AGREEMENT
BETWEEN THE PARTIES TO THE POLICE COOPERATION CONVENTION FOR SOUTHEAST EUROPE ON THE AUTOMATED EXCHANGE OF DNA DATA, DACTYLOSCOPIC DATA AND VEHICLE REGISTRATION DATA

The Parties to this Agreement,

Based on the Police Cooperation Convention for Southeast Europe (hereinafter referred to as: "the PCC SEE"),

Desirous of strengthening cross-border cooperation, particularly in combating terrorism, cross-border crime and illegal migration and endeavouring the implementation of the PCC SEE, in particular on the transmission and comparison of DNA profiles, dactyloscopic data and vehicle registration data,

Having in mind the Conclusions of the 11th PCC SEE Committee of Ministers (01/2014), the Conclusions of the 12th PCC SEE Committee of Ministers (05/2014) and the Conclusions of the 15th PCC SEE Committee of Ministers (01/2016), highlighting the strong need for the development of automated DNA data, dactyloscopic data and vehicle registration data information exchange, within the PCC SEE legal framework,

Acknowledging the PCC SEE developments in the Area of Data Protection, where all Parties have successfully passed the evaluations in the area of personal data protection and have, consequently, fulfilled the preconditions to exchange personal data, while taking into account the common European data protection principles and standards as enshrined in Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (hereinafter referred to as: "Directive (EU) 2016/680") and the relevant Convention of the Council of Europe on Protection of Personal Data and relevant Council of Europe recommendation for protection of personal data for the Police sector (hereinafter referred to as: "relevant Council of Europe Convention and recommendations"),

Having in mind the provisions deriving from the Treaty of 27 May 2005 between the Kingdom of Belgium, the Federal Republic of Germany, the Kingdom of Spain, the French Republic, the Grand Duchy of Luxembourg, the Kingdom of the Netherlands and the Republic of Austria on the stepping up of cross-border cooperation, particularly in combating terrorism, cross-border crime and illegal migration (hereinafter referred to as: "the Prüm Treaty"), the Implementing Agreement of the Prüm Treaty, the Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime (hereinafter referred to as: "the Prüm Decision") and the Council Decision 2008/616/JHA of 23 June 2008 on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in

combating terrorism and cross-border crime (hereinafter referred to as: ”the Prüm Implementing Decision”),

Have agreed as follows:

CHAPTER I
General Provisions

Article 1
Aim, scope and definitions

(1) By means of this Agreement, the Parties intend to strengthen cross-border police cooperation with respect to fighting threats to public security with respect to prevention, detection and investigation of criminal offences as laid down in the PCC SEE. To this end, this Agreement contains rules for automated exchange of DNA data, dactyloscopic data and vehicle registration data and exchange of available subsequent personal and case-related data in case of a hit.

(2) For supporting the implementation of the transmission and comparison of DNA data, dactyloscopic data and vehicle registration data the Parties lay down:

(a) provisions on the conditions and procedure for the automated transfer of DNA profiles, dactyloscopic data and vehicle registration data;

(b) the necessary administrative and technical provisions for the implementation of automated exchange of DNA data, dactyloscopic data and vehicle registration data.

(3) For the purposes of this Agreement:

(a) “**search**” and “**comparison**” mean the procedures by which it is established whether there is a match between, respectively, DNA data or dactyloscopic data which have been communicated by one Party and DNA data or dactyloscopic data stored in the databases of one, several, or all of the Parties;

(b) “**automated searching**” means an online access procedure for consulting the databases of one, several, or all of the Parties;

(c) “**DNA profile**” means a letter or number code which represents a set of identification characteristics of the non-coding part of an analysed human DNA sample, i.e. the particular molecular structure at the various DNA locations (loci);

(d) “**non-coding part of DNA**” means chromosome regions not genetically expressed, i.e. not known to provide for any functional properties of an organism;

(e) “**DNA data**” mean DNA profile, reference number and personal identification data;

(f) “**DNA reference data**” mean DNA profile and reference number;

(g) “**reference DNA profile**” means the DNA profile of an identified person;

(h) “**unidentified DNA profile**” means the DNA profile obtained from traces collected during the investigation of criminal offences and belonging to a person not yet identified;

(i) "**note**" means a Party's marking on a DNA profile in its national database indicating that there has already been a match for that DNA profile on another Party's search or comparison;

(j) "**dactyloscopic data**" mean fingerprint images, images of fingerprint latents, palm prints, palm print latents and templates of such images (coded minutiae), when they are stored and dealt within an automated fingerprint identification system (AFIS) database;

(k) "**vehicle registration data**" mean the data-set as specified in Article 9;

(l) "**personal data**" shall mean any information relating to an identified or identifiable natural person (the "data subject");

(m) "**core personal data**" means Name (Family Name(s), First Name(s)), Date of Birth, Nationality, Gender, Alias Name(s) and Date(s) of Birth, Date Fingerprinted / DNA sampled, Reason Fingerprinted / DNA sampled, Place Fingerprinted / DNA sampled, and if available True Identity Confirmation Status, Address, Height, Weight, Number of Passport, Picture (Face);

(n) "**individual case**" means a single investigation or prosecution file. If such a file contains more than one DNA profile or one piece of dactyloscopic data they may be transmitted together as one request;

(o) "**processing of personal data**" means any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, sorting, retrieval, consultation, use, disclosure by supply, dissemination or otherwise making available, alignment, combination, erasure or destruction of data. Processing within the meaning of this Agreement shall also include notification of whether or not a hit exists;

(p) "**automated search procedure**" means online access to the databases of another Party where the response to the search procedure is fully automated;

(q) "**missing persons**" means persons whose absence is assumed in connection to a crime, a suicide, an accident or a disaster;

(r) "**match / no-match**" means the result of a machine (AFIS or DNA-match-engine). It would also mean that a no-match is always a no-hit. On the other hand it is also possible that a match is a no-hit after the necessary forensic verification / validation;

(s) "**hit**" means the confirmed positive identification result confirmed by a human being (expert) after forensic verification / validation. Forensic confirmation has to be carried out in line with forensic quality management requirements (e.g. accreditation standards);

(t) "**DNA analysis files**" mean national DNA databases and linked administrative subsystems as e.g. crime scene stain / person identification databases and lab information systems (LIMs), which contain all relevant information for forensic and investigative confirmation of DNA profiles analysed with DNA technologies and will allow also secure linkage to Individual case / personal data of DNA profiles;

(u) "**criminal offences**" mean those offences which are prosecuted ex officio in accordance with the Parties' national legislation.

CHAPTER II
ONLINE ACCESS AND FOLLOW-UP REQUESTS

Article 2
Establishment of national DNA analysis files

(1) The Parties shall open and keep national DNA analysis files for the investigation of criminal offences and assist in the identification of missing persons and unidentified human remains in accordance with the national legislation. Processing of data kept in those files, under this Agreement, shall be carried out in accordance with this Agreement, in compliance with the PCC SEE and the national legislation applicable to the data processing.

(2) For the purpose of implementing this Agreement, the Parties shall ensure the availability of reference data from their national DNA analysis files as referred to in the first sentence of paragraph 1. Reference data shall only include DNA profiles established from the non-coding part of DNA and a reference number. Reference data shall not contain any data from which the data subject can be directly identified. Reference data which is not attributed to any individual (unidentified DNA profiles) shall be recognisable as such.

(3) Each Party shall inform the Depositary of the national DNA analysis files to which Articles 2 to 4 and Article 7 apply and the conditions for automated searching as referred to in Article 3(1).

Article 3
Automated searching of DNA profiles

(1) For the investigation of criminal offences and to assist in the identification of missing persons and unidentified human remains, the Parties shall allow other Parties' national contact points as referred to in Article 8, access to the reference data in their DNA analysis files, with the power to conduct automated searches by comparing DNA profiles. Searches may be conducted only in individual cases and in compliance with the requesting Party's national legislation.

(2) Should an automated search show that a DNA profile supplied matches DNA profiles entered in the receiving Party's searched file, the national contact point of the searching Party shall receive in an automated way the reference data with which a match has been found. If no match can be found, automated notification of this shall be given.

Article 4
Automated comparison of DNA profiles

(1) For the investigation of criminal offences and to assist in the identification of missing persons and unidentified human remains, the Parties shall, by mutual consent, via their national contact points, compare the DNA profiles of their unidentified DNA profiles with all DNA profiles from other national DNA analysis files' reference data. Profiles shall be supplied and compared in automated form. Unidentified DNA profiles shall be supplied for comparison only where provided for under the requesting Party's national legislation.

(2) Should a Party, as a result of the comparison referred to in paragraph 1, find that any DNA profiles supplied match any of those in its DNA analysis files, it shall, without delay, supply the other Party's national contact point with the DNA reference data with which a match has been found.

Article 5
Dactyloscopic data

For the purpose of implementing this Agreement, Parties shall ensure the availability of reference data from the file for the national automated fingerprint identification systems established for the prevention and investigation of criminal offences and to assist in the identification of missing persons and unidentified human remains. Reference data shall only include dactyloscopic data and a reference number. Reference data shall not contain any data from which the data subject can be directly identified. Reference data which is not attributed to any individual (unidentified dactyloscopic data) must be recognisable as such.

Article 6
Automated searching of dactyloscopic data

(1) For the prevention and investigation of criminal offences and to assist in the identification of missing persons and unidentified human remains, Parties shall allow other Parties' national contact points, as referred to in Article 8, access to the reference data in the automated fingerprint identification systems which they have established for that purpose, with the power to conduct automated searches by comparing dactyloscopic data. Searches may be conducted only in individual cases and in compliance with the requesting Party's national legislation.

(2) The confirmation of a match of dactyloscopic data with reference data held by the Party administering the file shall be carried out by the national contact point of the requesting Party by means of the automated supply of the reference data required for a hit.

Article 7
Supply of further personal data and other information

Should the procedures referred to in Articles 3 and 4 show a hit between DNA profiles or the procedures referred to in Article 6 show a hit between dactyloscopic data, the supply of further available personal data in addition to core personal data and other information relating to the reference data shall be governed by the national legislation, including the legal assistance rules, of the requested Party. Subject to Article 8 paragraph 2, the supply will be provided by a national contact point.

Article 8
National contact points

(1) For the purposes of the supply of data as referred to in Articles 3, 4 and 6, and subsequent supply of further available personal data and other information relating to the reference data, as referred to in Article 7, each Party shall designate national contact points. It shall indicate the national contact point, mentioned in Articles 3 and 4 for DNA data, the national contact point, mentioned in Article 6 for dactyloscopic data, the national contact point, mentioned in Article 9 for vehicle registration data and the national contact point, mentioned in Article 7 for personal data.

(2) The national contact point as referred to in Article 7 shall supply such subsequent personal data in accordance with the national legislation of the Party designating the responsible contact point. Other available legal assistance channels need not be used unless necessary in accordance with the national legislation, including the legal assistance rules, of the Parties.

Article 9
Automated searching of vehicle registration data

(1) For the prevention and investigation of criminal offences and to assist in the identification of missing persons and unidentified human remains and in dealing with other offences coming within the jurisdiction of the courts or the public prosecution service in the searching Party, as well as in maintaining public security, Parties shall allow other Parties' national contact points, access to the following national vehicle registration data, with the power to conduct automated searches in individual cases:

(a) data relating to owners or operators; and

(b) data relating to vehicles.

Searches may be conducted only with a full chassis number or a full registration number. Searches may be conducted only in compliance with the searching Party's national legislation.

(2) For the purposes of the supply of data as referred to in paragraph 1, each Party shall designate a national contact point for incoming requests. The powers of the national contact points shall be governed by the applicable national legislation. Details of technical arrangements for the procedure shall be laid down in a vehicle registration data User manual.

CHAPTER III
COMMON PROVISIONS ON THE FRAMEWORK FOR DATA EXCHANGE

Article 10
Principles of DNA and dactyloscopic data exchange

(1) The Parties shall use existing standards for DNA and dactyloscopic data exchange.

(2) The transmission procedure, in case of automated searching and comparison of DNA profiles and of dactyloscopic data shall take place within a decentralised structure.

(3) Appropriate measures shall be taken to ensure confidentiality and integrity for data being sent to other Parties, including their encryption.

(4) The Parties shall take the necessary measures to guarantee the integrity of the DNA profiles and dactyloscopic data made available or sent for comparison to the other Parties and to ensure that these measures comply with international standards.

Article 11
Technical and procedural specifications

(1) The Parties shall observe common technical specifications in connection with all requests and answers related to searches and comparisons of DNA profiles, dactyloscopic data and vehicle registration data.

(2) These technical and procedural specifications are laid down in the Implementing Agreement and User manuals.

CHAPTER IV
DATA PROTECTION

Article 12
Level of data protection

As regards the processing of personal data which are or have been supplied pursuant to this Agreement, each Party shall in its national legislation ensure an adequate level of protection of personal data essentially equivalent to the principles and standards enshrined in Directive (EU) 2016/680 and the relevant Council of Europe Convention and recommendations.

Article 13
Purpose

(1) Processing of personal data by the receiving Party shall be permitted solely for the purposes for which the data have been supplied in accordance with this Agreement. Processing for other purposes shall be permitted solely with the prior authorisation of the Party administering the file and subject only to the national legislation of the receiving Party. Such authorisation may be granted provided that processing for such other purposes is permitted under the national legislation of the Party administering the file.

(2) Processing of data supplied pursuant to Articles 3, 4 and 6 by the searching or comparing Party shall be permitted solely in order to:

(a) establish whether there is a match between the compared DNA profiles;

(b) establish whether there is a match between the compared dactyloscopic data;

(c) prepare and submit a police or judicial request for legal assistance in compliance with national legislation if there is a hit between those data via the national contact point designated in accordance with Articles 7 and 8;

(d) record within the meaning of Article 17.

(3) The Party administering the file may process the data supplied to it in accordance with Articles 3, 4 and 6 solely where this is necessary for the purposes of comparison, providing automated replies to searches or recording pursuant to Article 17. The supplied data shall be deleted immediately following data comparison or automated replies to searches unless further processing is necessary for the purposes mentioned under points (b) and (c) of the second paragraph.

(4) Data supplied in accordance with Article 9 may be used by the Party administering the file solely where this is necessary for the purpose of providing automated replies to search procedures or recording as specified in Article 17. The data supplied shall be deleted immediately following automated replies to searches unless further processing is necessary for recording pursuant to Article 17. The searching Party may use data received in a reply solely for the procedure for which the search was made.

Article 14
Competent authorities

Personal data supplied may be processed only by the competent law enforcement authorities with responsibility for a task in furtherance of the aims mentioned in Article 13. In particular, data may be supplied to other entities only with the prior authorisation of the supplying Party and in compliance with the national legislation of the receiving Party.

Article 15
Accuracy, current relevance and storage time of data

(1) The Parties shall ensure the accuracy and current relevance of personal data. Should it transpire ex officio or from a notification by the data subject that incorrect data or data which should not have been supplied have been supplied, this shall be notified without delay to the receiving Party or Parties. The Party or Parties concerned shall be obliged to correct or delete the data. Moreover, personal data supplied shall be corrected if they are found to be incorrect. If the receiving body has reason to believe that the supplied data are incorrect or should be deleted the supplying body shall be informed forthwith.

(2) Data, the accuracy of which the data subject contests and the accuracy or inaccuracy of which cannot be established shall, in accordance with the national legislation of the Parties, be marked with a flag at the request of the data subject. If a flag exists, this may be removed subject to the national legislation of the Parties and only with the permission of the data subject or based on a decision of the competent court or independent data protection authority.

(3) Personal data supplied which should not have been supplied or received shall be deleted. Data which are lawfully supplied and received shall be deleted:

(a) if they are not or no longer necessary for the purposes for which they were supplied; if personal data have been supplied without request, the receiving body shall immediately check if they are necessary for the purposes for which they were supplied;

(b) following the expiry of the maximum period for keeping data laid down in the national legislation of the supplying Party where the supplying body informed the receiving body of that maximum period at the time of supplying the data.

Where there is reason to believe that deletion would prejudice the interests of the data subject, the data shall be kept in accordance with the national legislation.

Article 16
Technical and organisational measures to ensure data protection and data security

(1) The supplying and receiving bodies shall take steps to ensure that personal data is effectively protected against accidental or unauthorised destruction, accidental loss, unauthorised access, unauthorised or accidental alteration and unauthorised disclosure.

(2) The features of the technical specification of the automated search procedure are regulated in the implementing measures as referred to in Article 20 which guarantee that:

(a) state-of-the-art technical measures are taken to ensure data protection and data security, in particular data confidentiality and integrity;

(b) encryption and authorisation procedures recognised by the competent authorities are used when having recourse to dedicated networks; and

(c) the admissibility of searches in accordance with Article 17(2), (4) and (5) can be checked.

Article 17
Logging and recording: special rules governing automated and non-automated supply

(1) Each Party shall guarantee that every non-automated supply and every non-automated receipt of personal data by the body administering the file and by the searching body is logged in order to verify the admissibility of the supply. Logging shall contain the following information:

(a) the reason for the supply;

(b) the data supplied;

(c) the date of the supply; and

(d) the name or reference code of the searching body and of the body administering the file.

(2) The following shall apply to automated searches for data based on Articles 3, 4 and 6 and Article 9:

(a) only specially authorised officers may carry out automated searches or comparisons. The list of officers authorised to carry out automated searches or comparisons shall

be made available upon request to the supervisory authorities referred to in paragraph 5 and to the other Parties;

(b) each Party shall ensure that each supply and receipt of personal data by the body administering the file and the searching body is recorded, including notification of whether or not a match exists. Recording shall include the following information:

(i) the data supplied;

(ii) the date and exact time of the supply; and

(iii) the name or reference code of the searching body and of the body administering the file.

The searching body shall also record the reason for the search or supply as well as an identifier for the official who carried out the search and the official who ordered the search or supply.

(3) The recording body shall immediately communicate the recorded data upon request to the competent data protection authorities of the relevant Party at the latest within four weeks following receipt of the request. Recorded data may be used solely for the following purposes:

(a) monitoring data protection;

(b) ensuring data security.

(4) The recorded data shall be protected with suitable measures against inappropriate use and other forms of improper use and shall be kept for two years. After the conservation period the recorded data shall be deleted immediately.

(5) Responsibility for legal checks on the supply or receipt of personal data lies with the independent data protection authorities or, as appropriate, the judicial authorities of the respective Parties. Anyone can request these authorities to check the lawfulness of the processing of data in respect of their person in compliance with national legislation. Independently of such requests, these authorities and the bodies responsible for recording shall carry out random checks on the lawfulness of supply, based on the files involved.

(6) The results of such checks shall be kept for inspection for 18 months by the independent data protection authorities. After this period, they shall be immediately deleted. Each data protection authority may be requested by the independent data protection authority of another Party to exercise its powers in accordance with national legislation. The independent data protection authorities of the Parties shall perform the inspection tasks necessary for mutual cooperation, in particular by exchanging relevant information.

Article 18
Data subjects' rights to information and damages

(1) At the request of the data subject under national legislation, information shall be supplied in compliance with national legislation to the data subject upon production of proof of identity, without unreasonable expense, in general comprehensible terms and without unacceptable delays, on the data processed in respect of the person, the origin of the data,

the recipient or groups of recipients, the intended purpose of the processing and, where required by national legislation, the legal basis for the processing. Moreover, the data subject shall be entitled to have inaccurate data corrected and unlawfully processed data deleted. The Parties shall also ensure that, in the event of violation of the rights in relation to data protection, the data subject shall be able to lodge an effective complaint to an independent court or a tribunal within the meaning of Article 6(1) of the European Convention on Human Rights or an independent data protection authority established by national legislation according to the standards essentially equivalent to Directive (EU) 2016/680 and the relevant Council of Europe Convention and recommendations and that the data subject is given the possibility to claim for damages or to seek another form of legal compensation. The detailed rules for the procedure to assert these rights and the reasons for limiting the right of access shall be governed by the relevant national legislation of the Party where the data subject asserts these rights.

(2) Where a body of one Party has supplied personal data under this Agreement, the receiving body of the other Party cannot use the inaccuracy of the data supplied as grounds to evade its liability vis-à-vis the injured Party under national legislation. If damages are awarded against the receiving body because of its use of inaccurate transfer data, the body which supplied the data shall refund the amount paid in damages to the receiving body in full.

Article 19
Information requested by the Parties

The receiving Party shall inform the supplying Party on request of the processing of supplied data and the result obtained.

CHAPTER V
FINAL PROVISIONS

Article 20
Implementing Agreement and User manuals

(1) On the basis and within the scope of this Agreement, the Parties shall conclude an agreement for its implementation.

(2) User manuals shall be prepared and kept up to date by expert working groups composed of representatives of the Parties. User manuals contain administrative and technical information needed for efficient and effective exchange of data.

Article 21
Evaluation of the data exchange

(1) An evaluation of the administrative, technical and financial application of the data exchange pursuant to Chapter II of this Agreement shall be carried out. The evaluation must be carried out before starting the data exchange. If needed, the evaluation can be repeated

for those Parties already applying this Agreement. The evaluation shall be carried out with respect to the data categories for which data exchange has started among the Parties concerned. The evaluation shall be based on reports of the respective Parties.

(2) The evaluation shall be carried out by a joint working group made up of representatives of the Parties. The working group shall meet at the request of a Party or on a regular basis every five years.

Article 22
Relationship with other international agreements

(1) This Agreement shall not affect any rights, obligations and responsibilities of the Parties arising from other international agreements to which they are parties.

(2) Unless otherwise stipulated explicitly in this Agreement, cooperation shall be performed within the scope of the respective national legislation of the Parties.

Article 23
Implementation and Application

(1) The Parties shall inform the Depositary that they have implemented the obligations imposed on them under this Agreement and designated national contact points according to this Agreement.

(2) Once a positive evaluation of a Party in the context of this Agreement (Article 21) or the European Union has been made, the respective Party is entitled to apply this Agreement immediately in relation to all other Parties which also have been evaluated positively. The respective Party shall inform the Depositary accordingly.

(3) Declarations submitted in accordance with paragraph 1 of this Article may be amended at any time.

Article 24
Depositary

(1) Depositary of this Agreement is the Republic of Serbia.

(2) The Depositary shall send a certified copy of this Agreement to each Party.

(3) The Depositary shall notify the Parties of the deposit of any instrument of ratification, acceptance, approval or accession, of any declarations, statements or notifications made in connection with this Agreement.

(4) The Depositary shall notify all Parties on any date of entry into force of this Agreement in accordance with Article 26.

Article 25
Ratification, Acceptance, Approval, Accession or Reservation

(1) This Agreement is subject to ratification, acceptance, or approval of the Parties. The instruments of ratification, acceptance or approval shall be deposited with the Depositary.

(2) This Agreement shall be open for accession by any PCC SEE Party. The instrument of accession shall be deposited with the Depositary.

(3) No reservations may be made to this Agreement.

Article 26
Entry into Force

(1) This Agreement shall enter into force on the sixtieth day following the date of the deposit of the second instrument of ratification, acceptance, approval, or accession.

(2) For each Party ratifying, accepting, approving, or acceding to this Agreement after the deposit of the second instrument of ratification, acceptance, approval, or accession, the Agreement shall enter into force on the sixtieth day after deposit by such Party of its instrument of ratification, acceptance, approval, or accession.

Article 27
Withdrawal and Suspension

(1) This Agreement shall be concluded for an indefinite period of time.

(2) Any Party may withdraw from this Agreement at any time by written notification to the Depositary. The withdrawal shall take effect six months after the date of receipt of the notification by the Depositary.

(3) Regardless of the termination of this Agreement the provisions laid down in Chapter IV shall apply regarding the processed data.

(4) Any Party may suspend the operation of this Agreement in full or in part if necessary for reasons of public order, protection of national security or protection of public health. The Parties shall notify the Depositary without delay of taking or revoking such a measure. Any measure taken under this paragraph shall take effect 15 days after the date of receipt of the notification by the Depositary.

(5) The Depositary shall inform other Parties of the notification of withdrawal or suspension without delay.

In witness whereof the undersigned, being duly authorised have signed this Agreement:

For the Republic of Albania

For the Republic of Austria

For Bosnia and Herzegovina

For the Republic of Bulgaria

For Hungary

For the Republic of Macedonia

For the Republic of Moldova

For Montenegro

For Romania

For the Republic of Serbia

For the Republic of Slovenia

Done in Vienna, on …….. 2018, in a single original copy in the English language.