  |  |
| *BMVI* |  |  |  |  |  |  |  |  |
| *Total* |  |  |  |  |  |  |  |  |

*\* Cumulative amounts for all transfers during programming period.*

|  |  |
| --- | --- |
| *[Table 9 Transfers to instruments under direct or indirect management\*]* | *Transfer amount* |
| *Instrument 1[name]* |  |
| *Instrument 2[name]* |  |
| *Total* |  |

*\* Cumulative amounts for all transfers during programming period*

1. **Enabling conditions**

*Reference: Article 17(3)(h)*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Table *10*** | | | | | |
| **Enabling condition** | **Fulfilment of enabling condition** | **Criteria** | **Fulfilment of criteria** | **Reference to relevant documents** | **Justification** |
|  |  | Criterion 1 | Y/N | [500] | [1000] |
|  |  | Criterion 2 |  |  |  |

1. **Programme authorities**

*Reference: Article 17(3)(j), Article 65 and 78 CPR*

|  |  |  |  |
| --- | --- | --- | --- |
| **Table *11*** | **Name of the institution** [500] | **Contact name and position** [200] | **e-mail [200]** |
| Managing authority |  |  |  |
| Audit authority |  |  |  |
| Body which receives payments from the Commission |  |  |  |

1. **Partnership**

*Reference: Article 17(3)(g) CPR;*

|  |
| --- |
| *text field [10 000]* |

1. **Communication and visibility**

*Reference: Article 17(3)(i) CPR, Article 42(2) CPR*

|  |
| --- |
| *Text field [4 500]* |

1. **Use of unit costs, lump sums, flat rates and financing not linked to costs**

*Reference: Articles 88 and 89 CPR*

|  |  |  |
| --- | --- | --- |
| *[Intended use of Articles 88 and 89][[7]](#footnote-7)* | ***YES*** | ***NO*** |
| *From the adoption programme will make use of reimbursement of the Union contribution based on unit costs, lump sums and flat rates under the priority according to Article 88 CPR (if yes, fill in Appendix 1)* | ***☐*** | ***☐*** |
| *From the adoption programme will make use of reimbursement of the Union contribution based on financing not linked to costs according to Article 89 CPR (if yes, fill in Appendix 2)* | ***☐*** | ***☐*** |

***Appendix 1:* [*Union contribution based on unit costs, lump sums and flat rates][[8]](#footnote-8)***

**Template for submitting data for the consideration of the Commission**

**(Article 88)**

|  |  |
| --- | --- |
| Date of submitting the proposal |  |
| Current version |  |

**A. Summary of the main elements**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Fund[[9]](#footnote-9)*** | ***Specific objective[[10]](#footnote-10)*** | **Estimated proportion of the total financial allocation within the priority to which the SCO will be applied in % (estimate)** | **Type(s) of operation** | | **Corresponding indicator name(s)** | | **Unit of measurement for the indicator** | **Type of SCO (standard scale of unit costs, lump sums or flat rates)** | **Corresponding standard scales of unit costs, lump sums or flat rates** |
|  |  |  | Code | Description | Code | Description |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |

**B. Details by type of operation (to be completed for every type of operation)**

**Did the managing authority receive support from an external company to set out the simplified costs below?**

**If so, please specify which external company: Yes/No – Name of external company**

Types of operation:

|  |  |
| --- | --- |
| 1.1. Description of the operation type |  |
| 1.2 *]*specific objective*~~)~~[[11]](#footnote-11)* |  |
| 1.3 Indicator name[[12]](#footnote-12) |  |
| 1.4 Unit of measurement for indicator |  |
| 1.5 Standard scale of unit cost, lump sum or flat rate |  |
| 1.6 Amount |  |
| 1.7 Categories of costs covered by unit cost, lump sum or flat rate |  |
| 1.8 Do these categories of costs cover all eligible expenditure for the operation? (Y/N) |  |
| 1.9 Adjustment(s) method |  |
| 11.10 Verification of the achievement of the unit of measurement  - describe what document(s) will be used to verify the achievement of the unit of measurement  - describe what will be checked during management verifications (including on-the-spot), and by whom  - describe what arrangements there are to collect and store the data/documents described |  |
| 1.11 Possible perverse incentives or problems caused by this indicator, how they could be mitigated, and the estimated level of risk |  |
| 1.12 Total amount (national and EU) expected to be reimbursed |  |

**C: Calculation of the standard scale of unit costs, lump sums or flat rates*\****

*1.* Source of data used to calculate the standard scale of unit costs, lump sums or flat rates (who produced, collected and recorded the data; where the data are stored; cut-off dates; validation, etc.).

*2.* Please specify why the proposed method and calculation is relevant to the type of operation:

*3.* Please specify how the calculations were made, in particular including any assumptions made in terms of quality or quantities. Where relevant, statistical evidence and benchmarks should be used and attached to this annex in a format that is usable by the Commission.

*4*. Please explain how you have ensured that only eligible expenditure was included in the calculation of the standard scale of unit cost, lump sum or flat rate.

*5*. Assessment of the audit authority(ies) of the calculation methodology and amounts and the arrangements to ensure the verification, quality, collection and storage of data.

*\* Justifications on the underlying data, the calculation methodology and resulting rate or amount and related assessment by the audit authority [(in points 1, 3 and 5)] are not required when the simplified cost options submitted in this Appendix are established at Union level [(other policies or through the DA referred to in Article 88(4)].*

***Appendix 2:* *[Union contribution based on financing not linked to costs][[13]](#footnote-13)***

**Template for submitting data for the consideration of the Commission**

**(Article 89)**

|  |  |
| --- | --- |
| Date of submitting the proposal |  |
| Current version |  |

**A. Summary of the main elements**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Fund[[14]](#footnote-14)*** | ***Specific objective[[15]](#footnote-15)*** | ***The amount covered by the financing not linked to costs*** | **Type(s) of operation** | **Conditions to be fulfilled/results to be achieved** | **Corresponding indicator name(s)** | | **Unit of measurement for the indicator** | ***[Envisaged reimbursement to the beneficiaries][[16]](#footnote-16)*** |
|  |  |  |  |  | Code | Description |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
| The overall amount covered |  |  |  |  |  |  |  |  |

**B. Details by type of operation (to be completed for every type of operation)**

Types of operation:

|  |  |  |  |
| --- | --- | --- | --- |
| 1.1. Description of the operation type |  | | |
| 1.2 *S*pecific objective*[[17]](#footnote-17)* |  | | |
| 1.3 Conditions to be fulfilled or results to be achieved |  | | |
| 1.4 Deadline for fulfilment of conditions or results to be achieved |  | | |
| 1.5 Indicator definition for deliverables |  | | |
| 1.6 Unit of measurement for indicator for deliverables |  | | |
| 1.7 Intermediate deliverables (if applicable) triggering reimbursement by the Commission with schedule for reimbursements | Intermediate deliverables | Date | Amounts |
|  |  |  |
|  |  |  |
| 1.8 Total amount (including EU and national funding) |  | | |
| 1.9 Adjustment(s) method |  | | |
| 1.10 Verification of the achievement of the result or condition (and where relevant, the intermediate deliverables)  - what document(s) will be used to verify the achievement of the result or condition?  - describe what will be checked during management verifications (including on-the-spot), and by whom.  - what arrangements to collect and store the data/documents described? |  | | |
| 1.10a *Does the grant provided by Member State to beneficiaries take the form of financing not linked to costs? [Y/N][[18]](#footnote-18)* |  | | |
| 1.11 Arrangements to ensure the audit trail  Please list the body(ies) responsible for these arrangements. |  | | |

*[Appendix 3: Thematic Facility][[19]](#footnote-19)*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *Procedure reference / Specific objective* | *Modality: Specific action/ emergency assistance/ resettlement/ support to Member States contributing to solidarity* | *Type of intervention* | | *EU contribution (EUR)* |
| *<type='N' input='M'>* | *<type='S’ input='S'>* | *<type='S’ input='S'>* | | *<type='N' input='M'>* |
| *Description of the action* | *[text]* | | | |
| *Member State submits a thematic facility amendment /declines* | | | *Date: <type='N' input='M'>*  *Submit/Decline: <type='S’ input='S'>* | |
| *Comment  (if Member State declines or if indicators targets and millstones are not updated a justification should be encoded; tables 3, 5 and 6 should be revised)* | | | *[text]* | |

1. *Without prejudice to further alignment in relation to the outcome of interinstitutional negotiations on the articles of the CPR and the fund-specific regulations.* [↑](#footnote-ref-1)
2. Number in square brackets refer to number of characters *without spaces.* [↑](#footnote-ref-2)
3. *Some modifications are due to the aligment with Fund-specific Regulations (eg. change of numbering in the Fund-specific regulations after the adoption of the CPR proposal).* [↑](#footnote-ref-3)
4. *Some modifications are due to the aligment with Fund-specific Regulations (eg. change of numbering in the Fund-specific regulations after the adoption of the CPR proposal).* [↑](#footnote-ref-4)
5. *Some modifications are due to the aligment with Fund-specific Regulations (eg. change of numbering in the Fund-specific regulations after the adoption of the CPR proposal).* [↑](#footnote-ref-5)
6. *The Council’s partial mandate added this column.* [↑](#footnote-ref-6)
7. *The Council’s partial mandate replaced the table with a different one, in the same manner as in the Annex V.* [↑](#footnote-ref-7)
8. *The Council’s partial mandate changed the title of the appendix, linked to block 6.* [↑](#footnote-ref-8)
9. *Alignment with COM proposal for Annex VI* [↑](#footnote-ref-9)
10. *Alignment with COM proposal for Annex VI* [↑](#footnote-ref-10)
11. *The Council’s partial mandate deleted the text in [].* [↑](#footnote-ref-11)
12. Several complementary *common* indicators (for instance one output indicator and one result indicator) are possible for one type of operation. In these cases, fields 1.3 to 1.11 should be filled in for each indicator. [↑](#footnote-ref-12)
13. *The Council’s partial mandate amended the title, linked to block 6.* [↑](#footnote-ref-13)
14. *Alignment with COM proposal for Annex VI* [↑](#footnote-ref-14)
15. *Alignment with COM proposal for Annex VI* [↑](#footnote-ref-15)
16. *The Council partial mandate added this column.* [↑](#footnote-ref-16)
17. *Alignment to Annex VI* [↑](#footnote-ref-17)
18. *The Council’s partial mandate added point 1.10a, which COM is proposing to amend in order to improve clarity.* [↑](#footnote-ref-18)
19. *Pending agreed approach to the thematic facility under Fund-specific Regulations* [↑](#footnote-ref-19)