Council of the European Union

Brussels, 5 February 2019
(OR. fr)

6102/19
ADD 1

JAI 100
COPEN 43
CYBER 34
DROIPEN 16
JAIEX 8
ENFOPOL 45
DAPIX 41
EJUSTICE 14
MI 111
TELECOM 50
DATAPROTECT 27
USA 8
RELEX 97

COVER NOTE

From:	Secretary-General of the European Commission, signed by Mr Jordi AYET PUIGARNAU, Director
date of receipt:	5 February 2019
To:	Mr Jeppe TRANHOLM-MIKKELSEN, Secretary-General of the Council of the European Union
No. Cion doc.:	COM(2019) 70 final - ANNEX
Subject:	ANNEX to the Recommendation for a COUNCIL DECISION authorising the opening of negotiations in view of an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters

Delegations will find attached document COM(2019) 70 final - ANNEX.

Encl.: COM(2019) 70 final - ANNEX

EUROPEAN
COMMISSION

Brussels, 5.2.2019
COM(2019) 70 final

ANNEX

ANNEX

to

the Recommendation for a COUNCIL DECISION

authorising the opening of negotiations in view of an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters

ANNEX

1. OBJECTIVES

The Commission should, in the course of the negotiations, aim to achieve the specific objectives set out in detail below, while ensuring that the outcome of the negotiations is compatible with the Union's internal rules on electronic evidence, including as they evolve in the legislative procedure by the Union co-legislators and eventually in their final adopted form. These internal rules will serve as the baseline for the Union's negotiating position.

1. Set common rules and address conflicts of law for orders for obtaining electronic evidence in the form of content and non-content data, from a judicial authority in one contracting party, addressed to a service provider that is subject to the law of the other contracting party. This should reduce the risk of fragmentation of practices and legal rules and enhance legal certainty between the Union and the United States of America when obtaining electronic evidence in criminal proceedings.

2. Allow for a transfer of electronic evidence directly on a reciprocal basis by a service provider to a requesting authority as set out in paragraph 1.

3. Ensure respect for the fundamental rights, freedoms and general principles of EU law as enshrined in the European Union Treaties and Charter of Fundamental Rights, including proportionality, procedural rights, the presumption of innocence and the rights of defence of persons subject to criminal proceedings as well as privacy and the protection of personal data and communications data when such data is processed, including transfers to law enforcement authorities in third countries, and any obligations incumbent on law enforcement and judicial authorities in this respect.

To achieve the objectives set out in part 1, the agreement should address in particular the following elements:

2. NATURE AND SCOPE OF THE AGREEMENT

4. The agreement should apply to criminal proceedings which include both pre-trial and trial phases.

5. The agreement should create reciprocal rights and obligations of the parties.

6. The agreement should set out the definitions and types of data that are to be covered, including both content and non-content data.

7. The agreement should define its exact scope of application in terms of the criminal offences covered and the thresholds.

8. The agreement should set out what the conditions are to be met before a judicial authority can issue an order and the ways in which an order can be served.

9. The agreement should include a clause enabling effective judicial remedies for data subjects during criminal proceedings. The agreement should also define in which circumstances a service provider has the right to object to an order.

10. The agreement should define the time period for supplying the data covered by the order.

11. It should be without prejudice to other existing international agreements on judicial cooperation in criminal matters between authorities, such as the EU-U.S. Mutual Legal Assistance Agreement.

12. The agreement should, in the bilateral relations between the Union and the United States of America, take precedence over the Council of Europe Convention on Cybercrime and any agreement or arrangement reached in the negotiations of the Second Additional Protocol to the Council of Europe Convention on Cybercrime, in so far as the provisions of the latter agreement or arrangement cover issues dealt with by the agreement.

3. SAFEGUARDS

13. The agreement should be reciprocal in terms of the categories of persons whose data must not be requested pursuant to this agreement. The agreement should not discriminate between persons from different Member States.

14. The agreement should make applicable by reference the EU-U.S. Data Protection and Privacy Agreement, otherwise known as the "Umbrella Agreement", which entered into force on 1 February 2017.

15. The agreement should complement the Umbrella Agreement with additional safeguards that take into account the level of sensitivity of the categories of data concerned and the unique requirements of the transfer of electronic evidence directly by service providers rather than between authorities.

16. The additional privacy and data protection safeguards, to be reviewed subject to the scope of the agreement, should include inter alia:

    (a) The specification of the purposes for which personal data and electronic communications data may be requested and transferred.

    (b) The requirement that the order is limited to personal data and electronic communications data that is necessary and proportionate in relation to the purposes for which they are accessed.

    (c) The requirement that use by and disclosure to other U.S. authorities not bound by the Umbrella Agreement is subject to notification to, and prior authorisation by the competent judicial authority designated in the Member State in which the service provider is established or represented and may only take place if it is ensured that the receiving authority effectively protects the personal data and electronic communications data in line with the provisions of the agreement. When considering such prior authorisation, the competent judicial authority should take due account of all relevant factors, including the seriousness of the offence and the purpose for which the data is initially transferred.

    (d) The requirement that onward transfers to other third countries may only be made to law enforcement authorities responsible for the prevention, investigation, detection or prosecution of criminal offenses, including terrorism, and should be subject to notification to, and prior authorisation by the competent judicial authority designated by the Member State in which the service provider is established or represented. When considering such prior authorisation, the competent judicial authority should take into account the factors as set out in Article 7(2) of the Umbrella Agreement.

(e) The agreement may consider the exceptional circumstances and the safeguards required where onward transfer may take place without prior authorisation, in case of serious and imminent threat to public security of a Member State or a third country.

(f) The notification of an information security incident to the competent authority designated by the Member State in which the service provider is established or represented shall be made under the conditions of Article 10(2) of the Umbrella Agreement.

17. The additional procedural rights safeguards, to be reviewed subject to the scope of the agreement, should include inter alia:

(a) The appropriate safeguards to ensure that data may not be requested for the use in criminal proceedings that could lead to the death penalty.

(b) The adequate conditions to ensure necessity and proportionality of orders for access to electronic evidence, distinguishing in particular between data categories as appropriate.

(c) The procedural safeguards for individuals subject to a data order in the framework of criminal proceedings.

(d) The specific safeguards for data protected by privileges and immunities,

(e) The confidentiality safeguards for authorities and service providers, including non-disclosure requirements.

4. GOVERNANCE OF THE AGREEMENT

18. The agreement should stipulate that the parties shall undertake periodic joint reviews of application of the agreement and examine how to make most effective use thereof. For this purpose, statistics should be collected on both sides to facilitate this process.

19. The agreement should include a clause on its duration. Whether the duration is to be indefinite or definite shall be assessed in the light of the results of negotiation. In either case, a provision should be included requiring a review of the agreement in due course.

20. The agreement should stipulate that the parties should consult each other to facilitate resolution of any dispute regarding interpretation or application of the agreement.

21. The agreement should provide for the possibility of suspension and termination of the agreement by either Party in the event that the above-mentioned consultation procedure is unable to resolve the dispute.

22. The agreement should include a clause addressing its territorial application.

23. The agreement will be equally authentic in all official Union languages.