ACORD BILATERAL

ДВУСТОРОННЕЕ СОГЛАШЕНИЕ

MEMORANDUMUL DE ÎNŢELEGERE
între Republica Moldova şi Oficiul European de Poliţie
privind linia securizată de comunicare

din 16.01.2014

Monitorul Oficial nr.27-34/120 din 07.02.2014

* * *

Republica Moldova

Reprezentată în scopul prezentului Memorandum de Înţelegere de către Domnul Dorin Recean, Ministru al Afacerilor Interne al Republicii Moldova, denumită în continuare "Moldova",

şi

Oficiul European de Poliţie

Reprezentat în scopul prezentului Memorandum de Înţelegere de către Domnul Eugenio Orlandi, Director Adjunct, denumit în continuare "Europol",

Denumite colectiv drept "Părţi" sau individual "Parte",

Avînd la bază Acordul strategic de Cooperare între Republica Moldova şi Europol semnat la 12 februarie 2007 (denumit în continuare "Acord"),

Prin care Părţile conştientizează că schimbul de informaţie în baza Acordului necesită crearea unei linii securizate de comunicare între ele,

Au convenit asupra următoarelor:

Articolul 1
Scopul şi domeniul de aplicare

1. Scopul prezentului Memorandum de Înţelegere este de a reglementa crearea, implementarea, operarea, înlocuirea şi demontarea liniei securizate de comunicare prin care se va realiza schimbul de informaţie.

2. Schimbul de informaţie între Părţi va fi realizat numai în conformitate cu cadrul legal existent al Părţilor şi prevederile relevante ale Acordului.

3. Schimbul de informaţii atribuite la secretul de stat prin intermediul liniei securizate de comunicare este limitat la nivelul RESTREINT UE/EU RESTRICTED şi echivalentul acestuia în Moldova.

Articolul 2
Definiţii

În scopul prezentului Memorandum de Înţelegere:

a) "Punct de demarcaţie" înseamnă interfaţa dintre reţeaua de operaţiuni Europol şi reţeaua din Moldova, prin care controlul operaţional şi dreptul de proprietate asupra echipamentului de comunicare este transmisă unei alte Părţi de către cealaltă;

b) "Reţea de operaţiuni Europol" (OPS NET) înseamnă reţeaua Tehnologii Informaţionale şi de Comunicaţii (TIC) utilizată în scopuri operaţionale, destinată în scopul procesării informaţiilor privind criminalitatea, inclusiv date cu caracter personal, în cadrul sistemelor Europol de procesare a informaţiei în conformitate cu cadrul legal al Europol;

c) "Nivel minim de securitate" înseamnă cerinţe minime de securitate aplicate sistemelor interconectate ale ambelor Părţi.

Articolul 3
Puncte de contact

Fiecare Parte va desemna un punct de contact pentru orice subiect legat de implementarea tehnică a prezentului Memorandum de Înţelegere.

Articolul 4
Codul de Conectare

1. Părţile se angajează să implementeze controale minime de securitate stabilite în Anexa "Codul de Conectare al Reţelei de operaţiuni Europol" la prezentul Memorandum de Înţelegere (denumită în continuare "Anexă"). Fiecare Parte va proteja sistemul său interconectat în conformitate cu nivelul minim de securitate prin intermediul controalelor procedurale, tehnice şi fizice stabilite în Anexă.

2. Prin semnarea prezentului Memorandum de Înţelegere, Moldova confirmă Declaraţia de Conformitate cu Codul de Conectare prevăzut în Partea D la Anexă.

3. În cazul în care Părţile fac o interconectare ulterioară la altă reţea, o astfel de conectare va fi condiţionată de încheierea unui acord privind respectarea principiilor şi a cerinţelor echivalente cu cele stabilite în prezentul Cod de Conectare.

4. O Parte nu va interfera cu echipamentul TIC al celeilalte Părţi, inclusiv (de)conectarea cablurilor sau echipamentului, doar în cazul unei instrucţiuni speciale în scris a celeilalte Părţi sau în caz de urgenţă.

5. În cazul unui incident de securitate iminent, în special cele menţionate în Partea C a Anexei, Partea vizată va informa cealaltă Parte fără întîrziere şi va întreprinde toate măsurile necesare în vederea protejării confidenţialităţii şi integrităţii informaţiei schimbate, de asemenea, se va face deconectarea de la sistemul celeilalte Părţi în scopul prevenirii răspîndirii eventualei infectări.

6. Înainte de a opera careva modificări ale interconectărilor sau sistemelor cu impact asupra reţelei unei Părţi, se va expedia anticipat informaţie relevantă şi suficientă, în formă scrisă, la punctul de contact al celeilalte Părţi. În cazul necesităţii unei întrevederi pentru a discuta subiectul modificărilor, aceasta trebuie organizată înaintea începerii implementării acestora.

Articolul 5
Dispoziţii generale şi obligaţii

1. Părţile vor utiliza sistemele interconectate numai în scopul Acordului şi în conformitate cu prevederile prezentului Memorandum de Înţelegere.

2. Fiecare Parte va fi responsabilă de securitatea propriilor sisteme, începând cu punctul de demarcaţie.

3. Părţile nu vor efectua nici un tip de teste, scanări de vulnerabilitate sau tentative de intruziuni în sistemul celeilalte Părţi fără autorizaţia prealabilă scrisă a celeilalte Părţi.

4. Fără a aduce atingere Articolului 4 (5), Părţile vor face schimb de informaţii referitoare la ameninţările şi vulnerabilităţile care pot interfera cu sistemele unei alteia.

5. Toate echipamentele utilizate pentru a stabili linia de comunicare pînă la punctul de demarcaţie al Reţelei de operaţiuni Europol, vor fi furnizate de către şi vor rămâne în proprietatea Europol.

6. Echipamentul Europol instalat la sediul din Moldova va rămâne în proprietatea Europol. Echipamentul propriu al Moldovei instalat la sediul Europol va rămâne în proprietatea Republicii Moldova. Proprietarul echipamentului va fi responsabil pentru securitatea acestuia, cu excepţia cazului în care s-a convenit altfel în scris de către Părţi.

7. Fiecare Parte va fi responsabilă de instalarea, întreţinerea, înlocuirea şi defectarea propriului echipament. Cererile de sprijin pot fi făcute de către administratorii de sistem ale reţelei respective a fiecărei Părţi, în scopul de a facilita soluţionarea problemelor de suport şi

întreţinere. O procedură pentru gestionarea unor astfel de cereri poate fi convenită în scris de către Părţi.

8. Europol este responsabil pentru crearea, întreţinerea şi, dacă este necesar, pentru înlocuirea liniei de comunicaţii securizate. Moldova, în conformitate cu procedurile aplicabile, va oferi acces personalului desemnat de către Europol, pentru astfel de întreţineri sau înlocuiri ale echipamentelor defecte, în zonele relevante ale sediului său. În cazul în care o defecţiune este detectată de către Moldova, personalul desemnat de Europol va fi prima linie de asistenţă tehnică.

9. Linia securizată de comunicare va fi demontată la încetarea prezentului Memorandum de Înţelegere. Europol va fi responsabil pentru demontarea liniei securizate de comunicare şi a echipamentelor sale proprii instalate la sediul din Moldova. O Parte, în conformitate cu procedurile aplicabile, va oferi acces pentru orice membru al personalului desemnat de către cealaltă Parte pentru demontarea liniei securizate de comunicare şi propriului echipament.

10. Părţile vor transfera reciproc echipamentul respectiv. În acest scop, aranjamentele practice vor fi convenite în scris de către Părţi.

Articolul 6
Distribuirea cheltuielilor

1. În conformitate cu regulile aplicabile privind achiziţionarea, Europol va procura toate bunurile şi serviciile necesare pentru crearea, implementarea, operarea, înlocuirea şi demontarea liniei securizate de comunicare.

2. Cheltuielile pentru crearea şi înlocuirea liniei securizate de comunicare vor fi suportate de către Europol.

3. Cheltuielile lunare pentru exploatarea liniei securizate de comunicare vor fi partajate între Părţi, fiecare acoperind 50% din cost. Europol va achita în avans toate cheltuielile lunare necesare pentru exploatare. Moldova va rambursa 50% din costurile lunare de exploatare după emiterea de către Europol a unui ordin de recuperare a cheltuielilor în conformitate cu Regulamentul Financiar al Europol.

4. În cazul în care oricare dintre Părţi decide relocarea liniei securizate de comunicare, costurile de relocare vor fi suportate de către Partea respectivă.

5. Costurile pentru demontarea liniei securizate de comunicare în conformitate cu articolul 5(9) vor fi suportate de către Europol. Fiecare Parte va suporta costurile pentru demontarea şi transferul de echipament propriu, în conformitate cu articolul 5 (10).

Articolul 7
Răspunderea şi soluţionarea litigiilor

1. Fără a aduce atingere Articolului 14 al Acordului, o Parte va fi responsabilă de orice prejudiciu cauzat celeilalte Părţi în urma creării, implementării, operării, înlocuirii şi demontării liniei securizate de comunicare. În astfel de cazuri, Părţile vor găsi o soluţie echitabilă pentru compensarea oricărui prejudiciu cauzat.

2. Costurile apărute în procesul de apărare a unei acţiuni, cereri sau proceduri în instanţă a unei părţi terţe şi compensaţia plătită de către o Parte unei părţi terţe pentru orice prejudiciu în legătură cu acest Memorandum de Înţelegere vor fi rambursate, la cerere, de către cealaltă Parte, în cazul în care acestea au fost cauzate de o acţiune sau inacţiune intenţionată sau din neglijenţă din partea celeilalte Părţi. Părţile îşi vor acorda asistenţă reciprocă şi vor depune eforturi pentru a găsi o soluţie echitabilă pentru rambursare.

3. Orice litigiu între Părţi privind interpretarea sau aplicarea prezentului Memorandum de Înţelegere va fi soluţionat în conformitate cu prevederile Articolului 15 al Acordului.

Articolul 8
Amendamente

Amendamentele la prezentul Memorandum de Înţelegere vor fi convenite de comun prin schimbul de note între Părţi.

Articolul 9
Suspendarea

În cazul în care o Parte se abate semnificativ de la prevederile prezentului Memorandum de Înţelegere, linia securizată de comunicare sau serviciile specifice între cele două reţele pot fi suspendate în mod unilateral de către cealaltă Parte printr-o notificare scrisă, pînă cînd problemele sunt rezolvate.

Articolul 10
Încetarea

1. Memorandumul de Înţelegere poate fi denunţat, printr-o notificare scrisă cu trei luni înainte, de către fiecare Parte.

2. Fără a aduce atingere alineatului 1, efectele juridice ale acestui Memorandum de Înţelegere vor rămîne în vigoare.

Articolul 11
Intrarea în vigoare şi semnăturile

1. Memorandumul de Înţelegere este încheiat pe o perioadă nedeterminată şi va intra în vigoare în ziua semnării de către ultima Parte.

2. Memorandumul de Înţelegere este încheiat în limbile română şi engleză. În cazul divergenţelor de interpretare, varianta engleză va prevala.

Semnat la Haga, la 16 ianuarie 2014, în două exemplare.

Pentru Republica Moldova	**Pentru Europol**
Domnul Dorin Recean	**Domnul Eugenio Orlandi**
Ministru al Afacerilor Interne	**Director Adjunct**
_____	_____

Anexa: Codul de Conectare a Reţelei de Operaţiuni Europol

1.1. **Partea A: Introducere**

Scopul principal al prezentului Cod de Conectare este de a asigura ca Reţeaua de operaţiuni Europol şi reţelele externe, care sunt interconectate la aceasta, să fie protejate împotriva ameninţărilor la adresa confidenţialităţii, integrităţii şi disponibilităţii. Este conştientizat faptul că un accident de securitate în Reţeaua de operaţiuni Europol sau în oricare dintre reţelele interconectate ar putea afecta toate celelalte reţele interconectate.

Principiul de bază al prezentului Cod de Conectare este că toate reţelele interconectate la Reţeaua de operaţiuni Europol trebuie să implementeze un set minim de control de securitate. Acest nivel minim de securitate are drept scop reducerea riscului incidentelor de securitate, care apar oriunde în sistemul interconectat, şi care au influenţă asupra securităţii întregii reţele la un nivel acceptat de către Autoritatea de Acreditare a Securităţii. Fiecare Parte este responsabilă de securitatea sistemului propriu începînd cu punctul de demarcare.

Codul de Conectare este obligatoriu pentru Părţi. Conceptele, principiile, controalele şi obligaţiile menţionate în el trebuie respectate şi realizate.

1.2. **Partea B: Minimul control al securităţii**

1.2.1. **Cerinţe de securitate specifice sistemului Reţelei Europol de Operaţiuni**

Europol prezintă o listă de cerinţe de securitate a infrastructurii reţelei sub forma unui document întitulat “Cerinţe de securitate specifice sistemului Reţelei de operaţiuni Europol

(SSSR)[1]. SSSR este o declaraţie completă şi explicită a principiilor de securitate, care trebuie respectate şi a cerinţelor detaliate de securitate pe care un sistem trebuie să le îndeplinească. Acesta are la bază principii-cheie ale securităţii stabilite de Manualul de Securitate Europol şi rezultatul evaluării riscului.

[1] Dosarul nr.2440-72

SSSR a fost adoptată de către Consiliul de Conducere la recomandarea Comitetului de Securitate Europol. Prezentul document este subiectul unei revizuiri şi actualizări periodice în contextul reacreditării sistemului.

O cerinţă obligatorie pentru interconectarea unei reţele externe la Reţeaua de operaţiuni Europol este că Moldova şi Europol vor implementa politici, proceduri şi măsuri tehnice, care sunt comparabile cu cele menţionate în SSSR. Aceasta nu înseamnă că procedurile actuale sau aspectele tehnice sunt aceleaşi, dar este important ca conceptele menţionate în cadrul SSSR să fie abordate în conformitate cu politicile şi directivele naţionale. Acest lucru este în conformitate cu Articolul 2 al Deciziei Consiliului 2009/968/JHA din 30 noiembrie 2009 "Cu privire la adoptarea normelor privind confidenţialitatea informaţiei Europol"[2], în care stabileşte că toată informaţia care este procesată de către sau prin intermediul Europol va avea un nivel de protecţie, care este echivalent cu nivelul de protecţie acordat unei astfel de informaţii de către Europol.

[2] Decizia Consiliului 2009/968/JAI din 30 noiembrie 2009

1.2.2. **Măsuri de bază**

SSSR va fi utilizată drept ghid pentru a defini nivelul minim de securitate pentru orice sistem interconectat. În principiu, Părţile care se conectează pot alege cum să implementeze măsurile care sunt compatibile politicilor de securitate şi reglementărilor locale de abordare a ameninţărilor şi conceptelor menţionate în SSSR. Cu toate acestea, în scopul garantării nivelului minim de asigurare a securităţii, măsurile de control enumerate mai jos vor servi drept bază şi condiţia unei interconectări de reţea.

1.2.2.1. **Controale procedurale**

Moldova trebuie să utilizeze minimum de controale procedurale după cum urmează:

• Utilizatorii sistemului trebuie să fie în posesia unui document (certificat de securitate) care atestă dreptul de acces la informaţia atribuită la secret de stat la nivel naţional corespunzător.

• O politică de autentificare, ceea ce înseamnă principii de bază pentru crearea şi gestionarea parolei, trebuie să fie aplicată.

• Trebuie realizate măsuri de audit şi evidenţă pentru conectare la sistem.

• Informaţia privind incidentele de securitate, care ar putea afecta securitatea reţelei Europol sau oricăror alte reţele interconectate (ex. focar de viruşi), vor fi raportate fără întîrziere în conformitate cu art.4 (5) al prezentului Memorandum de Înţelegere. O listă indicativă a acestor incidente de securitate este inclusă în Partea C a prezentei Anexe.

1.2.2.2. **Controale tehnice**

Moldova trebuie să folosească următoarele controale tehnice configurate:

• Limita (perimetrul) dispozitivelor de securitate aşa ca paravanuri de protecţie sau rutere de evaluare.

• Tehnologii anti malware.

• Nici o staţie de lucru, conectată direct la o reţea de calculatoare publice, cum ar fi internetul, să nu fie conectată la Reţeaua de operaţiuni Europol sau să nu fie folosită pentru accesarea Reţelei de operaţiuni Europol.

• Sistemele care sunt conectate indirect la reţeaua publică, cum ar fi internetul, să fie protejate corespunzător pentru a putea proteja Reţeaua de operaţiuni Europol de o astfel de reţea publică.

• Criptarea de trafic în timpul utilizării liniilor publice de comunicare, cum ar fi tehnologia de criptare, trebuie să aibă o putere corespunzătoare pentru clasificarea datelor, care urmează a fi protejate.

• Testele şi evaluările privind securitatea informaţiei trebuie realizate pentru a asigura că vulnerabilitatea este identificată şi remediată.

• Sistemele de conectare vor fi supuse unui regim de Acreditare (sau echivalentul acestuia).

1.2.2.3. **Controlul fizic**

Sistemele de conectare vor include următoarele controale fizice:

• Sistemul de conectare va fi amplasat corespunzător într-o locaţie securizată.

• Echipament sensibil, cum ar fi consolele, echipamentul de tip server, paravanuri de protecţie, comutatoare de reţea şi dispozitive de criptare trebuie să includă controlul accesului fizic (ex: să fie amplasat într-o încăpere încuiată).

• Accesul la staţii de lucru, terminale etc., unde este posibil accesul la Reţeaua de operaţiuni Europol, trebuie fizic restricţionat. În cazul în care staţiile de lucru trebuie să fie situate într-o zonă accesibilă publicului, din motive organizatorice sau operaţionale, astfel de echipament trebuie protejat fizic permanent pentru a împiedica accesul neautorizat, furtul sau pierderea acestuia. De exemplu, astfel de echipament nu trebuie lăsat nesupravegheat în locurile publice.

• Tot echipamentul instalat de către Europol în scopul asigurării interconectării reţelei va fi amplasat într-un suport de 19inch, care este proprietate Europol. Dimensiunile suportului sunt: înălţimea 2245h x lăţimea 640 x adîncimea 1395 mm şi are o greutate de 245 kg. Partea care se interconectează va asigura spaţiul necesar în camera de calculatoare pentru a amplasa acest suport.

1.3. **Partea C: Exemple de incidente de securitate**

Următoarele incidente constituie incidente de securitate grave prevăzute în art.4 (5) al prezentului Memorandum de Înţelegere şi trebuie tratate în conformitate cu dispoziţia menţionată.

• Pană de curent extinsă ce face linia indisponibilă.

• Propagare sporită a viruşilor în reţea sau alte incidente malware.

• Pierderea sau furtul de echipament care conţine informaţii Europol sau poate conţine informaţii care ar putea duce la accesul neautorizat la Reţeaua de operaţiuni Europol.

• Acces neautorizat în spaţiile securizate în care este amplasat echipamentul Părţilor.

• Acţiuni rău intenţionate de către utilizatori interni care ar putea duce la scurgerea sau falsificarea informaţiei Europol.

• Modificări neautorizate ale configurării dispozitivelor de protecţie ce ar duce la expunerea critică a liniei de comunicare.

• Orice alt incident în care există o ameninţare potenţială sau actuală pentru informaţia Europol.

1.4. **Partea D: Declaraţie de conformitate a Codului de Conectare**

• Utilizatorii sistemului trebuie să fie în posesia unui document (certificat de securitate) care atestă dreptul de acces la informaţia atribuită la secret de stat la nivel naţional corespunzător.

• O politică de autentificare, ceea ce înseamnă principii de bază pentru crearea şi gestionarea parolei, este în vigoare şi implementată.

• O politică pentru orice acces de la distanţă şi măsuri de autentificare corespunzătoare sistemului de conectare, este în vigoare şi în proces de implementare.

• Măsurile de evidenţă şi audit pentru sistemele de conectare sunt în vigoare şi implementate.

• Informaţia privind incidentele de securitate, care au potenţial să afecteze reţeaua de securitate Europol sau alte reţele interconectate (ex. infecţie cu virus) este raportată fără întîrziere în conformitate cu art.4 (5) al prezentului Memorandum de Înţelegere.

• Limita dispozitivelor de securitate ce ar fi paravanuri de protecţie sau rutere de evaluare sunt implementate.

• Tehnologiile antimalware sunt implementate.

• Nici o staţie de lucru, conectată direct la o reţea de calculatoare publice, cum ar fi Internetul, este conectată la Reţeaua de operaţiuni Europol sau este folosită pentru accesarea Reţelei de operaţiuni Europol.

• Sistemele care sunt conectate indirect la o reţea publică, cum ar fi Internetul, sunt protejate corespunzător în scopul apărării Reţelei de operaţiuni Europol de o astfel de reţea publică.

• Criptarea de trafic în timpul utilizării liniilor publice de comunicare, cum ar fi tehnologia de criptare, trebuie să aibă o putere corespunzătoare pentru clasificarea datelor, care urmează a fi protejate.

• Evaluările şi verificările securităţii informaţiei sunt realizate în scopul asigurării identificării şi remedierii vulnerabilităţilor.

• Sistemele de conectare sunt supuse unui regim de Acreditare (sau la un regim echivalent).

• Sistemele de conectare sunt amplasate corespunzător într-o încăpere securizată.

• Echipament sensibil cum ar fi consolele, echipamentul de server, paravanuri de protecţie, comutatoare de reţea şi dispozitiv de incriptare trebuie să includă controlul accesului fizic (de ex: să fie amplasat într-o încăpere încuiată).

• Accesul la staţii de lucru, terminale etc., unde există posibilitatea accesului la Reţeaua Europol, trebuie fizic restricţionat. În cazul în care staţiile de lucru trebuie să fie situate într-o zonă accesibilă publicului, din motive organizatorice sau operaţionale, este necesar ca un astfel de echipament să fie protejat fizic permanent pentru a împiedica accesul neautorizat, furtul sau pierderea.