EUROPEAN
COMMISSION

Brussels, 5.2.2019
COM(2019) 70 final

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

EXPLANATORY MEMORANDUM

1. CONTEXT

Cross-border data flows are rising together with the growing use of social media, webmail, messaging services and apps to communicate, work, socialise and obtain information, including for unlawful purposes. An increasing number of criminal investigations therefore rely on electronic evidence that is not publicly available. The borderless nature of the internet and the way services can be provided from all over the world, including by non-European companies, means that facilitating cross-border access to electronic evidence is a pressing issue concerning almost any type of crime. In particular, the recent terrorist attacks have underlined the need, as a matter of priority, to find ways for European Union Member State prosecutors and judges to secure and obtain electronic evidence more quickly and effectively.

More than half of all criminal investigations today require access to cross-border electronic evidence. Electronic evidence is needed in around 85% of criminal investigations, and in two-thirds of these investigations there is a need to obtain evidence from online service providers based in another jurisdiction. The number of requests to the main online service providers grew by 84% in the period between 2013 and 2018. These types of data are essential in criminal investigations to identify a person or to obtain information about their activities.

Electronic evidence refers to various types of data in electronic form that are relevant in investigating and prosecuting criminal offences, and are often stored on the servers of online service providers. This includes 'content data' such as e-mails, text messages, photographs and videos as well as 'non-content data', such as subscriber data or traffic information regarding an online account.

Cooperation between judicial authorities is the traditional method for authorities to work together to tackle all types of crime. Today, the main instrument that Member States use to request access to cross-border electronic evidence in most other European Union countries is the European Investigation Order.

European Union Member States have recourse to Mutual Legal Assistance requests with third countries (and Denmark and Ireland who do not participate in the European Investigation Order). Several different authorities are involved on both sides. The procedures were designed at a time before the internet, when volumes of requests were a fraction of today's, and they did not face the volatility of electronic evidence.

One of the main recipients of Mutual Legal Assistance (MLA) requests from European Union Member States (and from around the world) for access to electronic evidence is the United States of America, where the largest service providers are headquartered. An agreement on Mutual Legal Assistance between the European Union and the United States of America was signed on 25 June 2003 and entered into force on 1 February 2010. The agreement is a key transatlantic mechanism for ensuring effective cooperation in the field of criminal justice and combatting organised crime and terrorism.

A first joint review of the agreement took place in 2016[1]. This concluded that the agreement adds value to the EU-U.S. Mutual Legal Assistance relationship and generally works well. Further efforts will be made to improve this cooperation. While judicial cooperation between public authorities, including with the United States of America, is crucial, this method is often too slow, when taking into account the volatile nature of electronic evidence, taking an average of 10 months, and can entail a disproportionate expense of resources. Moreover,

[1] Review of the 2010 EU-U.S. Mutual Assistance Agreement, 7 April 2016, 7403/16.

whereas sovereignty is an important aspect in judicial cooperation in a particular investigation, it is becoming increasingly common that the only connection to another state is the location of the data or the service provider. Specifically on electronic evidence, the 2016 joint review encouraged Member States to cooperate directly with U.S. service providers in order to secure and obtain electronic evidence more quickly and effectively.

Direct cooperation with U.S. service providers has developed as an alternative channel to judicial cooperation. It is limited to non-content data[2] and is voluntary from the perspective of U.S. law. In practical terms, the public authorities of the European Union Member State directly contact a service provider in the United States of America with requests pursuant to national rules of criminal procedure to which the service provider has access, typically data on a user of the services it provides. This concerns some service providers established in the United States of America and, to a more limited extent, in Ireland, which reply directly to requests from Member States' law enforcement authorities on a voluntary basis, as far as the requests concern non-content data.

U.S. law[3] allows U.S.-based service providers to cooperate directly with European public authorities with regard to non-content data. However, this cooperation is voluntary. Thus, providers have created their own policies or decide on a case-by-case basis on whether and how to cooperate. In addition to the increase in direct cooperation with service providers, recent rulings and court cases in the United States of America sought to clarify whether U.S. authorities have the right to request the production of data stored abroad by a service provider whose main seat is in the United States of America, including notably the "Microsoft Ireland" case[4].

The scale of direct cooperation requests on a voluntary basis has rapidly increased with more than 124 000 in 2017. While ensuring faster access compared to Mutual Legal Assistance, direct cooperation on a voluntary basis is limited to non-content data. Moreover, it can be unreliable, it may not ensure respect of the appropriate procedural safeguards, is only possible with a limited number of service providers which all apply different policies, is not transparent and lacks accountability. The resulting fragmentation may generate legal uncertainty, raise questions on the legality of prosecution as well as concerns on the protection of fundamental rights and procedural safeguards for the persons related to such requests. In addition, less than half of all the requests to service providers are fulfilled[5].

As regards possible reciprocal requests by U.S. authorities to service providers in the European Union, in many Member States the telecommunications legal framework currently prohibits national telecommunications providers from responding directly to requests from foreign authorities, including for non-content data. In addition, there is no legal framework allowing direct cooperation in other communication sectors. U.S. authorities can usually only obtain such data from EU service providers through a Mutual Legal Assistance request.

---

2 Content data may only be obtained on a voluntary basis in cases considered to be an emergency involving danger of death or serious physical injury to any person.

3 Section 2701(2) of the Electronic Communications and Privacy Act 1986 (ECPA) 41.

4 The case was heard by the US Supreme Court on February 27 2018. The Court dismissed the case on 17 April 2018, after being informed by the parties that the CLOUD Act had been signed into law enabling a new warrant to be issued to obtain the requested information from Microsoft.

5 Commission Impact Assessment accompanying the electronic evidence package, 17 April 2018, SWD(2018) 118 final.

2. OBJECTIVES OF THE PROPOSAL

The European Commission committed in the April 2015 European Agenda on Security[6] to review obstacles to criminal investigations into cyber-enabled crimes, notably on cross-border access to electronic evidence. On 17 April 2018, the Commission proposed to the European Parliament and the Council a Regulation on European Production and Preservation orders for electronic evidence in criminal matters[7] and a Directive laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings ("e-evidence proposals")[8].

The purpose of these proposals is to speed up the process in the European Union to secure and obtain electronic evidence directly from service providers established in another jurisdiction. The scope of the proposals includes specific types of service providers that are providing services in the European Union. A provider is offering services in the European Union when it enables users in one or more Member States to use its services and where it has a substantial connection to the Union, for instance when it has an establishment in a Member State or because it provides services to a large number of users in that Member State. Those without a presence in the European Union are obliged to appoint a legal representative against whom production orders can be enforced.

The European Council has stressed the importance of this issue both internally and externally. The European Council Conclusions of 18 October 2018 state that "*Solutions should be found to ensure swift and efficient cross-border access to electronic evidence in order to effectively fight terrorism and other serious and organised crime, both within the EU and at international level; the Commission proposals on electronic evidence and access to financial information, as well as to better combat money laundering, should be agreed on by the end of the legislature*[9]. *The Commission should also urgently submit negotiating mandates for the international negotiations on electronic evidence*".

The Commission's e-evidence proposals provide the basis for a coordinated and coherent approach both within the European Union and by the European Union at international level, with due regard to European Union rules, including on non-discrimination between European Union Member States and their nationals. While the Commission, in its Impact Assessment for the e-evidence proposals, already noted that the proposals could usefully be complemented by bilateral or multilateral agreements on cross-border access to electronic evidence with accompanying safeguards, the Commission decided to propose EU rules on the appropriate modalities and safeguards for cross-border access to electronic evidence, before engaging in negotiations with third parties.

At the international level, discussions are taking place as part of the negotiations on a Second Additional Protocol to the Council of Europe Convention on Cybercrime[10]. Cross-border

---

6 Communication from the Commission to the European Parliament and Council: The European Agenda on Security, 28 April 2015, COM(2015) 185 final.

7 Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, 17 April 2018, COM(2018) 225 final.

8 Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, 17 April 2018, COM(2018) 226 final.

9 While negotiations with the European Parliament and the Council are ongoing, the Council agreed a general approach on the Commission proposal for a Regulation at the Justice and Home Affairs Council on 7 December 2018.

10 Council of Europe Budapest Convention on Cybercrime (CETS N° 185), 23 November 2001, http://conventions.coe.int

access to electronic evidence has been a regular point on recent EU-U.S. Justice and Home Affairs Ministerial meetings.

The two recommendations to open negotiations with the United States of America and to participate in the negotiations of the Second Additional Protocol to the Council of Europe Convention on Cybercrime are being adopted by the Commission at the same time. While the two processes will progress at a different pace, they address inter-linked issues and commitments taken in one negotiation may have a direct impact on other strands of negotiations.

While the e-evidence proposals address the situation of specific types of service providers providing services on the EU market, there is a risk of conflicting obligations with laws in third countries. In order to address these conflicts of law, and in line with the principle of international comity, the e-evidence proposals include provisions for specific mechanisms in case a service provider is confronted with conflicting obligations deriving from the law of a third country when evidence is requested. These mechanisms include a review procedure to clarify such a situation. An EU-U.S. Agreement should aim to avoid conflicting obligations between the European Union and the United States of America.

Major service providers holding relevant evidence for criminal investigations operate under U.S. jurisdiction. The Stored Communications Act of 1986 prohibited the disclosure of content data, whereas non-content data can be provided on a voluntary basis. The United States CLOUD Act (Clarifying Lawful Overseas Use of Data), adopted by United States Congress on 23 March 2018, clarifies through an amendment of the Stored Communications Act of 1986 that U.S. service providers are obliged to comply with U.S. orders to disclose content and non-content data, regardless of where such data is stored, including in the European Union. The CLOUD Act also allows the conclusion of executive agreements with foreign governments, on the basis of which U.S. service providers would be able to deliver content data directly to these foreign governments. The scope of data covered by the CLOUD Act is stored data and interception of wire or electronic communication, while the offences covered are “serious crimes”. The executive agreements with foreign governments are subject to certain conditions, that the foreign country has sufficient protections in place, including to restrict access to data related to U.S. citizens.

The purpose of this initiative is to address, through common rules, the specific legal issue of access to content and non-content data held by service providers in the European Union or the United States of America. This initiative would, in the context of an international agreement, complement the EU’s electronic evidence proposals by addressing conflicts of law, in particular as regards content data and speeding up access to electronic evidence. This recommendation includes negotiating directives for the opening of negotiations on an EU-wide agreement with the United States of America on cross-border access to electronic evidence. The European Union has an interest in a comprehensive agreement with the United States of America, both from the perspective of protecting European rights and values such as privacy and personal data protection and from the perspective of our own security interests.

In terms of content data, as outlined above, U.S. law (Stored Communications Act of 1986) as it currently stands, bars U.S. service providers from responding to requests from foreign law enforcement authorities. U.S. law currently requires that probable cause be shown before a Mutual Legal Assistance request from a third country can be executed. European Union Member State service providers cannot currently respond to direct requests from third country authorities. An EU-U.S. Agreement would complement the objective and the effectiveness of the e-evidence proposals, in particular when it comes to content data held by U.S. service providers in the United States of America. It would allow direct cooperation with a service

provider by creating a more efficient legal framework for judicial authorities as EU practitioners currently face difficulties in obtaining content data through Mutual Legal Assistance requests.

As regards non-content data, due to the growing number of Mutual Legal Assistance requests addressed to the United States of America, the U.S. authorities have encouraged EU law enforcement and judicial authorities to request non-content data from U.S. service providers directly, and U.S. law allows but does not require U.S.-based service providers to respond to such requests. An EU-U.S. Agreement would provide more certainty, clear procedural safeguards and reduce fragmentation for EU authorities to access non-content data held by U.S. service providers. It would also allow for reciprocal access by U.S. authorities to data held by EU service providers.

The recommendation for a Council decision is to launch negotiations between the European Union and the United States of America, so that a transatlantic agreement can be reached on cross-border access to electronic evidence directly from service providers for use in criminal proceedings. It seeks to adapt cooperation mechanisms to the digital age, giving the judiciary and law enforcement tools to address the way criminals communicate today and to counter modern forms of criminality.

An agreement between the European Union and the United States would offer a number of practical advantages:

- It would provide for reciprocal access for judicial authorities to content data;
- It would address access to non-content data on the basis of orders from judicial authorities, ensure reciprocal access by EU and U.S. authorities and review the conditions and safeguards for direct cooperation to service providers;
- It would contribute to improving timely access to data for judicial authorities;
- It would address the risk of conflicts of laws;
- It would reduce the risk of fragmentation of rules, procedures, and harmonise the rights and safeguards through a single negotiation mandate for all European Union Member States with the United States ensuring non-discrimination between European Union Member States and their nationals;
- It would clarify the binding nature and enforcement of orders on service providers while also detailing the obligations for judicial authorities.

The agreement should be conditional on strong protection mechanisms for fundamental rights. These negotiating directives aim to improve legal certainty for authorities, service providers and persons affected, ensuring proportionality, protection of fundamental rights, transparency and accountability of both judicial authorities and service providers.

3. RELEVANT PROVISIONS IN THE POLICY AREA

The current European Union legal framework consists of Union cooperation instruments in criminal matters, such as the Directive 2014/41/EU regarding the European Investigation Order in criminal matters[11] (EIO Directive), the Convention on Mutual Assistance in Criminal

[11] Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, OJ L 130, 1.5.2014, p.1.

Matters between the Member States of the European Union[12], Regulation 2018/1727 on Eurojust[13], Regulation (EU) 2016/794 on Europol[14], Council Framework Decision 2002/465/JHA on joint investigation teams[15] and the proposed Regulation on preventing the dissemination of terrorist content online[16].

On 17 April 2018, the Commission proposed to the Council and the European Parliament a Regulation on European Production and Preservation orders for electronic evidence in criminal matters[17] and a Directive laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings[18]. Externally, the European Union has concluded a number of bilateral agreements between the Union and third countries, such as the Agreement on Mutual Legal Assistance ('MLA') between the European Union and the United States of America[19]. This agreement is intended as a complement to these arrangements.

Personal data covered by this recommendation for a Council decision is protected and may only be processed in accordance with the General Data Protection Regulation (GDPR)[20] and for authorities in the European Union, the Data Protection Directive for Police and Criminal Justice Authorities (Law Enforcement Data Protection Directive)[21]. The agreement should complement the EU-U.S. Data Protection and Privacy Agreement, otherwise known as the "Umbrella Agreement" which entered into force on 1 February 2017 and the U.S. Judicial Redress Act (JRA), extending the benefits of the U.S. Privacy Act to EU citizens that was adopted by the United States Congress on 24 February 2016.

---

12 Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union.

13 Regulation (EU) 2018/1727 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for Criminal Justice Cooperation (Eurojust), and replacing and repealing Council Decision 2002/187/JHA.

14 Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA.

15 Council Framework Decision 2002/465/JHA of 13 June 2002 on joint investigation teams.

16 Proposal for a Regulation on preventing the dissemination of terrorist content online, 12 September 2018, COM(2018) 640 final

17 Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, 17 April 2018, COM(2018) 225 final

18 Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, 17 April 2018, COM(2018) 226 final.

19 Council Decision 2009/820/CFSP of 23 October 2009 on the conclusion on behalf of the European Union of the Agreement on extradition between the European Union and the United States of America and the Agreement on mutual legal assistance between the European Union and the United States of America.

20 Regulation (EU) 2016/679 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 and on the free movement of such data, and repealing Directive 95/46/EC.

21 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.

Electronic communications data covered by this recommendation for a Council decision is protected and can only be processed in accordance with the Directive 2002/58/EC (the ePrivacy Directive)[22].

The agreement should respect the fundamental rights, freedoms and general principles of EU law as enshrined in the European Union Treaties and Charter of Fundamental Rights, procedural rights including right to an effective remedy and to a fair trial, presumption of innocence and right of defence, principles of legality and proportionality of criminal offences and penalties and any obligations incumbent on law enforcement or judicial authorities in this respect. As regards the necessary data protection safeguards for personal data transferred from the European Union to U.S. law enforcement authorities, the applicable provisions of the EU-U.S. Data Protection and Privacy Agreement will be complemented by additional safeguards to 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.

The agreement should also 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. The agreement should, in the bilateral relations between the United States of America and the European Union, take precedence over any agreement or arrangement reached in the negotiations of the Second Additional Protocol to the Council of Europe Convention on Cybercrime.

The Council shall authorise the opening of negotiations, adopt negotiating directives and authorise the signing and conclusion of the agreement as set out in Article 218 (3) and (4) of the Treaty on the Functioning of the European Union.

Fundamental rights

The agreement could potentially affect a number of fundamental rights:

- rights of the individual whose data is accessed: including right to protection of personal data; right to respect of private and family life, home and communications; right to freedom of expression and assembly; right to an effective remedy and to a fair trial, presumption of innocence and right of defence, principles of legality and proportionality of criminal offences and penalties;
- rights of the service provider: right to freedom to conduct a business; right to an effective remedy;
- rights to liberty and security of persons.

Taking into account the relevant privacy and data protection acquis, sufficient and important safeguards should be included in the agreement to ensure that the rights of these persons are protected in line with general principles of EU law and relevant case law of the European Court of Justice.

[22] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p.37), amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws.

The EU-U.S. Agreement should be compatible with the Commission's e-evidence proposals, including as they evolve in the legislative procedure and in their final adopted form.

The definitions of criminal proceedings for which such data could be obtained, the types of data covered, the requirements to issue an order, the judicial remedies and safeguards, and the scope of offences concerned will form an important part of the negotiations in order to avoid conflicts of law and improve access for authorities. The definitions and scope should be compatible with those of the EU-internal electronic evidence rules as they evolve.

The Commission believes that it is in the interest of both the European Union and United States of America to conclude a comprehensive agreement as this would provide legal clarity for judicial and law enforcement authorities from both sides and avoid conflicting legal obligations for service providers. This is also the only way to avoid that we have different rules for EU citizens and service providers depending on their nationality.

The agreement should clarify the binding nature and enforcement of orders on service providers, while the agreement should also define the obligations for judicial authorities.

In point 1 - 3 of the negotiating directives, the Commission proposes the three main objectives of the agreement, namely to set common rules and address conflicts of law for orders on 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 another contracting party; secondly, on the basis of such an order, to allow for a transfer of electronic evidence directly on a reciprocal basis by a service provider to a requesting authority and thirdly, 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.

In point 4 of the negotiating directives, the Commission proposes that the agreement should apply to criminal proceedings which include both pre-trial and trial phases. It should be compatible with Article 3 of the proposed Regulation on European Production and Preservation Orders for electronic evidence in criminal matters. Both during the pre-trial and trial phase, all legal protections for the affected persons and in particular, criminal law procedural safeguards are applicable.

With point 5 of the negotiating directives, the Commission proposes that the agreement should create reciprocal rights and obligations of the parties to the agreement.

In point 6 of the negotiating directives, the Commission proposes that the agreement sets out the definitions and types of data that are to be covered, including both content and non-content data. Content data includes the content of the electronic exchange and is considered the most intrusive category of electronic evidence. Non-content data encompasses both subscriber data, which is the most frequently requested type of data for the purposes of criminal investigations, and traffic data which includes information on the identities of the senders and recipients of electronic messages and metadata including the timing, frequency and duration of the exchanges.

In point 7 of the negotiating directives, the Commission proposes that the agreement should define its exact scope of application in terms of the criminal offences covered and the thresholds of levels of penalties. It should be compatible with Article 5 (4) of the proposed Regulation on European Production and Preservation Orders for electronic evidence in criminal matters. The issuing authority should be required to ensure in the individual case that the measure is necessary and proportionate, including in view of the gravity of the offence

under investigation. The agreement should include appropriate thresholds of levels of penalties for content and non-content data. It should be compatible with the three-year threshold, which limits the scope of the instrument to more serious crimes, without excessively limiting the possibilities of its use by practitioners.

The Commission proposes in point 8 of the negotiating directives that the agreement should set out what are the conditions to be met before a judicial authority can issue an order and the ways in which an order can be served. It should be compatible with Article 5 on conditions for issuing an order of the proposed Regulation on European Production and Preservation Orders for electronic evidence in criminal matters.

In point 9 of the negotiating directives, the Commission proposes that the agreement should include a clause enabling effective judicial remedies for suspects and accused persons during the criminal proceedings. The agreement should also define in which circumstances a service provider has the right to object to an order. For affected persons, the baseline for these provisions are Article 17 of the proposed Regulation on European Production and Preservation Orders for electronic evidence in criminal matters which ensures that persons affected by the European production order have effective remedies in accordance with national law, normally during the criminal proceedings. Remedies of data subjects are also defined in in Directive (EU) 2016/680 and Regulation (EU) 2016/679. As the order is a binding measure, it may also affect the rights of service providers, in particular the freedom to conduct a business and the conditions for this. The Commission proposes that the agreement should include a right for the service provider to raise certain claims in the issuing State, for example if the order has not been issued or validated by a judicial authority.

In point 10 of the negotiating directives, the Commission proposes that the agreement should define the time period for supplying the data covered by the order. It should be compatible with Article 9 of the proposed Regulation on European Production and Preservation Orders for electronic evidence in criminal matters which obliges addressees to reply in a normal deadline of 10 days, while authorities may set a shorter deadline where justified.

The Commission proposes in point 11 of the negotiating directives that the agreement 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.

In point 12 of the negotiating directives the Commission proposes that the agreement should, in the bilateral relations between the European 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 Convention, in so far as the provisions of the latter agreement or arrangement cover issues dealt with by this agreement.

In point 13 of the negotiating directives, the Commission proposes that 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 European Union Member States. The Commission considers that this agreement, which is of EU-wide application, is one safeguard to achieve this requirement.

Points 14-16 of the directives cover the data protection safeguards required for this specific agreement. Point 14 of the negotiating directives states that the agreement should make

applicable by reference the EU-U.S. Data Protection and Privacy Agreement, otherwise known as the "Umbrella Agreement". In point 15 the Commission states that 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. Point 16 sets out the additional safeguards that the Commission proposes as required for this agreement including the specification of the purpose, the purpose limitation, notification and onward transfer.

Point 17 of the negotiating directives covers the additional procedural rights that the Commission proposes will be required to take account of the unique requirements of the transfer of electronic evidence directly by service providers rather than between authorities. These include that the data may not be requested for the use in criminal proceedings that could lead to the death penalty, the proportionality of orders, and specific safeguards for data protected by privileges and immunities. Immunities and privileges of certain professions such as lawyers, as well as fundamental interests of national security or defence in the State of the addressee must also be taken into account during trial in the issuing State. The review by a judicial authority serves as a further safeguard here.

In the governance provisions in points 18-23, the Commission proposes in the negotiating directives that the agreement includes periodic joint reviews of application of the agreement and a clause on its duration. It is also proposed that the agreement stipulates that the parties consult each other to facilitate resolution of any dispute regarding interpretation or application of the agreement. Statistics should be collected on both sides to facilitate the review process. In addition, the negotiating directives propose that the future agreement includes a suspension and termination clause in the event that the consultation procedure is unable to resolve the dispute.

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

THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 218(3) and (4) thereof,

Having regard to the recommendation from the European Commission,

(1) On 17 April 2018, the Commission submitted legislative proposals for a Regulation on European Production and Preservation orders for electronic evidence in criminal matters and a Directive laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings ("e-evidence proposals")[23]. The Council agreed on a general approach on the Commission proposal for the regulation at the Justice and Home Affairs Council on 7 December 2018[24].

(2) Negotiations should be opened with a view to concluding an agreement between the Union and the United States of America on cross-border access by judicial authorities in criminal proceedings to electronic evidence held by a service provider.

(3) The agreement should include the necessary safeguards for fundamental rights and freedoms and observe the principles recognised by the Charter of Fundamental rights of the European Union, in particular the right to private and family life, home and communications recognised in article 7 of the Charter, the right to protection of personal data recognised in Article 8 of the Charter, the right to effective remedy and fair trial recognised in Article 47 of the Charter, the presumption of innocence and right of defence recognised in Article 48 of the Charter and principles of legality and proportionality of criminal offences and penalties recognised in Article 49 of the Charter. The agreement should be applied in accordance with those rights and principles.

[23] Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, 17 April 2018, COM(2018) 225 final. Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, 17 April 2018, COM(2018) 226 final.

[24] Regulation of the European Parliament and of the Council on European production and preservation orders for electronic evidence in criminal matters, Council General Approach, ST 15292 2018 INIT, 12 December 2018

(4) The European Data Protection Supervisor was consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725 of the European Parliament and of the Council[25] and delivered an opinion on …[26]

HAS ADOPTED THIS DECISION:

Article 1

The Commission is hereby authorised to negotiate, on behalf of the Union, an agreement between the Union and the United States of America on cross-border access by judicial authorities in criminal proceedings to electronic evidence held by a service provider.

Article 2

The negotiating directives are set out in the Annex.

Article 3

The negotiations should be conducted in consultation with a special committee to be designated by the Council.

Article 4

This decision is addressed to the Commission.

Done at Brussels,

For the Council
The President

[25] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L295, 21.11.2018, p. 39).

[26] OJ C ….