

**Acord
între
Guvernul României
și
Guvernul Republicii Macedonia de Nord
privind consolidarea cooperării în domeniul controlului intern și al prevenirii și
combaterii corupției**

Guvernul României și Guvernul Republicii Macedonia de Nord, denumite în continuare „Părți”,

Ghidate de dorința de încurajare în continuare a cooperării bilaterale în domeniul afacerilor interne, în special în domeniul controlului intern și al prevenirii și combaterii corupției,

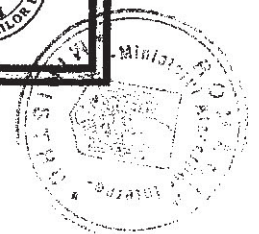
Acționând în interesul securității propriilor cetățeni și vizând respectarea drepturilor și libertăților acestora,

Luând în considerare principiile dreptului internațional și legislația națională a ambelor state,

Au convenit următoarele:

**Articolul 1
Domenii și obiective ale cooperării**

- (1) Părțile vor coopera și vor asigura asistență în întărirea cooperării în domeniul controlului intern și al prevenirii și combaterii corupției în baza prezentului Acord și în conformitate cu legislația națională a statelor Părților.
- (2) Cooperarea va fi orientată în special pe combaterea corupției în rândul polițiștilor și al altor angajați ai autorităților competente ale Părților, cu accent pe combaterea implicării acestora în activități de crimă organizată, trafic de ființe umane și migrație ilegală, trafic de migranți, trafic de țigări sau alte produse; producție ilicită, transport și trafic de substanțe stupefiante și substanțe psihotrope și precursori și, de asemenea, pe respectarea drepturilor și libertăților omului, în conformitate cu legislația națională a statelor Părților.
- (3) În ceea ce privește controlul intern, în baza prezentului Acord, activitățile principale ce pot fi derulate în comun vizează în special stabilirea obiectivelor și indicatorilor de performanță, planificarea, organizarea și procedurarea activităților, managementul riscurilor, identificarea funcțiilor sensibile, precum și monitorizarea și evaluarea performanțelor.



Articolul 2 Forme ale cooperării

- (1) Cooperarea între autoritățile competente ale Părților, stabilită în conformitate cu articolul 3 al prezentului Acord va cuprinde următoarele:
 - a) schimburi de experiență;
 - b) implementarea de proiecte în comun;
 - c) activități operaționale comune;
 - d) pregătire comună.
- (2) Autoritățile competente în domeniul afacerilor interne ale altor State Membre ale Uniunii Europene, statelor în proces de aderare la Uniunea Europeană sau statelor cu statut de candidat la Uniunea Europeană se pot alătura cooperării dintre cele două Părți atunci când primesc o invitație în acest sens. Invitațiile pot fi transmise către autoritățile competente anterior menționate, doar în măsura în care ambele Părți își exprimă în scris acordul în acest sens.
- (3) În vederea îndeplinirii obiectivelor prezentului Acord, Părțile vor elabora un Plan de acțiuni comun cu măsuri concrete pentru cooperare în domeniul de referință.
- (4) Părțile vor evalua și, dacă este necesar, vor conveni extinderea cooperării, în cadrul unei întâlniri la nivelul miniștrilor de resort și al experților.

Articolul 3 Autorități competente

Părțile, pentru implementarea prevederilor prezentului Acord, vor desemna următoarele autorități competente:

(a) Pentru România:

Ministerul Afacerilor Interne, prin:

- Corpul de Control al Ministrului;
- Direcția Generală Anticorupție;
- Direcția Generală de Protecție Internă.

(b) Pentru Republica Macedonia de Nord:

Ministerul Afacerilor Interne, prin:

- Departamentul pentru Control Intern, Investigații Criminale și Standarde Profesionale;
- Biroul pentru Securitate Publică – Departamentul de Combatere a Criminalității Organizate și Grave;
- Biroul pentru Securitate Publică – Departamentul de Poliție Criminală.



Articolul 4

Protecția datelor. Limitarea Scopului și a utilizării

- (1) Schimbul de informații între Părți va avea loc numai în scopul și în conformitate cu dispozițiile prezentului Acord. Transmiterea datelor cu caracter personal de către Părți trebuie să fie necesară, în cazuri individuale, în scopul menționat la Articolul 1 din prezentul Acord.
- (2) Informațiile transmise pot fi utilizate numai în scopul pentru care au fost transmise inițial, iar Părțile se angajează să respecte orice restricție în ceea ce privește utilizarea, ștergerea sau distrugerea, inclusiv posibile restricții de acces general sau în condiții specifice. Părțile se asigură că datele cu caracter personal prelucrate sunt relevante și nu sunt excesive sau incompatibile prin raportare la scopul prelucrării.
- (3) Utilizarea informațiilor într-un alt scop decât scopul pentru care acestea au fost transmise inițial trebuie să fie autorizată de către Partea care le transmite.
- (4) Părțile se asigură că vor furniza reciproc numai informațiile colectate, stocate și transmise în conformitate cu legislația națională și care au fost obținute cu respectarea dispozițiilor în materia drepturilor omului și a libertăților fundamentale.
- (5) Transmiterea către terți a informațiilor primite se limitează la autoritățile responsabile cu prevenirea și combaterea infracțiunilor și trebuie să aibă loc în aceleași condiții ca și cele care se aplică comunicării inițiale. Orice altă transmitere ulterioară, inclusiv către state terțe sau organizații internaționale trebuie să fie consimțită de către Partea care transmite.
- (6) Datele cu caracter personal nu vor fi transferate atunci când Partea solicitantă ar urma să le folosească pentru a solicita, a pronunța sau a executa pedeapsa cu moartea sau orice alt tratament crud, inuman sau degradant.

Articolul 5

Transmiterea de date cu caracter personal

- (1) Cererile Părților referitoare la datele cu caracter personal trebuie să fie însoțite de o precizare detaliată a scopului și a motivului solicitării.
- (2) În absența unei precizări, potrivit alineatului (1) al prezentului articol, Părțile nu pot să transmită date cu caracter personal.
- (3) Părțile vor indica în momentul transmiterii datelor cu caracter personal sau anterior, scopul pentru care au fost transmise datele și orice restricție privind utilizarea, ștergerea sau distrugerea acestora, inclusiv posibile restricții referitoare la acces, în general sau în condiții specifice. În cazul în care necesitatea unor astfel de restricții devine evidentă după primire, Părțile se informează ulterior, reciproc cu privire la astfel de restricții.
- (4) Părțile stabilesc fără întârziere, în termen de cel mult șase luni de la primirea datelor cu caracter personal, dacă și în ce măsură datele cu caracter personal sunt necesare în scopul pentru care au fost furnizate și informează Partea care transmite. Datele cu caracter personal trebuie să fie șterse în cazul în care acestea nu mai sunt necesare în scopul pentru care au fost transmise.



- (5) Prelucrarea datelor cu caracter personal care dezvăluie originea rasială sau etnică, opiniile politice, confesiunea religioasă sau convingerile filozofice, afilierea sindicală, prelucrarea datelor genetice, prelucrarea datelor biometrice pentru identificarea unică a unei persoane fizice sau prelucrarea datelor privind sănătatea sau a datelor privind viața sexuală și orientarea sexuală a unei persoane fizice este interzisă și se poate realiza, în cazuri excepționale, doar dacă:
- (a) este strict necesară într-un caz determinat;
 - (b) sunt instituite garanții adecvate pentru drepturile și libertățile persoanei vizate;
 - (c) este îndeplinită una dintre următoarele condiții:
 - (i) prelucrarea este prevăzută expres de lege;
 - (ii) prelucrarea este necesară pentru a proteja interesele vitale ale persoanei vizate sau ale unei alte persoane fizice;
 - (iii) prelucrarea se referă la date care sunt făcute publice în mod manifest de persoana vizată.
- (6) Părțile trebuie să implementeze metode eficiente pentru a demonstra legalitatea prelucrării datelor cu caracter personal și trebuie să țină o evidență a tuturor comunicărilor de date cu caracter personal și a motivelor care stau la baza acestor comunicări.

Articolul 6

Stocarea, revizuirea, rectificarea și ștergerea datelor cu caracter personal

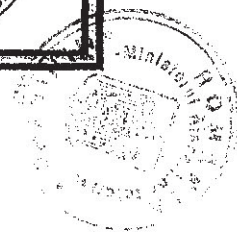
- (1) Părțile stochează datele personale pe perioada strict necesară îndeplinirii scopului în care au fost transmise. Necesitatea continuării stocării trebuie să fie revizuită în termen de cel mult trei ani de la transmitere. În timpul examinării, Părțile pot decide cu privire la continuarea stocării datelor, până la următoarea revizuire, care va avea loc după o altă perioadă de trei ani, numai dacă este încă necesară pentru îndeplinirea sarcinilor sale. În cazul în care nu se ia nicio decizie privind continuarea stocării datelor, acestea se șterg în mod automat.
- (2) În cazul transmiterii datelor cu caracter personal în baza prezentului Acord, Părțile vor indica, în măsura în care este posibil, acuratețea informațiilor, avându-se în vedere următoarele criterii:
- (a) informații a căror acuratețe nu este pusă la îndoială;
 - (b) informație verificată de către sursă, dar care nu este verificată de persoana abilitată să o transmită;
 - (c) informații neverificate de către sursă, dar care sunt coroborate cu alte informații deja înregistrate;
 - (d) informații care nu sunt verificate de către sursă și care nici nu pot fi coroborate cu alte informații.
- (3) În cazul în care una dintre Părți constată că datele cu caracter personal transmise anterior de către aceasta sunt incorecte, inexacte, nu sunt actualizate sau nu ar fi trebuit transmise, informează în cel mai scurt timp, dar nu mai târziu de 7 zile cealaltă Parte, care are obligația de a corecta sau de a șterge datele cu caracter personal și de a transmite o confirmare în acest sens.



- (4) În cazul în care o Parte are motive să creadă că datele cu caracter personal primite anterior de către aceasta sunt incorecte, inexacte, nu mai sunt valabile sau nu ar fi trebuit transmise, aceasta informează cealaltă Parte, care asigură adoptarea măsurilor adecvate raportat la aspectele sesizate, fără întârzieri nejustificate.
- (5) Prin excepție de la alineatele (3) și (4), Partea care primește o notificare cu privire la necesitatea corectării sau ștergerii datelor primite de la cealaltă Parte, poate decide să păstreze informațiile necesare dacă din celelalte informații pe care aceasta le deține, care relevă aspecte noi față de cele cunoscute de cealaltă Parte, rezultă o necesitate ulterioară, compatibilă cu scopul inițial, de a prelucra respectivele date.

Articolul 7 Securitatea datelor

- (1) Având în vedere stadiul actual al tehnologiei și costurile implementării și ținând seama de natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și de riscurile cu grade diferite de probabilitate și de gravitate la adresa drepturilor și libertăților persoanelor fizice, Părțile implementează măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător acestui risc
- (2) Părțile au obligația punerii în aplicare a măsurilor menite:
- (a) să împiedice accesul persoanelor neautorizate la echipamentele de prelucrare utilizate pentru prelucrare;
 - (b) să împiedice orice citire, copiere, modificare sau eliminare neautorizată a suporturilor de date;
 - (c) să împiedice introducerea neautorizată de date cu caracter personal și inspectarea, modificarea sau ștergerea neautorizată a datelor cu caracter personal stocate;
 - (d) să împiedice utilizarea sistemelor de prelucrare automată de către persoane neautorizate cu ajutorul echipamentelor de comunicare a datelor;
 - (e) să asigure faptul că persoanele autorizate să utilizeze un sistem de prelucrare automată au acces numai la datele cu caracter personal pentru care au autorizare;
 - (f) să asigure că este posibilă verificarea și identificarea organismelor cărora le-au fost transmise sau puse la dispoziție sau s-ar putea să le fie transmise sau puse la dispoziție date cu caracter personal utilizându-se echipamente de comunicare a datelor;
 - (g) să asigure că este posibil ca ulterior să se verifice și să se identifice datele cu caracter personal introduse în sistemele de prelucrare automată, momentul introducerii datelor cu caracter personal și entitatea care le-a introdus;
 - (h) să împiedice citirea, copierea, modificarea sau ștergerea neautorizată a datelor cu caracter personal în timpul transferurilor de date cu caracter personal sau în timpul transportării suporturilor de date;



- (i) să asigure posibilitatea recuperării sistemelor instalate în cazul unei întreruperi;
- (j) să asigure funcționarea sistemului, raportarea defecțiunilor de funcționare (fiabilitate) și imposibilitatea coruperii datelor cu caracter personal stocate din cauza funcționării defectuoase a sistemului.

Articolul 8

Notificarea unui incident de securitate a informațiilor personale

- (1) Atunci când constată existența unui incident care implică distrugerea sau pierderea accidentală ori accesarea, divulgarea sau modificarea neautorizată a informațiilor cu caracter personal, care prezintă un risc semnificativ de deteriorare, autoritatea competentă destinatară evaluează cu promptitudine probabilitatea și amploarea daunelor cauzate persoanelor fizice și integrității programului autorității competente care a transferat informațiile și ia, cu promptitudine, măsuri corespunzătoare pentru a atenua orice astfel de daune.
- (2) Printre măsurile de atenuare a daunelor se numără notificarea autorității competente care a transferat informațiile. Cu toate acestea, notificarea poate:
 - (a) să includă restricții corespunzătoare cu privire la transmiterea ulterioară a notificării;
 - (b) să fie amânată sau omisă în cazul în care o astfel de notificare poate pune în pericol securitatea națională;
 - (c) să fie amânată în cazul în care o astfel de notificare poate pune în pericol operațiuni de siguranță publică.
- (3) Măsurile de atenuare a daunelor includ, de asemenea, notificarea persoanei fizice în cauză, după caz, având în vedere circumstanțele incidentului, cu excepția cazului în care o astfel de notificare poate pune în pericol:
 - (a) ordinea și siguranța publică sau securitatea națională;
 - (b) anchetele, investigațiile sau procedurile oficiale;
 - (c) prevenirea, depistarea, investigarea sau urmărirea penală a infracțiunilor;
 - (d) drepturile și libertățile altor persoane, în special protecția victimelor și a martorilor.
- (4) Autoritățile competente implicate în transferul de informații cu caracter personal se pot consulta în ceea ce privește incidentul și răspunsul la acesta.
- (5) Incidentul de securitate va fi notificat către autoritatea de supraveghere menționată la articolul 14 din prezentul Acord, potrivit dreptului intern aplicabil statului în care se produce incidentul de securitate.

Articolul 9

Informații care se pun la dispoziția persoanei vizate

- (1) La momentul colectării datelor, se comunică persoanei vizate următoarele date:
 - (a) scopurile în care sunt prelucrate datele cu caracter personal;
 - (b) categoriile de date cu caracter personal prelucrate, datele de identificare și datele de contact ale autorității publice, operatorul de date cu caracter personal;



- (c) informații cu privire la destinatarii sau categoriile de destinatari cărora li s-au dezvăluit datele;
 - (d) perioada pentru care se preconizează că vor fi stocate datele cu caracter personal sau, dacă acest lucru nu este posibil, criteriile utilizate pentru a stabili această perioadă;
 - (e) existența dreptului de a solicita operatorului rectificarea sau ștergerea datelor cu caracter personal ori restricționarea prelucrării datelor cu caracter personal referitoare la persoana vizată sau a dreptului de a se opune prelucrării;
 - (f) dreptul de a depune o plângere în fața unei autorități de supraveghere;
 - (g) în cazul în care datele cu caracter personal nu au fost colectate de la persoana vizată, orice informații disponibile privind sursa acestora;
- (2) Părțile, în conformitate cu legislațiile naționale, pot restricționa accesul la informații în cazul în care o astfel de restricție, cu respectarea intereselor legitime ale persoanei vizate, reprezintă o măsură necesară și proporțională:
- (a) pentru a evita obstrucționarea anchetelor, cercetărilor sau procedurilor oficiale sau legale;
 - (b) pentru a evita compromiterea activităților de prevenire, combatere, cercetare și urmărire penală a infracțiunilor;
 - (c) pentru a proteja ordinea și siguranța publică;
 - (d) pentru a proteja securitatea națională;
 - (e) pentru a proteja persoana vizată sau drepturile și libertățile celorlalți.

Articolul 10

Acces

- (1) Părțile se asigură că orice persoană fizică are dreptul de a solicita accesul la informațiile sale cu caracter personal și, sub rezerva restricțiilor prevăzute la alineatul (2), de a-l obține. Accesul respectiv se solicită și se obține din partea autorității competente în conformitate cu dispozițiile cadrului juridic aplicabil al statului în care se introduce cererea.
- (2) Obținerea unor astfel de informații într-un anumit caz poate face obiectul unor restricții rezonabile prevăzute în temeiul dreptului intern. Ținând seama de drepturile fundamentale și interesele legitime ale persoanei fizice, o astfel de măsură este necesară și proporțională într-o societate democratică pentru:
- a) evitarea obstrucționării cercetărilor, anchetelor sau procedurilor oficiale sau juridice;
 - b) a nu prejudicia prevenirea, depistarea, investigarea sau urmărirea penală a infracțiunilor sau executarea pedepselor;
 - c) protejarea ordinii și siguranței publice;
 - d) protejarea securității naționale;
 - e) protejarea drepturilor și libertăților celorlalți.
- (3) Nu se impun persoanelor fizice cheltuieli excesive ca o condiție de acces la informațiile lor cu caracter personal.



- (4) O persoană fizică are dreptul de a autoriza, atunci când acest fapt este permis în temeiul dreptului intern aplicabil, un alt reprezentant să solicite accesul în numele său.
- (5) În cazul în care accesul este refuzat sau restricționat, autoritatea competentă căreia i s-a adresat solicitarea va furniza, fără întârzieri nejustificate, persoanei fizice sau reprezentantului său autorizat în mod corespunzător, astfel cum se prevede la alineatul (4), motivele refuzului sau ale restricționării accesului.

Articolul 11 **Rectificare**

- (1) Părțile se asigură că orice persoană fizică are dreptul de a solicita corectarea sau rectificarea informațiilor sale cu caracter personal despre care aceasta susține că sunt inexacte sau au fost prelucrate în mod necorespunzător. Corectarea sau rectificarea poate include completarea, ștergerea, blocarea sau alte măsuri ori metode de remediere a inexactităților sau a prelucrării necorespunzătoare. Respectiva corectare sau rectificare se solicită și se obține din partea unei Autorități competente în conformitate cu cadrul juridic aplicabil al statului în care se introduce cererea.
- (2) În cazul în care autoritatea competentă destinatară concluzionează în urma:
- (a) unei cereri prezentate în temeiul alineatului (1);
 - (b) a notificării de către furnizor, sau
 - (c) a propriilor investigații sau anchete.
- că informațiile pe care le-a primit în temeiul prezentului Acord sunt inexacte sau au fost prelucrate în mod necorespunzător, aceasta ia măsuri de completare, ștergere sau blocare ori aplică alte metode de corectare sau rectificare, după caz.
- (3) O persoană fizică are dreptul de a autoriza, atunci când acest fapt este permis în temeiul dreptului intern aplicabil, un alt reprezentant să solicite corectarea sau rectificarea în numele său.
- (4) În cazul în care corectarea sau rectificarea este refuzată sau restricționată, Autoritatea competentă căreia i s-a adresat solicitarea va furniza, fără întârzieri nejustificate, persoanei fizice sau reprezentantului său autorizat în mod corespunzător, astfel cum se prevede la alineatul (3), un răspuns care precizează motivele refuzului sau ale restricționării corectării ori rectificării.

Articolul 12 **Căi de atac administrative**

- (1) Părțile se asigură că orice persoană fizică are dreptul de a exercita căi de atac administrative în cazul în care aceasta consideră că cererea sa de acces prezentată în temeiul articolului 10 sau de rectificare a unor informații inexacte ori a unei prelucrări necorespunzătoare prezentată în temeiul articolului 11 a fost refuzată pe nedrept. Căile de atac respective se introduc în fața autorității competente și se soluționează de către aceasta în conformitate cu dispozițiile cadrului juridic aplicabil al statului în care se exercită căile de atac.



- (2) O persoană fizică are dreptul de a autoriza, atunci când acest fapt este permis în temeiul dreptului intern aplicabil, un alt reprezentant să exercite căile de atac administrative în numele său.
- (3) Autoritatea competentă în fața căreia se introduc căile de atac efectuează anchetele și verificările corespunzătoare și, fără întârzieri nejustificate, răspunde în scris, inclusiv prin mijloace electronice, comunicând rezultatul, precum și măsurile de îmbunătățire sau corective întreprinse, dacă este cazul.

Articolul 13 **Căi de atac judiciare**

- (1) Părțile prevăd în cadrele lor juridice aplicabile că, sub rezerva oricăror cerințe conform cărora trebuie să se epuizeze mai întâi căile de atac administrative, orice cetățean al statului unei Părți are dreptul de a solicita controlul jurisdicțional cu privire la:
 - (a) refuzul de către o autoritate competentă de a acorda acces la înregistrările care conțin informațiile sale cu caracter personal;
 - (b) refuzul de către o Autoritate competentă de a modifica înregistrările care conțin informațiile sale cu caracter personal; și
 - (c) divulgarea ilegală a respectivelor informații, efectuată în mod voit sau intenționat, care include posibilitatea unor despăgubiri compensatorii.
- (2) Căile de atac judiciare respective se introduc și se soluționează în conformitate cu dispozițiile cadrului juridic aplicabil al statului în care se exercită acestea.
- (3) Alineatele (1) și (2) nu aduc atingere oricăror altor căi de atac judiciare disponibile cu privire la prelucrarea informațiilor cu caracter personal ale unei persoane fizice efectuată în temeiul legislației statului în care se exercită căile de atac.

Articolul 14 **Supravegherea eficace**

Părțile desemnează, potrivit dreptului intern aplicabil, una sau mai multe autorități publice de supraveghere care:

- (1) exercită funcții și competențe de supraveghere independentă, inclusiv control jurisdicțional, investigare și intervenție, dacă este cazul, din proprie inițiativă;
- (2) au competența de a accepta și de a da curs plângerilor înaintate de persoane fizice cu privire la măsurile de punere în aplicare a prezentului Acord; și
- (3) au competența de a dispune urmărirea penală sau sancționarea disciplinară, după caz, a încălcărilor legii care au legătură cu prezentul Acord.

Articolul 15 **Informații clasificate**

În situația în care, în procesul de implementare a prezentului Acord, se identifică necesitatea schimbului de informații clasificate între autoritățile competente prevăzute la articolul 3, demersurile specifice vor fi realizate în conformitate cu *Acordul între Guvernul României și Guvernul Republicii Macedonia privind protecția reciprocă a informațiilor clasificate, semnat la București, la 04 august 2016.*



Articolul 16
Soluționarea litigiilor

Toate litigiile ce apar în cursul implementării sau interpretării acestui Acord vor fi soluționate prin intermediul consultărilor și negocierilor dintre Autoritățile Competente ale Părților.

Articolul 17
Costuri

(1) În situația în care Părțile nu decid altfel, fiecare Parte va suporta costurile pentru deplasarea personalului propriu pe teritoriul statului celeilalte Părți (transport internațional, cazare, mese, diurnă, transport intern, asigurări de călătorie și cheltuieli privind salariile), cu ocazia participării la activități comune derulate în vederea îndeplinirii obiectivelor de la articolul I.

(2) Partea pe teritoriul statului căreia au loc activitățile comune are obligația de a pune la dispoziție spațiul și echipamentele pentru desfășurarea în bune condiții a lucrărilor (săli de conferințe, echipamente IT&C, materiale de birotică și papetărie).

Articolul 18
Intrarea în vigoare și încetarea valabilității

(1) Prezentul Acord se încheie pentru o perioadă nedeterminată de timp și va intra în vigoare la data primirii ultimei notificări scrise, transmisă prin canale diplomatice, prin care Părțile se vor informa reciproc cu privire la faptul că procedurile interne necesare pentru intrarea în vigoare au fost îndeplinite.

(2) Prezentul Acord poate fi modificat numai cu acordul ambelor Părți. Modificările vor intra în vigoare în conformitate cu prevederile alineatului (1).

(3) Încetarea valabilității prezentului Acord nu va afecta obligațiile asumate în timpul implementării acestuia, în legătură cu activitățile de cooperare în derulare.

Semnat la București, la 15 septembrie 2022, în două exemplare originale, fiecare în limbile română, macedoneană și engleză, toate textele fiind egal autentice. În cazul unor diferențe de interpretare, textul în limba engleză va prevala.

Pentru
Guvernul României

Pentru
Guvernul Republicii Macedonia de
Nord

Copie certificată pentru conformitate cu originalul

Felix Zărnescu

Direcția Tratatelor Internaționale, Ministerul Afacerilor Externe



**Agreement
between
the Government of Romania
and
the Government of the Republic of North Macedonia
on strengthening cooperation
in the area of internal control and of preventing and combating corruption**

The Government of Romania and the Government of the Republic of North Macedonia, hereinafter referred to as "Parties",

Guided by the desire to further foster bilateral cooperation in the field of internal affairs, more specifically in the area of internal control and of preventing and combating corruption,

Acting in the interest of their citizens' security and for observing their rights and liberties,

Having in mind the principles of international law and the national legislation of their States,

Have agreed on the following:

**Article 1
Areas and Objective of Cooperation**

- (1) On the basis of this Agreement and according to the national legislations of their States, the Parties shall cooperate and shall provide assistance for strengthening cooperation in the area of internal control and of preventing and combating corruption.
- (2) Cooperation will focus mostly on the repression of corruptive behavior of police officers and other employees of the Competent Authorities of the Parties, with special emphasis of repressing the involvement of employees of the Competent Authorities of the Parties in organized crime, trafficking in human beings and illegal migration, smuggling of migrants, cigarettes and any other goods, illicit production, transport and trafficking in narcotic drugs, psychotropic substances and precursors, as well as respect of human rights and freedom, pursuant to the national legislation of their States.
- (3) Regarding internal control, on the basis of this Agreement, the main joint activities aim in particular at establishing performance objective and indicators, planning, organizing and proceeding activities, risk management, identifying sensitive functions, as well as monitoring and evaluating performances.



Article 2
Forms of Cooperation

- (1) The cooperation between the Competent Authorities of the Parties, appointed according to article 3 of this Agreement, shall consist of the following:
 - a) Exchange of experience;
 - b) Joint implementation of projects;
 - c) Joint operational activities;
 - d) Joint training.
- (2) The Competent Authorities in the area of internal affairs of the other European Union Member States, acceding countries and EU candidate countries may join the cooperation between the two Parties having received invitation to this end. Invitations shall be transmitted to the above mentioned Competent Authorities only if the Parties agreed in writing about this.
- (3) For achieving goals of this Agreement the Parties shall draft a joint action plan with concrete measures of cooperation in the area of reference.
- (4) The Parties will evaluate and if necessary will agree about the improvement of the cooperation in the framework of ministerial and experts meeting.

Article 3
Competent Authorities

For implementing the provisions of this Agreement the Parties appoint the following Competent Authorities.

(a) For Romania:

The Ministry of Internal Affairs, through:

- The Minister's Control Body;
- The Anti-corruption General Directorate;
- The General Directorate of Internal Protection.

(b) For the Republic of North Macedonia:

The Ministry of Interior, through:

- The Department for Internal Control, Criminal Investigations and Professional Standards;
- Bureau for Public Security – The Department for Suppression of Organized and Serious Crime;
- Bureau for Public Security – Department for Criminal Police.



Article 4
Personal Data Protection. Purpose and Use Limitation

- (1) Exchange of information between the Parties shall only take place for the purpose of and in accordance with the provisions of this Agreement. The transmissions of personal data by the Parties must be necessary, in individual cases, for the purpose referred to in Article 1 of this Agreement.
- (2) The information transmitted may be used only for the purposes which were initially transmitted and any restriction regarding the use, deletion or destruction, including possible access restrictions, in general or regarding specific terms, must be respected by the Parties. The Parties shall ensure that the personal data is processed in a manner that is directly relevant to and not excessive or overbroad in relation to the purposes of the processing.
- (3) The use of information for a purpose different than the purpose for which it was initially transmitted must be authorised by the transmitting Party.
- (4) The Parties shall supply each other only on information collected, stored and transmitted in accordance with their national legal framework and which has been obtained in accordance with the regulations in the field of human rights and fundamental freedoms.
- (5) Transmission to a third Party of the information received shall be restricted to the authorities responsible for preventing and combating criminal offences and shall take place under the same conditions as those applying to the original transmission. Any other onward transmission, including to third States or international organisations must be consented to by the transmitting Party.
- (6) Personal data will not be transferred when the requesting Party would use them to request, pronounce or execute the death penalty or any other cruel, inhuman or degrading treatment.

Article 5
Transmission of Personal Data

- (1) Requests from the Parties for personal data must be accompanied by a detailed indication of the purpose and reason for it.
- (2) In the absence of an indication as mentioned in paragraph (1) of the present Article, the Parties are not permitted to transmit personal data.
- (3) The Parties shall indicate at the moment of the transmission of personal data or before, the purpose for which the data were transmitted and any restrictions on its use, deletion or destruction, including possible access restrictions, in general or in specific terms. Where the need for such restrictions becomes apparent after the supply, the Parties shall inform each other of such restrictions at a later stage.
- (4) The Parties shall determine without undue delay, no later than six months after receipt, if and to what extent the personal data which have been supplied are necessary for the purpose for which they were supplied and inform the transmitting Party thereof. The personal data must be deleted when the data is no longer necessary for the purpose for which it was transmitted.



- (5) The processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, processing of genetic data, processing of biometric data for unique identification of a person or processing data concerning a person's health or sexual life and orientation is forbidden and may be authorised in exceptional cases only if:
- (a) It is strictly necessary, in a determined case;
 - (b) Appropriate safeguards for the rights and liberties of the data subject are provided;
 - (c) One of the following conditions is fulfilled:
 - (i) Processing is explicitly foreseen by law;
 - (ii) Processing is necessary to protect the vital interests of the data subject or of another natural person;
 - (iii) Processing relates to personal data which are manifestly made public by the data subject.
- (6) The Parties shall have in place effective methods of demonstrating the lawfulness of the processing of personal data and shall keep a record of all communications of personal data and of the grounds for such communications.

Article 6

Storage, Review, Correction and Deletion of Personal Data

- (1) The Parties shall retain personal data only as long as it is necessary for the purpose for which it was transmitted. The need for continued storage shall be reviewed no later than three years after the transmission. During the review, the Parties may decide on the continued storage of data until the following review which shall take place after another period of three years, if that is still necessary for the performance of its tasks. If no decision is taken on the continue storage of data, the data shall be deleted automatically.
- (2) When personal data is supplied by the Parties on the basis of this Agreement, the reliability of the information shall be indicated, as much as possible, on the basis of the following criteria:
- (a) Information whose accuracy is not in doubt;
 - (b) Information known personally to the source but not known personally to the official passing it on;
 - (c) Information not known personally to the source but corroborated by other information already recorded;
 - (d) Information which is not known personally to the source and which cannot be corroborated.
- (3) Where a Party has reason to believe that personal data previously transmitted by it is incorrect, inaccurate, no longer up to date or should not have been transmitted, it shall inform the other Party, as soon as possible but no later than 7 days, who shall correct or delete the personal data, and provide notification thereof.
- (4) Where a Party has reason to believe that personal data previously received by it is incorrect, inaccurate and no longer up to date or should not have been transmitted, it shall inform the other Party, which shall take appropriate measures in relation with this aspect, without undue delay.



- (5) By exception from paragraphs (3) and (4), in the event that one of the Parties is notified of the necessity to correct or delete the data received from the other Party, it may nonetheless decide not to delete the information if, based on the information in its files that is more extensive than that possessed by the other Party, it has further need to process that information, compatible with the initial purpose.

Article 7
Data Security

- (1) Taking into account the latest technology, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the right and freedoms of natural persons, the Parties shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk.
- (2) The Parties have the obligation to implement measures to:
- (a) Deny unauthorised persons access to processing equipment used for processing personal data;
 - (b) Prevent any unauthorised reading, copying, modification or removal of data media;
 - (c) Prevent unauthorised input of personal data and unauthorised inspection, modification or deletion of stored personal data;
 - (d) Prevent the use of automated data-processing systems by authorized persons using data communications equipment;
 - (e) Ensure that persons authorised to use an automated data-processing systems have access only to the personal data for which they have authorization;
 - (f) Ensure that it is possible to verify and identify the bodies to which personal data has been transmitted or has been made available or could be transmitted or could be made available using data communications equipment;
 - (g) Ensure that it is possible to subsequently verify and identify the personal data that have been input into automated data-processing systems, the moment when the data were input into automated data-processing systems, and the entity who input the data;
 - (h) Prevent the unauthorized reading, copying, modification or deletion of personal data during transfers of personal data or during transportation of data media;
 - (i) Ensure the possibility to recover the systems in place, in case of an interruption;
 - (j) Ensure the functioning of the system, the report of the malfunctions (reliability) and the impossibility to corrupt the stored personal data because of a malfunction of the system.

Article 8
Notifying a Data Security Incident

- (1) Upon discovery of an incident involving accidental destruction or loss or unauthorized access, disclosure, or modification of personal data, when there is a significant risk of damage, the receiving Competent Authority shall promptly



assess the likelihood and scale of damage to natural persons and to the integrity of the program of the Competent Authority transferring the data and shall promptly take appropriate action to mitigate any such damage.

- (2) Action to mitigate damage shall include notification to the transferring Competent Authority. However, notification may:
 - (a) Include appropriate restrictions as to the further transmission of the notification;
 - (b) Be delayed or omitted when such notification may endanger national security;
 - (c) Be delayed when such notification may endanger public security operations.
- (3) Action to mitigate damage shall include also notification of the data subject, where appropriate given the circumstances of the incident, unless such notification may endanger:
 - a) Public security or national security;
 - b) Official inquiries, investigations or proceedings;
 - c) The prevention, detection, investigation or prosecution of criminal offences;
 - d) Rights and freedoms of others, in particular the protection of victims and witnesses.
- (4) The Competent Authorities involved in the transfer of personal information may consult concerning the incident and the response thereto.
- (5) The data security incident will be notified to the supervisory public authorities mentioned in article 14 of this Agreement, according to the national legislation applicable to the state in which the security incident occurs.

Article 9

Information Made Available to the Data Subject

- (1) At the moment of data collection, the following data shall be communicated to the data subject:
 - (a) The purpose for which the personal data are processed;
 - (b) The categories of processed personal data, the identification data and the contact details of the public authority, the personal data controller;
 - (c) Information on the recipients or categories of recipients to whom the data have been disclosed;
 - (d) The period for which personal data will be stored or, where that is not possible, the criteria used to determine that period;
 - (e) The existence of the right to require to the controller rectification or ensure of personal data or restriction of the processing of personal data relating to the data subject or of the right to object to processing;
 - (f) The right to lodge a complaint with a supervisory authority;
 - (g) Where personal data have not been collected from the data subject, any available information on their source.
- (2) The Parties may, according to their national legislation, restrict access to information if such a restriction, respecting the legitimate interests of the data subject, represents a necessary and proportional measure:



- (a) To avoid obstructing official or legal inquiries, investigations or proceedings;
- (b) To avoid compromising the activities of preventing, combating, investigating and prosecuting criminal offences;
- (c) To protect public security;
- (d) To protect national security;
- (e) To protect the data subject or the rights and freedoms of others.

Article 10 **Access**

- (1) The Parties shall ensure that any natural person has the right to request access to his or her personal information and to obtain it, subject to the restrictions referred to in paragraph (2). Such access shall be sought and obtained from the Competent Authority in accordance with the provisions of the applicable legal framework of the State where the request is made.
- (2) Obtaining such information in a particular case may be subject to reasonable limits under national law.
Taking into account the fundamental rights and legitimate interests of the natural person, such a measure is necessary and proportionate in a democratic society for:
 - (a) Avoiding obstruction of official or legal investigations, inquiries or proceedings;
 - (b) Not to prejudice the prevention, detection, investigation or prosecution of criminal offences or the execution of penalties;
 - (c) Protecting public security;
 - (d) Protecting national security;
 - (e) Protecting the rights and freedoms of others.
- (3) Excessive expenses are not imposed on natural persons as a condition of access to their personal information.
- (4) A natural person shall have the right to authorize, where permitted under the applicable national law, another representative to request access on his or her behalf.
- (5) If the access is refused or restricted, the requested Competent Authority shall, without undue delay, provide the natural person or his or her duly authorized representative, as referred to in paragraph (4), with the reasons for the refusal or access restrictions.

Article 11 **Rectification**

- (1) The Parties shall ensure that any natural person has the right to request the correction or rectification of his or her personal information which he/ she alleges to be inaccurate or inappropriate. Correction or rectification may include completion, deletion, blocking or other measures or methods to correct



inaccuracies or inappropriate processing. That correction or rectification is requested and obtained from a Competent Authority in accordance with the applicable legal framework of the State where the request is made.

- (2) Where the receiving Competent Authority, following:
 - (a) A request submitted pursuant to paragraph (1);
 - (b) Notification by the supplier; or
 - (c) Its own investigations or inquiries concludes that the information it has received under this Agreement is inaccurate or has been improperly processed, it shall take action to complete, delete or block or apply other methods for correction or rectification, as appropriate.
- (3) A natural person shall have the right to authorize, where this is permitted under the applicable national law, another representative to request correction or rectification on his or her behalf.
- (4) If the correction or rectification is refused or restricted, the Competent Authority to which the request is submitted shall without undue delay provide the natural person or his or her duly accredited representative, as referred to in paragraph (3), with a reply stating the reasons for the refusal or for restraining the correction or rectification.

Article 12 Administrative Remedy

- (1) The Parties shall ensure that any natural person has the right to an effective administrative remedy if he or she considers that his or her request for access made under Article 10 or rectification of inaccurate or inappropriate processing provided under Article 11 was unjustly refused. Those remedies shall be brought before the Competent Authority and settled by it in accordance with the provisions of the applicable legal framework of the State in which the review procedures are sought.
- (2) A natural person shall have the right to authorize, where this is permitted under the applicable national law, another representative to exercise administrative remedies on his or her behalf.
- (3) The Competent Authority with which the remedies shall be lodged shall conduct appropriate investigations and verifications and, without undue delay, shall respond in writing, also by electronic means, communicating the result and any improvement or corrective action taken, where appropriate.

Article 13 Judicial remedy

- (1) The Parties shall stipulate in their applicable legal framework that, subject to any requirement that administrative remedy must be first exhausted, any citizen of a State of a Party shall have the right to request judicial review of:
 - (a) The refusal by a Competent Authority to grant access to records containing its personal information;



- (b) The refusal by a Competent Authority to modify records containing its personal information; and
 - (c) The unlawful disclosure of that information, whether willingly or intentionally, which includes the possibility of compensatory damages.
- (2) Such judicial remedies shall be introduced and resolved in accordance with the provisions of the applicable legal framework of the State in which they are sought.
- (3) Paragraphs (1) and (2) shall be without prejudice to any other judicial remedy available with regard to the processing of personal data of a natural person under the law of the State in which appeal is sought.

Article 14 **Effective Supervision**

The Parties shall designate, according to their national legislation, one or more supervisory public authorities, which:

- (1) Exercise independent supervisory functions and powers, including judicial review, investigation and intervention, where appropriate, on its own initiative;
- (2) Have the power to accept and prosecute complaints lodged by natural persons with regard to measures implementing this Agreement; and
- (3) Have the power to order the prosecution or disciplinary sanction, as the case may be, for law violations related to this Agreement.

Article 15 **Exchange of Classified Information**

In the process of implementation of the provisions of this Agreement will be identified the necessity to exchange classified information by the Competent Authorities mentioned in Article 3, this exchange shall be carried out observing the *Agreement between the Government of Romania and the Government of the Republic of Macedonia on mutual protection of classified information, signed in Bucharest on 4 of August 2016.*

Article 16 **Settlement of disputes**

All disputes emerging in the course of implementation or interpretation of this Agreement shall be settled through consultations and negotiations between Competent Authorities of the Parties.

Article 17 **Costs**

- (1) Unless the Parties decide otherwise, each Party will borne the costs related to the presence of its own personnel on the territory of the State of the other Party (international transport, accommodation, meals, subsistence, internal transportation, travel insurance and wages) during the participation in joint activities organized to achieve the objective mentioned in Article 1.



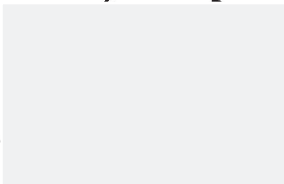
(2) The Party on whose territory the activities take place has the obligation to make available the space and the equipment for the performance in good conditions of the activities (conference rooms, ITC equipment's, office supplies and stationery).

Article 18
Entry into Force and Termination

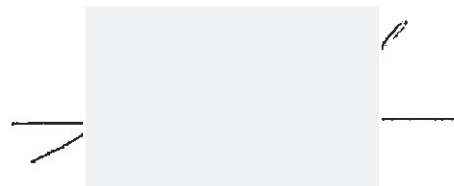
- (1) This Agreement shall be concluded for an indefinite period of time and shall enter into force on date of receipt of the last notification by diplomatic channels by which the Parties shall inform each other on the fulfillment of the necessary internal procedure for its entry into force.
- (2) This Agreement can be amended only with the agreement of both Parties. The amendments shall enter into force according to the procedure provided in paragraph (1).
- (3) The cease of validity of this Agreement shall not affect the obligations undertaken during its implementation regarding the on-going common projects.

Signed in Bucharest on 15 of September 2022 in two originals, each of them in Romanian, Macedonian and English language, all text being equally authentic. In case of any divergence in the interpretation, the English text shall prevail.

For
The Government
of Romania



For
The Government
of the Republic of North Macedonia



Copie certificată pentru conformitate cu originalul

Felix Zaharia / Director
Direcția Relații Internaționale
Ministerul Afacerilor Externe



- (3) Во однос на внатрешната контрола, врз основа на овој Договор, главните заеднички активности особено имаат за цел да се утврдат целите и индикаторите за успешноста, активностите за планирање, организирање и постапување, управување со ризик, идентификација на чувствителните функции, како и следење и оценување на работата.

Член 2

Форми на соработка

- (1) Соработката меѓу надлежните органи на Страните, утврдени во согласност со член 3 од овој Договор, се состои во следново:
- (а) размена на искуства;
 - (б) заедничко реализирање на проекти;
 - (в) заеднички оперативни активности;
 - (г) заеднички обуки.
- (2) Надлежните органи во областа на внатрешните работи во другите земји членки на Европската Унија, земји кои пристапуваат кон ЕУ и земји кандидатки може да се приклучат во соработката меѓу двете Страни откако ќе добијат покана за тоа.
Поканите ќе бидат доставени до горенаведените надлежни органи само доколку Страните писмено се договорат за истото.
- (3) За постигнување на целите на овој Договор, Страните составуваат заеднички акциски план со конкретни мерки за соработка во посочените области.
- (4) Страните имаат намера да ја оценат и доколку е неопходно, се согласни и да ја унапредат соработката во рамки на министерски и експертски состанок.

Член 3

Надлежни органи

За спроведување на одредбите од овој Договор, Страните ги назначуваат следниве надлежни органи:

- (а) за Романија:
- Министерство за внатрешни работи, преку:
 - Контролното тело на Министерот;
 - Генерална дирекција за борба против корупција;
 - Генерална дирекција за внатрешна безбедност.
- (б) за Република Северна Македонија:
- Министерство за внатрешни работи, преку:



- Оддел за внатрешна контрола, криминалистички истраги и професионални стандарди;
- Биро за јавна безбедност - Оддел за сузбивање на организиран и сериозен криминал;
- Биро за јавна безбедност - Оддел за криминалистичка полиција.

Член 4

Заштита на лични податоци, намена и ограничување на употребата

- (1) Размената на информации помеѓу Страните се одвива само за целите и во согласност со одредбите на овој Договор. Преносот на лични податоци од страните е неопходен, во поединечни случаи, за целите наведени во член 1 од овој Договор.
- (2) Пренесените информации се користат само за целите за кои првично биле пренесени и сите ограничувања по вреќа со употребата, бришењето или уништувањето, вклучително и можните ограничувања за пристап, општо или за специфични услови, мора да бидат почитувани од Страните. Страните обезбедуваат личните податоци да се обработуваат на начин што е директно релевантен за, а не претеран или прекумерен во однос на, целите на обработката.
- (3) Употребата на информации за намена различна од целта за која првично биле пренесени, мора да биде одобрена од Страната која ја пренесува.
- (4) Страните меѓусебно се снабдуваат само со информации, собрани, складирани и пренесени во согласност со нивната национална правна рамка и кои се добиени во согласност со прописите од областа на човековите права и основните слободи.
- (5) Преносот на добиените информации до трета Страна е ограничен на надлежните органи одговорни за спречување и борба против кривични дела и се одвиваат под нејките услови како и оние што се однесуваат на првичниот пренос. Секое друго наредно пренесување, вклучително и до трети држави или меѓународни организации, мора да биде одобрено од Страната пренесувач.
- (6) Личните податоци нема да се пренесат кога Страната барател ги користи за да побара, изрече или изврши смртна казна или која било друга сурова, нечовечна или понижувачка постапка.

Член 5

Пренос на лични податоци

- (1) Барањата од Страните за лични податоци се придружени со детални образложенија за целта и причините за истото.



- (2) Во отсуство на образложението, како што е наведено во ставот (1) на овој член, на страните не им е дозволено да пренесуваат лични податоци.
- (3) Страни во моментот на пренесување на лични податоци или пред тоа ја наведуваат, целта за која биле пренесени податоците и какви било ограничувања за нивната употреба, бришење или уништување, вклучително и можни ограничувања за пристап, општо или во специфични услови. Кога по преносот потребата за такви ограничувања станува очигледна, страните меѓусебно се информираат за ваквите ограничувања на повисоко ниво.
- (4) Страните без непотребно одложување утврдуваат, најдоцна во рок од шест месеци по приемот, дали и до кој степен личните податоци кои се доставени се неопходни за целта за која биле доставени и за тоа ја известуваат Страната пренесувач. Личните податоци се бришат кога податоците повеќе не се потребни за целта за која биле пренесени.
- (5) Обработка на лични податоци кои откриваат расно или етничко потекло, политички мислења, религиозни или филозофски убедувања, членство во синдикат, обработка на генетски податоци, обработка на биометриски податоци за единствена идентификација на личност или обработка на податоци во врска со здравјето или сексуалниот живот и ориентација на лицето е забрането и може да биде дозволено во исклучителни случаи, само ако:
- (а) е строго неопходно, во утврден случај;
 - (б) обезбедени се соодветни заштитни мерки за правата и слободите на субјектот на личните податоци;
 - (в) исполнет е еден од следниве услови:
 - обработката е експлицитно предвидена со закон;
 - обработката е неопходна за да се заштитат виталните интереси на субјектот на личните податоци или на друго физичко лице;
 - обработката се однесува на личните податоци кои се јасно објавени од субјектот на личните податоци.
- (6) Страните имаат воведено ефективни методи за докажување на законитоста на обработката на личните податоци и водат евиденција за сите комуникации на личните податоци и за основите за таквите комуникации.

Член 6

Чување, преглед, корекција и бришење на лични податоци

- (1) Страните ги задржуваат личните податоци само колку што е потребно за целта за која биле пренесени. Потребата за континуирано чување се разгледува не подоцна од три години по преносот. За време на прегледот, Страните можат да одлучат за продолжување на чувањето



на податоците до следниот презем што ќе се случи по друг период од три години, доколку тоа е сè уште неопходно за извршување на задачите. Доколку не се донесе одлука за продолжување на чувањето на податоците, податоците автоматски се бришат.

(2) Кога Страните доставуваат лични податоци врз основа на овој Договор, веродостојноста на информациите се покажува колку што е можно, врз основа на следниве критериуми:

(а) информации чија точност не е доведена во прашање;

(б) информации што се познати лично за изворот, но не се познати лично за службеникот што ги пренесува;

(в) информации кои не се познати лично за изворот, но се потврдени од други веќе евидентирани информации;

(г) информации кои не се познати лично за изворот и кои не можат да бидат потврдени.

(3) Кога Страната има причина да верува дека претходно пренесените лични податоци од негова страна се неточни, непрецизни, не се ажурирани или не треба да бидат пренесени, ја известува другата Страна што е можно поскоро, но не подоцна од 7 денови, која ќе ги коригира или избрише личните податоци и ќе приложи известување за истото.

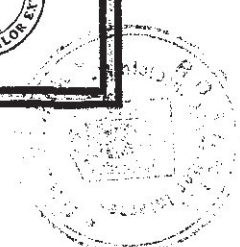
(4) Кога Страната има причина да верува дека претходно примените лични податоци од негова страна се неточни, непрецизни и не се ажурирани или не треба да бидат пренесени, ја известува другата Страна, која презема соодветни мерки во врска со овој аспект, без непотребно одложување.

(5) Со исклучок од ставовите (3) и (4), во случај кога една од Страните ќе биде известена за потребата да се поправат или бришат податоците добиени од другата Страна, истата може да одлучи да не ги брише информациите ако, врз основа на информациите во нејзините досиеја, кои се пообемни од оние кои ги поседува другата Страна, треба дополнително да ги обработува тие информации, кои се компатибилни со почетната цел.

Член 7

Безбедност на податоците

(1) Имајќи ја предвид најновата технологија, трошоците за спроведување и природата, обемот, контекстот и целите на обработката, како и ризикот од различни можности и сериозност за правото и слободите на физичките лица, Страните имплементираат соодветни технички и организациски мерки за да се обезбеди ниво на безбедност соодветно на ризикот.



(2) Страните имаат обврска да спроведат мерки за да:

(а) одбијат пристап на неовластено лице до опрема за обработка која се користи за обработка на лични податоци;

(б) спречат какво било неовластено читање, копирање, модификација или отстранување на податоци зачувани на медиум;

(в) спречат неовластено внесување на лични податоци и неовластено испитување, модификација или бришење на зачуваните лични податоци;

(г) спречат употреба на автоматски системи за обработка на податоци од

овластени лица кои користат опрема за комуникација на податоци;

(д) обезбедат лицата овластени да користат автоматски системи за обработка на податоци да имаат пристап само до личните податоци за кои имаат овластување;

(е) обезбедат дека е можно да се проверат и да се идентификуваат органите на кои се пренесени личните податоци или се ставени на располагање или може да се пренесат или може да бидат достапни со употреба на опрема за комуникација на податоци;

(ж) обезбедат дека е можно последователно да се проверат и идентификуваат личните податоци кои биле внесени во автоматски системи за обработка на податоци, моментот кога податоците биле внесени во автоматски системи за обработка на податоци и субјектот кој ги внесува податоците;

(з) спречат неовластено читање, копирање, модификација или бришење на лични податоци за време на пренос на лични податоци или за време на пренесување на податоци зачувани на медиум;

(и) обезбедат можност за враќање на воспоставените системи, во случај на прекин;

(к) обезбедат функционирање на системот, извештајот за дефект (сигурност) и неможност за корумпирање на зачуваните лични податоци заради дефект на системот.

Член 8

Известување за инцидент за безбедност на податоците

(1) По откривањето на инцидентот што вклучува случајно уништување или загуба или неовластен пристап, откривање или измена на личните податоци, кога постои значителен ризик од оштетување, надлежниот орган примател веднаш ја проценува веројатноста и обемот на штета на физичките лица и на интегритетот на програмата на надлежниот орган што ги пренесува податоците и навремено презема соодветни активности за да ја ублажи таквата штета.



- (2) Активността за намалување на штетата вклучува и известување до надлежниот орган што ги пренесува. Меѓутоа, известувањето може:
- (а) да вклучи соодветни ограничувања во врска со понатамошниот пренос на известувањето;
 - (б) да биде одложено или прескокнуто кога таквото известување може да ја загрози националната безбедност;
 - (в) да се одложи кога таквото известување може да ги загрози операциите од јавна безбедност.
- (3) Активностите за ублажување на штетата вклучуваат и известување за субјектот на личните податоци, доколку е потребно, со оглед на околностите на инцидентот, освен ако таквото известување може да загрози:
- (а) јавна безбедност или национална безбедност;
 - (б) службени испитувања, истраги или постапки;
 - (в) спречување, откривање, истрага или гонење на кривични дела;
 - (г) права и слободи на другите, особено заштитата на жртвите и сведоците.
- (4) Надлежните органи вклучени во пренесувањето лични информации можат да се консултираат во врска со инцидентот и одговорот на истиот.
- (5) За инцидентот за безбедноста на податоците ќе бидат известени надзорните јавни органи споменати во член 14 од овој Договор, во согласност со националното законодавство кое се применува во државата во која се случува безбедносниот инцидент.

Член 9

Информација кои се достапни на субјектот на личните податоци

- (1) Во моментот на собирање на податоците, следните податоци ќе бидат доставени до субјектот на личните податоци:
- (а) целта за која се обработуваат личните податоци;
 - (б) категории на обработени лични податоци, податоци за идентификација и детали за контакт на јавната власт, контролорот за лични податоци;
 - (в) информации за примателите или категориите на приматели на кои им биле откриени податоците;
 - (г) периодот за кој ќе се чуваат личните податоци или, кога тоа не е можно, критериумите што се користат за одредување на тој период;
 - (д) постоење на право да побара од контролорот да се изврши корекција или да се обезбедат личните податоци или ограничување на обработката на личните податоци кои се однесуваат на субјектот на личните податоци или правото на приговор за обработка;
 - (е) право на жалба до надзорен орган;



(е) сите достапни информации за нивниот извор, кога личните податоци не се собрани од субјектот на личните податоци.

(2) Страните можат, во согласност со нивното национално законодавство, почитувајќи ги законските интереси на субјектот на личните податоци, да го ограничат пристапот до информации доколку таквото ограничување претставува неопходна и пропорционална мерка:

(а) да се избегне попречување на службени или судски истражувања, истраги или постапки;

(б) да се избегне загрозување на активностите за спречување, борба, истрага и гонење кривични дела;

(в) заштитата на јавната безбедност;

(г) заштитата на националната безбедност;

(д) да го заштити субјектот на личните податоци за правата и слободите на другите.

Член 10

Пристап

(1) Страните ќе обезбедат дека секое физичко лице има право да побара пристап до неговите лични информации и да ги добие, во согласност со ограничувањата од ставот (2). Таквиот пристап ќе се бара и добие од надлежниот орган во согласност со одредбите на важечката правна рамка на државата во која е поднесено барањето.

(2) Добивањето на вакви информации во одреден случај може да биде предмет на разумни граници според националното законодавство. Имајќи ги предвид основните права и легитимни интереси на физичкото лице, таквата мерка е неопходна и сразмерна во едно демократско општество за:

(а) избегнување на пречки во службени или судски истражувања, истраги или постапки;

(б) да не е во спротивност со спречувањето, откривањето, истрагата или гонењето на кривични дела или извршување на казните;

(в) заштитата на јавната безбедност;

(г) заштитата на националната безбедност;

(д) заштитата на правата и слободите на другите.

(3) Прекумерните трошоци не се наметнуваат на физички лица како услов за пристап до нивните лични информации.

(4) Физичко лице има право, доколку е дозволено според важечкиот национален закон, да овласти друг претставник да побара пристап во негово име.



- (5) Доколку пристапот е одбиен или ограничен, замолените надлежен орган, без непотребно одложување, ги обезбедува на физичкото лице или неговиот соодветно овластен застапник, како што е наведено во ставот (4), причините за одбивањето или пристапот ограничувања.

Член 11 Исправка

- (1) Страните обезбедуваат дека секое физичко лице има право да побара корекција или исправка на неговите лични информации за кои смета дека се неточни или несоодветни. Корекција или исправка може да вклучува завршување, бришење, блокирање или други мерки или методи за да се поправат неточностите или несоодветната обработка. Оваа корекција или исправка е побарана и добиена од надлежен орган во согласност со важечката правна рамка на државата во која е поднесено барањето.
- (2) Надлежниот орган примател, во случај кога:
- (а) барање е поднесено согласно став (1);
 - (б) известување од доставувачот; или
 - (в) сопствените истражувања или истраги заклучуваат дека информациите што ги добиле според овој Договор се неточни или биле неправилно обработени, презема активности за да ги комплетира, избрише или блокира или примени други методи за корекција или исправка, како што е соодветно.
- (3) Физичко лице има право да овласти, кога тоа е дозволено според важечкиот национален закон, друг претставник да побара корекција или исправка во свое име.
- (4) Доколку корекцијата или исправката е одбиена или ограничена, надлежниот орган до кој е поднесено барањето без непотребно одлагање доставува одговор на физичкото лице или неговиот соодветно акредитиран претставник од ставот (3) на овој член, наведувајќи ги причините за одбивањето или за ограничување на корекцијата или исправката.

Член 12 Административна постапка

- (1) Страните обезбедуваат дека секое физичко лице има право на ефективен управен лек доколку смета дека неговото барање за пристап направено според член 10 или исправка на неточна или несоодветна обработка предвидено со член 11, неправедно било одбиено. Овие лекови ќе бидат изведени пред надлежниот орган и



решени од него во согласност со одредбите на важечката правна рамка на државата во која се бараат ревизија на процедурите.

- (2) Физичко лице има право да оспори, кога тоа е дозволено според важечкиот национален закон, друг претставник да примени управни лекови во негово име.
- (3) Надлежниот орган до кој ќе се поднесат лековите спроведува соодветни истраги и проверки и, без непотребно одложување, одговара писмено, исто така, преку електронски средства, соопштувајќи го резултатот и какви било преземени подобрувања или корективни активности, доколку е соодветно.

Член 13

Судска постапка

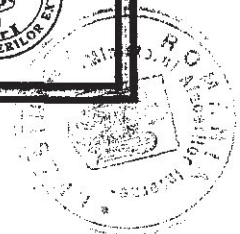
- (1) Страните во својата важечка законска рамка утврдуваат - зависно од евентуалното барање - дека мора првично да биде исцрпен управниот лек, сепак граѓанин на државата на Страната да има право да бара судска ревизија на:
 - (а) одбивање од надлежен орган да дозволи пристап до запис кои содржат нивни лични информации;
 - (б) одбивање од надлежен орган за измена на записите кои содржат нивни лични информации; и
 - (в) незаконско откривање на тие информации, доброволно или намерно, што вклучува можност за надомест на штети.
- (2) Ваквите правни лекови се воведуваат и решаваат во согласност со одредбите на важечката правна рамка на државата во која се бараат.
- (3) Ставовите (1) и (2) не се во спротивност со кој било друг правен лек достапен во однос на обработката на личните податоци на физичко лице според законот на државата во која се бара жалба.

Член 14

Ефективен надзор

Страните назначуваат, во согласност со нивното национално законодавство, еден или повеќе јавни надзорни органи, кои:

- (1) вршат независни надзорни функции и овластувања, вклучително и судска ревизија, истрага и интервенција, кога е потребно, на своја иницијатива;
- (2) имаат надлежност да прифаќаат и процесуираат постапки поднесени од физички лица во врска со мерките за спроведување на овој Договор; и



- (3) имаат надлежност да спроведат судска постапка или дисциплинска санкција, зависно од случајот, за прекршување на законите поврзани со овој Договор.

Член 15

Размена на класифицирани податоци

Доколку во постапката на спроведување на одредбите од овој Договор е утврдена потребата за размена на класифицирани информации од надлежните органи наведени во член 3, оваа размена се спроведува со почитување на Спогодбата меѓу Владата на Романија и Владата на Република Македонија за заемна заштита на класифицирани информации, потпишан во Букурешт на 4 август 2016 година.

Член 16

Решавање спорови

Споровите кои евентуално ќе произлезат при реализација или толкување на овој Договор, се решаваат преку консултации и преговори меѓу надлежните органи на Страните.

Член 17

Трошоци

- (1) Освен доколку Страните не одлучат поинаку, секоја Страна ги сноси трошоците поврзани со присуството на својот персонал на територијата на државата на другата Страна (меѓународен превоз, сместување, исхрана, издршка, внатрешен превоз, патничко осигурување и дневници) за време на учеството во заеднички активности организирани за исполнување на целите наведени во член 1.
- (2) Страната на чија територија се одвиваат активностите има обврска да стави на располагање простор и опрема за изведување во добри услови на активности (конференциски сали, опрема за ИТК, канцелариски материјал и меморандуми).

Член 18

Влегување во сила и откажување

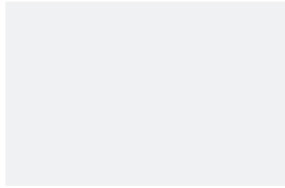
- (1) Овој Договор се склучува на неопределено време и влегува во сила со денот на приемот на последното известување по дипломатски канали со кое Страните се информираат едни со други за исполнувањето на потребната внатрешна постапка за негово влегување во сила.



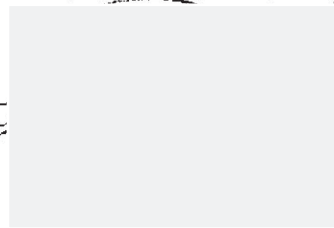
- (2) Овој Договор може да се измени и дополнува само со согласност на двете Страни. Измените и дополнувањата влегуваат во сила во согласност со поставката предвидена во ставот (1).
- (3) Престанокот на важноста на овој Договор не влијае на обврските преземени за време на неговото спроведување во врска со тековните засаднички проекти.

Потпишан во Букурешт на 15 септември 2022 година во два оригинални примероци, секој на романски, македонски и англиски јазик, при што секој од текстовите е еднакво автентичен. Во случај на разлики во толкувањето ќе преопладува текстот на англиски јазик.

За
Владата на Романија



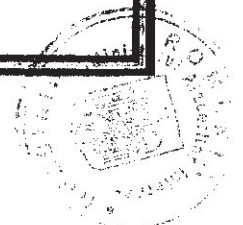
За
Владата на Република
Северна Македонија



Copie certificată pentru conformitate cu originalul

Felicia Zahar (d. [redacted])

Directorat Internațional
Ministerul Afacerilor Externe



ROMÂNIA
MINISTERUL AFACERILOR INTERNE



MINISTRU

București
Nr. 8753/193 din 16.05.2022
Nr. exemplar 1

Nr. 20/20775/M.N.
Data 05.08.2022

APROB
ROMANIA
Nicolae - Ionel JUCA
PRIM-MINISTRU

MEMORANDUM.

De la: Domnul Lucian Nicolae BODE
Ministrul Afacerilor Interne

Avizat: Domnul Bogdan – Lucian AURESCU
Ministrul Afacerilor Externe

Doamna Ancuța Gianina OPRE
Președintele Autorității Naționale de Supraveghere
a Prelucrării Datelor cu Caracter Personal

Domnul Adrian CĂCIU
Ministrul Finanțelor

Domnul Marian – Cătălin PREDOIU
Ministrul Justiției

Tema: Finalizarea negocierilor și semnarea Acordului între Guvernul României și Guvernul Republicii Macedonia de Nord privind consolidarea cooperării în domeniul controlului intern și al prevenirii și combaterii corupției



În dorința de a consolida cooperarea stabilită în domeniul afacerilor interne, în cadrul consultărilor bilaterale, autoritățile guvernamentale din România și Republica Macedonia de Nord și-au manifestat interesul pentru extinderea cadrului juridic, inclusiv în ceea ce privește conlucrarea în domeniul controlului intern și al prevenirii și combaterii corupției.

De urmare, în conformitate cu măsurile aprobate prin Memorandumul MAI nr. 285974/05.06.2012 cu tema: *Încheierea Memorandumului de cooperare între Ministerul Administrației și Internelor din România și Ministerul Afacerilor Interne din Republica Macedonia privind consolidarea cooperării în domeniul controlului intern și al prevenirii și combaterii corupției*, partea română a remis la Skopje un proiect de text al noului document de cooperare.

Schimbul de texte a continuat pe parcursul ultimilor ani, intervenind o serie de modificări legate de:

- actualizările necesare privind noua denumire a Republicii Macedonia de Nord;
- completarea textului cu prevederile privind protecția datelor cu caracter personal, urmare a noului cadru juridic adoptat la nivelul UE;
- nivelul de încheiere a documentului – s-a stabilit ca acesta să fie încheiat la nivel interguvernamental, având în vedere prevederile privind protecția datelor cu caracter personal (inițial documentul urma să fie încheiat între Ministerele de Interne);
- titlul documentului – *Acord de cooperare* în loc de *Memorandum de cooperare*, în conformitate cu practica și normele privind tratatele la nivel interguvernamental, în sensul Legii 590/2003 privind tratatele.

Încheierea Acordului de cooperare are ca finalitate consolidarea cooperării în domeniul controlului intern și al prevenirii și combaterii corupției între autoritățile competente din cele două state.

Cooperarea va fi orientată în special pe combaterea corupției în rândul polițiștilor și al altor angajați ai autorităților competente ale Părților, cu accent pe combaterea implicării acestora în activități de crimă organizată, trafic de ființe umane și migrație ilegală, trafic de migranți, trafic de țigări sau alte produse; producție ilicită, transport și trafic de substanțe stupefiante și substanțe psihotrope și precursori și, de asemenea, pe respectarea drepturilor și libertăților omului, în conformitate cu legislația națională a statelor Părților.

În ceea ce privește controlul intern, activitățile principale ce pot fi derulate în comun vizează în special stabilirea obiectivelor și indicatorilor de performanță, planificarea, organizarea și procedurarea activităților, managementul riscurilor, identificarea funcțiilor sensibile, precum și monitorizarea și evaluarea performanțelor.

Cooperarea se va realiza prin schimburi de experiență, implementarea de proiecte în comun, activități operaționale comune și pregătire comună.

Ultima versiune de text a fost remisă de partenerii din Macedonia de Nord, ca răspuns la proiectul consolidat remis de partea română în anul 2021. De asemenea, aceștia au informat despre faptul că au fost finalizate procedurile interne în vederea semnării acordului interguvernamental în cauză.

Față de cele de mai sus, propunem și rugăm să aprobați:

1. Finalizarea negocierilor și pregătirea pentru semnare a **Acordului de cooperare între Guvernul României și Guvernul Republicii Macedonia de Nord privind consolidarea cooperării în domeniul controlului intern și al prevenirii și combaterii corupției**, pe baza textului anexat la prezentul Memorandum;
2. În cazul în care nu vor mai interveni modificări de fond, Acordul să fie semnat, la o dată convenită de comun acord cu partenerii de cooperare de la Skopje;
3. Documentul să fie semnat, pentru partea română, de către ministrul afacerilor interne sau un alt demnitar desemnat în acest sens;
4. După caz, Ministerul Afacerilor Externe să elibereze Deplinele Puteri pentru reprezentantul părții române desemnat să semneze noul document juridic de referință.

Anexe la prezentul Memorandum:

- Proiectul convenit al Acordului de cooperare între Guvernul României și Guvernul Republicii Macedonia de Nord privind consolidarea cooperării în domeniul controlului intern și al prevenirii și combaterii corupției;
- Memorandumul MAI nr. 285974/05.06.2012 cu tema: *Încheierea Memorandumului de cooperare între Ministerul Administrației și Internelor din România și Ministerul Afacerilor Interne din Republica Macedonia privind consolidarea cooperării în domeniul controlului intern și al prevenirii și combaterii corupției*.

Întocmit: comisar șef de poliție dr. Vilhelmina Lucinscu, Direcția Generală Afaceri Europene, Schengen și Relații Internaționale, Ministerul Afacerilor Interne.

București, Piața Revoluției nr. 1A, et. VI, sector 1



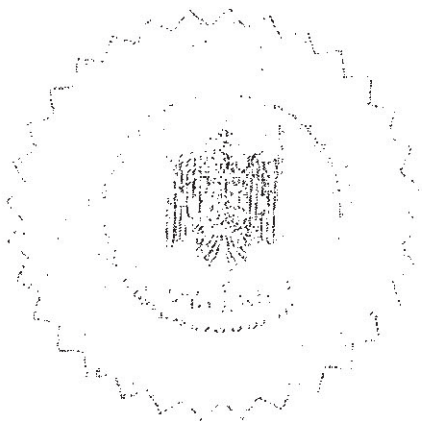


ROMÂNIA

MINISTERUL AFACERILOR EXTERNE

Certifică prin prezenta că domnul Lucian Nicolae BODE, ministrul
afacerilor interne,
are depline puteri pentru a semna:

*Acordul între Guvernul României și Guvernul Republicii Macedonia de
Nord privind consolidarea cooperării în domeniul controlului intern și
al prevenirii și combaterii corupției*



/BOGDAN AURESCU

MINISTRUL AFACERILOR EXTERNE

Nr. 1712
București, septembrie 2022



FULL POWERS

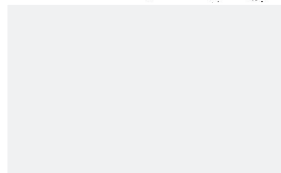
I, **Artan Grubi**, the First Deputy Prime Minister and Minister of Political System and Inter-Community Relations of the Republic of North Macedonia,

HEREBY AUTHORIZE Mr. Oliver Spasovski, Minister of Interior of the Republic of North Macedonia, on behalf of the Government of the Republic of North Macedonia to sign the Agreement between the Government of the Republic of North Macedonia and the Government of Romania on Strengthening Cooperation in the Area of Internal Control and of Preventing and Combating Corruption.

IN WITNESS WHEREOF, this FULL POWERS is issued to Mr. Oliver Spasovski.

Done in Skopje, on 13 09 .2022.

Artan Grubi, Ph.D.



ОВЛАСТУВАЊЕ

Јас, Артан Груби, Прв Заменик на Претседателот на Владата и Министер за политички системи и односи меѓу заедниците на Владата на Република Северна Македонија,

ГО ОВЛАСТУВАМ г. Оливер Спасовски, Министер за внатрешни работи на Република Северна Македонија, во име на Владата на Република Северна Македонија да го потпише Договорот помеѓу Владата на Република Северна Македонија и Владата на Романија за зајакнување на соработката во областа на внатрешната контрола и спречување и борба против корупција.

Во СВЕДОШТВО НА ГОРЕНАВЕДЕНОТО, го издавам ова овластување на г. Оливер Спасовски.

Скопје, 15 09 2022 година

dr.Artan Grubi

