Position Paper – E-Evidence

Bitkom views concerning the E-Evidence Proposal

10/10/2018

The Austrian Presidency of the Council of the European Union recently published its Discussion Papers 10981/18 and 12113/18 regarding the E-Evidence Proposal. The documents deal with several Articles of the Proposal for a Regulation on European production and preservation orders for electronic evidence in criminal matters.

Bitkom welcomes that the Presidency is raising questions with regard to Articles 1, 2, 4, 5, 6, 9, 11 and 20/21, especially because many details are still unclear. Bitkom would like to use this opportunity to comment on the latest developments and on the E-Evidence Proposal in general.

Introduction

Bitkom welcomes that the E-Evidence Proposal addresses the challenges of cross-border law enforcement requests and opens up the possibility of achieving better harmonization and legal certainty. We acknowledge that the combinations of processes and procedures nationally and internationally can make the process of seeking data lawfully confusing. We also acknowledge that the legal framework governing cross-border requests needs to be significantly improved. The current state of play leaves many service providers in legal uncertainty as to which data requests they have to fulfil. Especially with regard to the sensitivity of communications data, legal certainty and standardized procedures are needed which is why Bitkom welcomes that the EU Commission addresses the issue in the E-Evidence Proposal.

The proposed E-Evidence Regulation will create two new instruments: the European Production Order (EPO) and the European Preservation Orders (EPresO) which will enable law enforcement agencies (LEA) of one Member State to compel disclosure or preservation of evidence directly from the provider established or represented in a different Member State. The draft Regulation was presented by the commission in April 2018 to allow law enforcement in the EU to access data held by online service providers, including those who are not headquartered in the EU.

Federal Association
for Information Technology,
Telecommunications and
New Media

Rebekka Weiß, LL.M.
Head of Data Protection &
Consumer Law
P +49 30 27576 -161
r.weiss@bitkom.org

Albrechtstraße 10
10117 Berlin
Germany

President
Achim Berg

CEO
Dr. Bernhard Rohleder

In principle, Bitkom appreciates the EU´s initiative to reform the current system, which is most often based on Mutual Legal Assistant Treaties (MLATs) that proved to not be efficient and fast enough to address law enforcement´s needs. Increased legal certainty and a standardization of procedures will not only improve the judicial process but will also improve the situation for providers and citizens. The procedure might also set a positive precedent globally, as it establishes clear commitment of standards and principles for accessing and preserving electronic evidence, particularly those identified in Recitals 2, 13, 29, 30 and 54 of the Regulation's preamble.

As such, it is important that the Regulation emphasises important principles such a necessity, proportionality and a strong rule of law and fundamental rights protection. Also, the impact on the service providers, costs of the procedure and potential conflicts with other law regimes need detailed analyses.
In addition, Bitkom is concerned about the fact, that the provider should be obliged to assess whether the EPO violates fundamental rights, as in our opinion the necessary fundamental rights assessment cannot be outsourced from governmental institutions to private providers without involving national authorities. Furthermore, the details of the providers´ assessment obligations and rights remain unclear at this time and should be specified, enable assessment rights for providers but involve national (or EU) authorities for certain evaluations of the issued Orders.
Furthermore, secure data transmissions and data protection should have the highest priority and be ensured by the technical implementation. Bitkom would like to offer some input on the Regulation that is part of the E-Evidence Proposal, its Articles and related Recitals at this time.

Moreover, Bitkom is keen to emphasize that the E-Evidence proposal should be discussed in a wider political context, given the reciprocal nature of the addressed issues in international law enforcement cooperation. The recently adopted “CLOUD Act” in the United States has created a legal basis for executive agreements between the United States and other countries. E-Evidence should be supplemented by such an agreement between the EU (acting on behalf of the member states) and the United States to avoid a conflict of jurisdictions between EU and the US and vice versa.

1. General comments

1.1 Real Time interception and encryption

The current Proposal rightfully excludes real-time interception and provides the limitations of the scope of the orders to data held by a service provider at the time of the receipt of the EPO or EPresO. These restrictions should be upheld, because real time interception would give rise to several legally and technically complex questions which should – if the EU deems necessary – be addressed in another Regulation. In addition, Bitkom welcomes that the Proposal does not allow for a direct access, i.e. the option to access e-evidence without the cooperation of

a service provider or the owner of the data, as such an access to data would compromise both security and privacy and should not be permitted.

The Regulation should make it clear that the service providers are under no obligation to provide information on the encryption method used or take any other action that would result in the weakening of the confidentiality, security and integrity of the networks and services.

1.2 Necessity and Proportionality

Necessity and Proportionality are important principles which should be upheld and strengthened through a Proposal such as the E-Evidence Regulation and especially because communications data is at the center of the Draft Regulation. Bitkom welcomes that the Proposal already addresses these principles but we believe that the respective sections can be made even more robust and internationally applicable by: clearly defining standards such as 'necessity and proportionality' for international readers. This could include the requirement for a clear and detailed explanation of the ground(s) to believe that the subject of the order has committed a crime; a justification that the evidence cannot be obtained otherwise through less intrusive means; an explicit limit for the quantity of data required, including type of the data, number of users affected, time period covered mitigation measures to minimize collateral interference into the privacy and confidentiality of individuals which are not subject to an on-going investigation.

1.3 Timeline to respond

In Bitkom´s view, the proposed timelines for processing and responding to the production orders are very ambitious. Rather than establishing blanket timeframes for all production orders in all cases, the issuing authority should make an individualized assessment based on the particular circumstances of the investigation. The Regulation may set forth non-mandatory guidelines, such as no less than 24 hours in the case of an emergency and no greater than 21 days. With regard to the currently discussed 6-hour timeline, Bitkom would like to raise the issue that this would effectively lead to a 24/7 on-call duty of all providers. This would heavily burden all providers and will especially pose challenges for smaller providers with less financial and personal resources. The short timeline will oblige even small trade platforms to employ someone to constantly be on hold for a possible request by a LEA.

1.4 Assessment of the request by the providers

Currently, the Proposal provides that the provider is required to assess the validity of the request. Bitkom would like to raise the questions whether the necessary fundamental rights assessment can
a) be done in the very narrow timeframe,
b) can be outsourced from governmental institutions to private providers,
c) leads to a liability of the provider and
d) still enable a certain assessment for the provider (especially a factual, technical assessment, an assessment whether the provider is the right addressee and whether conflicting laws require the provider not to provide the data). With regard to the requirement to assess the request of the LEA, Bitkom would like to suggest introducing harmonized rules for reimbursement.

1.5 Notice

We welcome the requirement for law enforcement authorities to serve demands on the customer himself and only in exceptional circumstances may the authorities seek the data from the cloud provider directly. In such cases, competent authorities should explain why the issuing of a production order directly to the company or other entity would jeopardize the investigation, including in the EPO Certificate transmitted to the service provider.

We also welcome the steps towards requiring law enforcement to notify the users in certain circumstances, but we encourage legislators to go further and amend Article 11 to ensure that authorities are required to notify the persons unless there are exceptional circumstances warranting confidentiality.

Similarly, service providers should also be permitted to notify the users and customers affected by the request. Such notification should only be limited when authorities demonstrate that exceptional circumstances warrant confidentiality. Finally, any such gag order or confidentiality requirement should be governed by strict time limits.

We appreciate that service providers can alert the judicial authorities to requests in certain circumstances, including in cases when the production orders are too broad. Indeed, we often successfully narrow the scope of requests in a manner that respects the due process interests of customers and users, and fully satisfies the needs of the requesting authorities. The Regulation should allow the continuation of this practice. It should also allow companies to challenge gag orders, in particular when they involve an enterprise customer or prohibit notice for an unreasonably long period of time.

Beyond notifying impacted users and customers, the Regulation should make it clear that companies may notify the central authority in any Member State whose sovereign interests are implicated by the request. This interest may be

based on the location of the user or customer. Notification to the central authority would allow Member States to assess and evaluate the validity of the request and raise objections accordingly.

Furthermore, the Proposal should also address the question of transparency reports and which data can be published by providers.

1.6 Harmonization and legal asymmetries

There are legislative asymmetries amongst Member States which need to be addressed.

Clarity is needed to establish if the criminal law basis must be satisfied in both the issuing and recipient Member State. There is significant disparity across Member States' criminal law for crimes entailing a three-year sentence: this threshold is required for a transactional/content data Production Order, but could cause legal uncertainty and leave service providers in a difficult position.

There are several layers of different immunities across Member States. The proposal needs to ensure that national immunity provisions are upheld.
One way to resolve such uncertainties and addressing the questions we raised about the provider´s obligations to assess the validity of the EPO would be to involve the affected Member State´s authorities at an early stage. Such an involvement would strengthen the procedure as the competent national authority is equipped to quickly assess the legality of a measure which either affects persons with habitual residence in that Member State or which may have to be enforced by that Member State's authorities if the provider refuses to produce the data. The competent authorities in the investigating State would then be relieved of the responsibility of resolving legal issues that are more "familiar" to the affected Member State. This will enable affected Member States to assess whether there are any obstacles to the execution of the procedure, particularly due to conflicts with fundamental European values or inviolable principles of Member States' constitutions, or other obstacles relating to immunities or privileges (such as the protection of persons bound by professional secrecy or Members of Parliament). Legal remedies against the decisions to be made by the affected Member State are available in addition to the remedies available in the investigating Member State. Another possible way to address these issues would be to implement a competent EU authority.

1.7 Comity Clauses

Bitkom welcomes the suggested "comity clauses" in the proposed Regulation, which are an important way to help providers deal with conflicting legal obligations and to ensure that the legitimate sovereign interests of countries are taken into account. The proposed Regulation should also explicitly contemplate and support agreements with third

countries as an additional way to facilitate cross-border demands for digital evidence. These agreements would provide an important framework to avoid conflicting legal requirements.

While Bitkom appreciates the comity clauses as laid down in Articles 15 and 16 of the proposed Regulation it is important to keep in mind that these clauses may reduce the danger of international conflict of laws, but do not fully preclude such conflict constellations. Articles 15 and 16 of the proposed Regulation are leaving the possibility of a court confirming a legal conflict (e.g. between the European Production Order and United States blocking statues), while upholding the legal obligation for a service provider under the EPO system.

In such a situation, the judicial decision of a European court (a sovereign act) would literally create an obligation to infringe foreign law. Companies assuming such conflicts of law when receiving an EPO will bring these cases to court, since there is no legal means to be compliant under both legal frameworks. Given the reciprocal character of this specific issue, Bitkom is asking the EU Commission to push forward its efforts for an agreement with the United States aiming on the avoidance of the described conflicts.

The current version of the E-Evidence Framework shall enable EU Member States to easily produce or preserve data in respective other Member States for prosecution purposes. However, the current version leaves it quite open what happens if a Member State itself has concluded bilateral or multilateral agreements with non-EU states which regulate mutual legal assistance with regard to the exchange of data. Therefore, the current version of the framework contains the risk that one Member State could transfer data gathered through the E-Evidence Framework from other EU Member States to non-EU states. In such a situation, where data gathered on the basis of E-Evidence and such data leaves the EU without adequate legal grounds or consent of the other Member States should be explicitly ruled out by the E-Evidence Framework.

Moreover, EU Member States and their authorities making use of the advantages of E-Evidence should be clearly obliged by the E-Evidence Framework to use data gathered on its basis solely for their own prosecution purposes and should not be entitled to share it with non-EU states on which (legal) basis whatsoever.

In this context besides a clear rule setup concerning this topic in the Regulation itself, a centralized European authority as he issuing authority for orders is a reasonable choice to ensure the safety and conformity of data provisioning according to the E-Evidence Framework. The specific official assignment and rule set for such a centralized authority could also include the task to ensure that EU data only leaves the EU if this is based on a legal framework which has been accepted by the affected Member States or has been negotiated by EU organs.

1.8 Jurisdiction and Relationship to other Instruments

As decision-makers in the European Union deliberate the new European framework that governs cross-border access to electronic evidence, it is important that they do not lose sight of the international precedent their new legislation can set. Indeed, whether the EU decides to respect the legitimate sovereign interests of other jurisdictions, or, instead, opts for a unilateral solution, can have a decisive impact on how other countries will interact with European and other companies.

We are concerned, that the proposal significantly departs from the existing international standards, as outlined in the Budapest Convention on Cybercrime, which may result in the inappropriate extraterritorial application of the law. Article 18 of the Convention allows an authority to issue a production order (1) if the criminal justice authority has jurisdiction over the offence; (2) and if the service provider is in possession or control of the subscriber information; (3) and if the person or service provider is in the territory of the party, or the party considers that a service provider offers a service in its territory; (4) and if the subscriber information to be submitted relates to a service of the provider offered in the territory of the Party. All of the four conditions shall be met. The Commission's proposal, only references parts of these four criteria, namely the ones related to offering a service. Even in that case, the proposal does not require that a service provider offers services in the Member State of the issuing authority. It is enough, if the service is offered somewhere in the Union.

In more general terms, the relation of E-Evidence to the Budapest Convention and the existing MLAT procedures is widely unclear. Given the fact that a reform of the Budapest Convention is currently discussed at a political level[1] it is important, that E-Evidence clarifies, how both frameworks from a Commission´s perspective relate to each other, whether E-Evidence shall replace the MLAT framework partly or fully or whether E-Evidence shall complement the Budapest convention. Bitkom emphasizes that the rule of law standards of the frameworks must not differ fundamentally, since otherwise a race to the bottom (with respect to the legal requirements for disclosure orders) will be the result. The same principally applies to potential future executive agreements as foreseen in the U.S. CLOUD Act. Since Executive Agreements will likely add another layer to the international legal lawful access framework, The EU should consider paving a way and implementing standards for this new type of agreements, just as the CLOUD Act is setting such standards itself.

Expanding the reach of the Budapest Conventions' provisions this way will set an international precedent, which will likely cause reciprocal responses on part of other states and therefor threat the rights of European citizen. It will likely be copied by other countries around the world, including by those with lower or no rule of law and fundamental rights standards. This will expose all companies, including European ones and those with European user information, to an increasing number of mandatory extraterritorial demands for user data, regardless of the protection afforded in the country of the issuing authority. This would erode all the protection, however imperfect it

[1] https://ccdcoe.org/council-europe-ponders-new-treaty-cloud-evidence.html.

may be, offered by the MLAT system. Respecting the standard of possession or control has many benefits. It enables companies to maintain high organizational and security standards that limit access to such data to those who are trained to deal with law enforcement access requests. This is not just a reputational and business imperative, strong security and confidentiality standards are also a requirement under the General Data Protection Regulation. It is also more efficient for authorities to direct their production order to an entity that can properly evaluate each request. Without the standards set forth in the Budapest Convention, companies with an international presence will be more exposed to demands for data, often from jurisdictions without strong safeguards, and failure to comply may result in the arrest of employees, threats to the business, and less transparency in accessing users' data. Honoring the established principles will not undermine authorities' ability to obtain data. European authorities can continue to rely on this Regulation, the European Investigation Order, or the Mutual Legal Assistance Treaty process.

Clarification is also needed regarding whether the regulatory framework implemented with the E-Evidence is to be understood as being exhaustive. In some respects, the EPO provides for stricter requirements than those which apply in existing voluntary cooperation models of the member states on the basis of the applicable law. The latter play a decisive practical role in the case of requests for data from providers in non-EU countries.

For the providers concerned, it must be clarified which standards shall apply after the E-Evidence Regulation comes into force. It should be avoided that different standards and thresholds apply to the same constellation.

1.9 Authentification of Authority Procedure involving national Authorities

With regard to the requesting LEA, the question how the provider can assess the authority of the institution is still not clearly answered. The Regulation should therefore provide for Orders being directed to a national Single Point of Contact (SPOC). Creation of a 'one stop' Single Point of Contact resource for communications data in each country can greatly assist law enforcement in navigating the complex world of 21st century data requests: investigators access the system through the SPOCS, who become the de facto experts on data requests. A SPOC system could include individual SPOCs (or groups of SPOCs) in each region, law enforcement agency or city. Or it could be a national unit or group of SPOCs. Consideration should also be given to whether the number of SPOCs is limited. Whichever system a Member State uses, SPOCs should work very closely together and share professional development.SPOCs could therefore perform a variety of functions: establish clear points of contact for providers; enhance advice possibilities and training and develop expertise.

Furthermore, the Proposal provides for a request without involving national authorities (see suggestions on that question above). We propose to introduce verification and an assessment by the national authority to verify the request and provide for a governmental evaluation. This could also help in cases where dual criminality is an issue, e.g. when the requesting Member State is prosecuting an offense that is not equally punishable in the other

Member State. Such a procedure could also provide for good faith clauses which indemnifies providers if they comply in good faith.

If national authorities are involved, the procedure could be initiated by the investigating authority which addresses an EPO to the contact point of a provider. This should take place no later than the point at which the EPO is sent to the provider. The procedure is initiated by sending the form, complete with the details required by Article 5 (5) of the Regulation, to the competent authority of the affected Member State. Article 5 (5) of the Regulation should be supplemented to stipulate that the form must also include the facts of the case and considerations as to why the required evidence appears appropriate and necessary.

1.10 EU-Legislation

The E-Evidence Regulation proposes that the issuing state, based on their legislation, can directly approach providers enforcing them to comply, which means bypassing judicial process and failing to consider the state law of the enforced provider. This leaves the providers with concerns as to how the legitimacy of a data request can be verified, with concerns of potential violations to the EU Charter of Fundamental Human Rights, as well as potential violations of f.i. local secrecy of telecommunications law, which is manifested in the constitution of most EU member states, and can only be lifted under strict legal safeguards. As a result providers face increased risks of sanctions due to unlawful collection of customers' personal data in contradiction with data protection laws, and in contradiction with the national sovereignty of the targeted states (basically, this system would enable LEA to act without judicial authorization of the country where the data is stored).

E-Evidence potentially could impact the legal basis of Article 82 (1) of the EU Charter regarding judicial cooperation in criminal matters in the Union, which is based on the principle of mutual recognition of judgments and judicial decisions and shall include the approximation of the laws and regulations of the Member States. The risk of political persecution is a serious risk that needs to be considered.

Telecommunications providers are subject to the provisions of Directive 2014/41/EU, establishing a European Investigation Order (EIO). Unlike the EU's proposal for E-Evidence, the EIO respects national legislation as it allows the possibility under certain local legal conditions to reject an order that conflicts with local law e.g., domestic cases. EIO does not place providers in legal uncertainty as e-evidence potentially does.

The conditions under which a Member State may restrict the privacy rights and obligations in electronic communications are still under negotiation in the framework of the future ePrivacy Regulation.

Different data retention laws apply in the EU member states. Therefore, the obligations as to the data and the period retained are stipulated in local legislation, which may have the potential for e-evidence to conflict with national law.

1.11 Compatibility

Questions as to differences in terminology and data formats could be problematic to efficiently fulfil data requests. The Proposal also does not sufficiently distinguish between data controllers and data processors.

2. Subject Matter, Definitions and Scope, Articles 1-3

It must be ensured that the definitions do not conflict with the definitions of the ePrivacy regulation and the GDPR.

3. European Production Order

3.1. Article 4 – Issuing Authority

It should be considered that a centralized European authority as the issuing authority would be the better choice to ensure the safety of data provisioning and harmonization of different national laws. The Presidency proposes a new Article 4 No. 5 saying that in emergency cases the judicial validation can be sought ex post. It is important that the provider gets all information to verify the urgency (threat to life or physical integrity of a person or to a critical infrastructure).

3.2. Article 5 – Conditions for the EPO

With regard to Article 5 No. 4 it is necessary to clarify the conditions for the service provider´s obligation to provide the data under an EPO. The 3-year custodial sentence threshold for criminal offences in the issuing state for subscriber or access data is not transparent or verifiable for a service provider in another country with differing national criminal law. This is equally true for the catalogue of offences for transactional data or content data. The service provider would need consultation to ensure that the EPO stipulates the conditions set out in the Regulation. This is an additional financial burden on the service provider and would also make it difficult to provide the data within the time limits set out in Article 9 of the Regulation. Bitkom suggests that a catalogued list should be assembled with all criminal offences within the European Union that enable the issuing authority to send a EPO. Furthermore, there should be no liability of the provider for the liability of the EPO.

3.3. Article 6 – Conditions for issuing an EPO

It should be clarified, that the EPO only includes data that are already stored in compliance with the respective national laws and there will be no obligation to preserve future data. This is necessary to not cross the borders

to real time interception. It should be made mandatory that LEAs have to provide a statement explaining why addressing a production order directly to a company or other entity would create a substantial risk (not only the mere possibility) of jeopardising the investigation.

3.4. Article 7 – Addressee of a EPO and a EPresO

Providers established in more than one Member State and offering services by means of cross border infrastructure should have the choice, which entity should fulfil the Orders regardless of where the legal representative resides.

3.5. Article 8 – European Production and Preservation Order Certificate

It must be guaranteed that the process of issuing and valuating the EPO/EPresO is not misused or exploited. Secure technical measures to ensure data safety, e.g. the data needs to be encrypted when sent from the service provider to the authority, one technical ETSI standard interface should be used by all authorities and providers. In addition, there should be a technical interface which allows a clear identification of the sender and addressee (f.i. as with the SINA solution). This would make it easier for providers to see if the order is issued by a competent authority.

From a practical point of view the legislative initiative should therefore be accompanied by a technical directive from ETSI security standards to ensure the coordination of all national interests and guarantee the safety of data provisioning.

With regard to Article 8 No. 2 secure channels should be obligatory for all countries and not just compulsory in those Member States where they have already been established.

With regard to Article 8 No. 5 it should be clarified at what point of the process the decision shall be made or who decides if the translation into an official language of the Union –other than one of the official languages of the Member State where the legal representative resides- is necessary.

Also, the following standards on the basis of Regulation 910/2014/EU should be set for the national authorities for the requests: each representative issuing a request (natural person) should identify himself/herself with a secure identification method and any notice or printout of a legal person should be sealed. Every server connection between entities should be used with a QWAC to ensure identification and encryption and every record that is stored should be kept as evidence to be archived. An appropriately notified system of registered delivery should be used for the exchange (between different authorities) of communication with the authorities.

All in all, all eIDAS tools should be used by the authorities. Especially when handling digital material as evidence, which is subject to a forensic chain of custody, a high and EU-wide harmonised system and standard should be implemented.

3.6. Article 9 – Execution of the EPO

It will be difficult for providers to check if the orders are lawful and issued by the competent authority. Therefore, there should be an official list of competent authorities. Ideally there should be only one competent issuing authority per Member State.

The respond time in Article 9, especially the timeline for emergency cases in 9.2 is too short. In addition, we would like to note that any required response time can only be guaranteed if the LEA request will be received by the Service Provider promptly. However, the transfer could be affected in case of a communication failure between LEA and Service Provider. Therefore, periodic alive messages shall be supported to identify and log a communication failure.

Article 9 No. 5: the possibilities of the providers to refuse the data provision and seek assistance by local authorities are too limited and unambiguous, e.g. providers should also have the possibility to refuse the order if it considers that the country of the issuing state does not have the same level of data protection or the order does not comply with national legislation.

3.7. Article 11 – Transparency

The Regulation points out in Article 11 that trust between Member States is a key element in the Regulation. This trust will be bolstered by more transparency, especially transparency that allows Service Providers an increased ability to understand the background of the order and how it meets the provisions in the Regulation, including Recitals 2, 13, 29, 30 and 35.

Currently, the EPO and the EPresO contain no information on the background to the offense. An increase in information/context will provide comfort that requests indeed comply with laws on 'necessity and proportionality.' This could provide more comfort that requests are lawful and at the same time would enable the request to be challenged on 'fundamental rights' –if necessary. Best practice internationally, both from a legal and operational perspective indicates that inserting independent individuals into the communications data acquisition process is beneficial. This not only ensures that requests meet all the legal requirement, without the possible bias of someone wedded to the investigation. It also provides the benefit of an independent set of eyes on the investigation, possibly identifying other additional communications data opportunities.

Providing more information would also increase the ability of Service Providers to assess the request properly and inform the LEA as envisaged in Article 9 (3).

3.8. Article 12 – Reimbursement of costs

The simplification of legal assistance will most likely increase the number of investigation orders. Major investments in staff and technical infrastructure will be necessary. An adequate reimbursement of costs must be ensured. The providers should be able to claim reimbursement according to laws of the addressee or a binding and adequate reimbursement rule for all Member States should be added to Article 12. The currently discussed notice of the issuing state with which it shall inform the addressee about its own reimbursement rules does not suffice in this regard. In addition, the providers need adequate remedies in case the issuing authority refuses reimbursement.