



Council of the
European Union

Brussels, 27 March 2018
(OR. en)

7509/18

JAI 251
CATS 17
COPEN 86
EUROJUST 36
CYBER 49
EJUSTICE 24

COVER NOTE

From:	EUROJUST
To:	Delegations
No. prev. doc.:	6029/18
Subject:	12th Meeting of the Consultative Forum of Prosecutors General and Directors of Public Prosecutions of the Member States of the European Union Eurojust, The Hague, 6 October 2017 - Summary and compilation of replies on the use of digital tools in criminal proceedings

Delegations will find in Annex the Summary and the compilations of replies to the above mentioned questionnaire, discussed at the 12th meeting of the Consultative Forum of Prosecutors General and Directors of Public Prosecutions of the EU Member States held at Eurojust on 6 October 2017.

**12TH MEETING OF THE CONSULTATIVE FORUM OF PROSECUTORS GENERAL
AND DIRECTORS OF PUBLIC PROSECUTIONS OF THE MEMBER STATES
OF THE EUROPEAN UNION**

**THE HAGUE, 6 OCTOBER 2017
EUROJUST BUILDING, THE HAGUE**

SUMMARY OF THE REPLIES TO THE QUESTIONNAIRE ON THE USE OF DIGITAL TOOLS IN CRIMINAL PROCEEDINGS

This summary has been prepared on the basis of the 26 contributions received to date (2 October 2017) from the Forum members to the questions regarding Session I on “The Use of Digital Tools in Criminal Proceedings”. The replies have been submitted by the Forum members of the following Member States: Austria (AT), Belgium (BE), Bulgaria (BG), Croatia (HR), Cyprus (CY), Czech Republic (CZ), Denmark (DK), Estonia (EE), Finland (FI), France (FR), Germany (DE), Greece (EL), Hungary (HU), Italy (IT), Luxembourg (LU), Latvia (LV), Lithuania (LT), Poland (PL), Portugal (PT), Romania (RO), Slovakia (SK), Slovenia (SI), Spain (ES), Sweden (SE), the Netherlands (NL) and United Kingdom (UK).

1. Does your Member State foresee the use of electronic signatures in the public sector and, particularly, in the context of criminal proceedings? Please specify. Do you see any advantages/disadvantages to such use?

Majority of Member States are making use of electronic signatures in criminal proceedings

A **large majority** of Forum members **confirm the use and the validity of electronic signatures** in the public sector and, particularly, **in criminal proceedings** (AT, CY, CZ, EE, EL, FR, HU, DE, LV, LT, IT, PL, PT, RO, SK, ES, SE, NL, UK).

Some Forum members inform that they do not yet use electronic signatures in the public sector (HR, DK) or, more specifically, not in criminal proceedings (BG, HR, DK, BE, SI, FI, LU). In one Member State its use is generally related to the civil turnover (BG). In some Member States there is either no legal framework (BE) or there is a legal framework, but the Ministry still needs to lay down the conditions and methods for the electronic filing of submissions in an electronic format (SI). One Forum member explains that, in its Member State, a new system of criminal files is currently under development and electronic signatures are planned to be used in this new system (FI). In several Member States that currently do not use electronic signatures, there have been **pilot projects or alternative projects**. For instance, in one Member State, there was a pilot project in relation to digitalised signatures at police level for the signing of police reports (BE). In another Member State an “e-post system” was launched which requires for all citizens and companies to have a digital mailbox in the system and all emails sent from authorities to citizens and companies are sent via this secure electronic mail system (DK). In another Member State, cooperation with the financial intelligence unit of the office of the state prosecutor is done electronically (LU).

Electronic signatures are being used at different stages in the criminal proceedings depending on the Member State

There are **significant differences** in relation to the specific parts of the criminal proceedings where electronic signatures are being used in the different Member States. For instance, some Forum members explain that in their Member States electronic signatures can be used by **all the main actors throughout the criminal procedure** (HU, NL). For instance, in one Member State, the courts, the prosecution service, the investigating authority and the penal institution all use it, not only within their organisation and between each other, but also in the relation to their clients, i.e. defendants, victims and witnesses, with the only exception of persons who are kept in penal institutes, as the latter have no rights to use electronic case handling (HU). Another Forum member explains that in his Member States electronic signatures are being extensively used in the course of **pre-trial investigations** amongst the competent authorities involved in the pre-trial phase, but not by courts at the trial phase, and not when an electronic document is sent to third parties (LT).

Several Forum members gave some more specific examples as to when and by whom electronic signatures could be used, for instance: (i) by **prosecutors** when filing documents, including the indictment, to the courts (SE, HU); (ii) by **citizens** when filing criminal complaints (EL) or when submitting declarations, applications or reasons given in support thereof to the court or the public prosecution office (DE); (iii) by **(judicial) authorities** when serving judgments or orders (EL), when sending replies and notifications to natural and legal persons (LV), when sending other documents to accused, defence counsel, victims, penitentiary and custody institutions (SK), when releasing orders of prisoners (PL), when sharing data resulting from technical surveillance activities/procedures and communication of computer data with other authorities (RO); and (vi) by **witnesses** when making a written testimony following or in lieu of the oral questioning (HU).

A few Forum members underlined that the implementation of the use of electronic signatures in their Member States will be **further improved in the near future** by new software (EL) or the implementation of recently adopted legislation (DE, HU, PT).

Advantages in relation to the use of electronic signatures

Nearly all Forum members, including those coming from Member States where electronic signatures are currently not yet in use, underline the advantages that they see in relation to the use of electronic signatures, e.g.:

- To avoid undue delays, speed up the procedures and make it more effective and productive (CY, EE, FI, HU, DE, RO, SE, NL);
- To provide a system that is secure and that guarantees the authenticity and identity of the signatory (CY, BE, BG, RO);
- To ensure high interoperability in technical and legal areas (AT);
- To enable fast exchange of information and documents amongst the competent authorities involved and direct use of documents transmitted/received in this format (BE, EE, RO, UK);
- To facilitate communication (HU, DE) and ensure that all authorised participants in the process can access the complete file 24/7 (NL);

- To ensure a more environmentally friendly solution (SE) whereby retention and storage of hard copies of documents is removed from the process (UK) and files or pages will not get lost (NL);
- To choose for a progressive implementation of the elektronization and informatization into the criminal proceedings (SK).

Disadvantages in relation to the use of electronic signatures

Some Forum members point at possible disadvantages in relation to the use of electronic signatures. One Forum member underlines, however, that some of these “disadvantages” are, by nature, initial difficulties linked to the setting up of a new system, and they do not outweigh as such the advantages of creating a digital system (HU).

- Mass use of electronic signatures requires significant cultural change and is very different from the current paper form case handling that everyone is accustomed to use (HU);
- Signature creation is time consuming (AT);
- It could be difficult to provide validity in mixed cases, where it is important to issue both electronic and paper form documents (HU);
- Problems of security (e.g. risk of cyberattacks) and authenticity must be resolved in a satisfying way (DE, HU);
- A possible, but unlikely risk of digital signatures is that the contents of a statement could be altered after the witness has signed it. This could, however, be addressed by requiring a digitally signed statement to be saved to a non-editable format which would be time-stamped with procedures in place to ensure that the correct version of the statement is recorded and monitored (UK);
- Technical issues, e.g. due to the volume/size/form of paper documents (HU) or the interoperability of different case management systems (ES).

<p>2. To what extent does your Member State make use of digital information exchange in the context of criminal proceedings? Do you see any advantages/disadvantages to such use and/or do you see any margin for further use of digital tools in criminal proceedings?</p>
--

Majority of Member States already makes use of digital information exchange or is in the process of implementing such systems in the near future

A number of Forum members confirms that digital information exchange in criminal proceedings is **quite advanced and widespread** within their Member State (CZ, DK, EE, ES, PL, SE, UK). Two of these Forum members inform that **almost all documents between parties are exchanged digitally** (EE, UK). Some specify that case material is **presented digitally in court** by prosecutors and/or attorneys using tablet devices (DK, UK). One Forum member explains that its national uniform information system is used by law enforcement and prosecution and does not only serve as **database for statistics and search tool**, but is also designed to compose **electronic copies of criminal files** (CZ). Most of the Forum members coming from Member States that have already a quite advanced digital information exchange system in place, underline that their system is subject to further improvement and development (CZ, ES SE, UK).

Additionally, there is a considerable number of Forum members, who explain that, in their respective Member States, **considerable progress has been achieved recently, and/or can be expected in the near future**, as a consequence of e-projects and/or e-legislation that is aimed at a (full) digitalisation of the criminal proceedings (DE, FI, FR, IT, LV, LU, PT, SK, NL). The final objective for most of these countries is to have a digital system where all relevant actors police, prosecutors, court, defence lawyers will be connected and will exchange information digitally.

By contrast, **only a few** other Forum members acknowledge that digital information exchange is still **limited and/or at an early stage** in their Member States (BE, RO, SI). For instance, one Forum member explains that the vast majority of interactions in criminal files still occurs on the basis of exchange of physical files and that, since digital criminal files hardly exist, except in huge cases, lawyers and citizens need to move physically in order to have access to the criminal file (BE). In that same Member State, some digital initiatives have been initiated such as JustScan (scanning of criminal files in judicial investigations), e-deposit (electronically uploading of documents related to a file) and VAJA (creation of a central database of judgments), but some of these projects only apply to a limited number of cases (Just Scan) while others are still under construction (VAJA).

Some Forum members focus in their replies on specific applications where digital information exchange results very useful, for instance, information exchange regarding **bank accounts** (HR, LU) or information exchange with **telecom providers** (AT).

Several Forum members also mention, in their reply to this question, the need to reflect, **with the EU institutions**, to set up portals or systems that allow both an **effective and a secure exchange** of information (LT, LU, SI, ES, see also *infra* 3).

Advantages in relation to the use of digital information exchange

Nearly all Forum members, including those Member States where digital information exchange is not widely used, underline the advantages they see in relation to digital information exchange:

- Faster and easier access to relevant material when it is made available, greater control over who has access to case material and more secure transfer and management of documents (DK, HR, HU, LT, LV, PT, RO, SE, UK);
- Greater efficiency in the case management (UK, IT, LV, PT) and increased productivity, e.g. no need to register the same data twice and automatic registration of actions and received/sent documents (SE);
- Reduction of costs, e.g. savings in paper, storage and other ancillary costs associated with managing hard-copy material, automation of administrative functions reducing costs of administrative processes (UK, BE, IT, LT);
- Validity and integrity of the content of the documents and the identity of the documents' issuing authority can be properly ensured by electronic signatures (HU, RO);

- Mutual communication can be accelerated within the criminal proceedings (SK);
- Better statistics and easier archiving (SE).

Disadvantages in relation to the use of digital information exchange

Some Forum members point at possible disadvantages in relation to digital information exchange in criminal proceedings:

- There may be initial significant financial outlay for the purchasing/installation of IT software and hardware (UK);
- It requires significant cultural change (which cannot be underestimated) to achieve the full anticipated benefits of digitalisation (SK, NL, UK);
- Digital information exchange is not easy and takes time to develop and implement. There are often business/operational, judicial and technical challenges and lack of understanding of these facts can be frustrating (SE, NL);
- Electronic documents are more easily distributable in great numbers and, for this reason, investigations might become more transparent. This implies that the defendants and the defence counsels could harmonise their defence tactics more easily, as it is easy to share with each other the testimonies, records on investigative measures, which would otherwise be accessible by a few of them. It is easier also to put a pressure on the investigating authorities with continuously informing the society on the stance of the criminal proceeding and showing it in a disadvantageous aspect(HU);
- Computer systems are vulnerable against cyber-attacks. It is an easier way to attack a system in the cyberspace, than acquiring the paper form documents. Therefore the system containing data on criminal cases should be properly protected, which is an important task and a great challenge (HU, LU, SE);
- Transfer of big volume data is a technical challenge, particularly, vis-à-vis private persons as the latter cannot be expected to have similar broadband internet and storage capacities as a public authority. Electronic documents should be handled to them in such a way that they can access them with the tools and broadband they have in their possession (HU);
- Privacy issues must be given due consideration(IT);
- There is a financial impact of the technical support e.g. a secure technical frame, costs of technical equipment to be used for transmission and training of personnel (RO).

Some of these “disadvantages” seem, by nature, initial difficulties linked to the setting up of a new system, and they do not outweigh the advantages of creating a digital system. For instance, one Forum member underlines that the costs that are needed to set up and maintain a system of digital exchange are justified because of the more efficient activity, the speed, the safety and the integrity of the procedures (RO).

3. Have you encountered, in your relations with other EU Member States, any obstacles to judicial cooperation in criminal matters that are related to the use of electronic signatures and/or digital information exchange?

Generally, not many obstacles identified (due to a lack of experience)

Several Forum members reply that they **cannot identify any major obstacles** to judicial cooperation in criminal matters in relation to the use of electronic signatures and/or digital information exchange (AT, HR, CY, DK, EL, HU, LT, LU, PT, SK, SE). One Forum members says that this is due to the fact that the e-IDAS Regulation creates an appropriate basis for cross- border information exchange (AT). Several other Forum members argue that the main reason why obstacles are not identified is due to the fact that **electronic signatures are currently hardly ever used** in judicial cooperation in criminal matters, so there is not experience in this respect (HR, CY, EE, HU, LV, PT, SK, NL).

In judicial cooperation in criminal matters, **communication by e-mail is widely used** both by the police, judiciary and contact points of the networks (e.g. EJN, ECJN and others) (CZ). Eurojust is frequently used for transmitting/receiving requests or various data/information necessary to executing requests, or the results of executing the requests, however, without the use of electronic signatures (RO).

In relation to the **electronically sending of MLA requests**, one Forum member explains that such requests are accepted, and their execution is ordered without delays (CZ). Another Forum member confirms that usually there is a **need to send the original request via ordinary mail** in paper afterwards, while the exchange of MLA requests with countries that accept to do it paper-free is much faster (EE).

Some examples of obstacles in relation to the use of electronic signatures and digital information exchange in criminal matters

Some Forum members mention, **in general, the following obstacles for the digital exchange of communication** by judicial authorities:

- The lack of a secure way of data transmission (DE,RO, SI);
- The lack of common standards of encryption (DE, SK);
- Technical problems related to the submission of large volumes of data (DE, RO);
- Technical standards of digital documents (IT);
- The need to own the devices/apps to verify the certificate and provider (RO);
- The lack of interoperability between Justice systems of Member States which can complicate the activities and permanent exchange of information (including digital information) in the context of a joint investigation team (ES).

Additionally, one Forum member suggests to make a distinction between digital information in general and the **particularities related to** judicial cooperation in the **fight against cybercrime** where data stored in information systems is requested. In relation to the former, no particular issues have been identified with regard to the exchange of digital information. In relation to the latter, some of the main remaining issues that can be listed are: volatility of data, loss of location, different approaches to the concept of jurisdiction in this field, difficulties in identifying the competent jurisdiction or the jurisdiction where to address a MLA request, the need to find alternatives to traditional MLA requests, production order for subscriber information, confidentiality and disclosure or differing approaches to the possibility of trans- border access to stored computer data, among others.

Finally, two Forum members give **concrete examples** of cases where obstacles occurred in relation to an **MLA request/EIO and the use of electronic signatures**. One Forum member notes that, while all incoming requests are usually still manually signed, there have been cases where the request was only signed with an identification number and where there was a need to ask the requesting authority to provide an identification as the requested authority did not have the equipment to identify the number. This required further explanations and discussion amongst the authorities involved and caused some delay (BE). Another Forum member referred to a case where one Member State would not accept that a court issued an EIO without a wet signature (UK). In that case, an EIO was issued by the UK court and a Judge had granted the application and provided an electronic signature. The EIO was transmitted to the relevant Member State, but was returned by the prosecutor who requested that the UK Judge would need to provide a wet signature or a court stamp in order for the EIO to be recognised. The EIO was stamped by the UK court, but again was returned by the Member State who requested a wet signature from the issuing Judge. In relation to the transmission of requests issued *without* the electronic signature, e.g. scanned requests or requests sent by electronic mail, one Forum member says that it is not aware of any obstacles, as long as they are issued in conformity with the existing legal mechanisms (SK).

Important instruments in the EU legal area and future perspectives

Several Forum members refer to relevant legislation and/or initiatives at regional and European level which enhance the use of digital information exchange, such as the **Prüm Convention** (DE) or the **Budapest Convention** (IT). Another positive example is the **e-CODEX pilot EURegio** which implies cooperation of the authorities of North-Rhine-Westphalia with prosecution offices and courts in Belgium and the Netherlands, including means of direct communication between the police and prosecution offices (DE, NL). Two Forum members greatly support the development and implementation of the **e-Codex project** (SI, ES). Two other Forum members underline the importance of the initiative of the **European Commission** regarding **the creation of an electronic portal for the transmission of MLA and EIO requests** and the electronic evidence acquired in the execution of these requests (SK, LT).

One Forum members also refers to its national information system (Cassiopée) which will, in a near future, be able to **feed, automatically, from its national data base the Eurojust Case Management System** with relevant information on “European” cases (FR).



Consultative Forum



of Prosecutors General and
Directors of Public Prosecutions





12TH MEETING OF THE CONSULTATIVE FORUM OF PROSECUTORS GENERAL AND DIRECTORS OF PUBLIC PROSECUTIONS OF THE MEMBER STATES OF THE EUROPEAN UNION




THE HAGUE, 6 OCTOBER 2017





1. Does your Member State foresee the use of electronic signatures in the public sector and, particularly, in the context of criminal proceedings? Please specify. Do you see any advantages/disadvantages to such use?


Member State	Replies and observations
 AT	<p>The use of electronic signatures is supported, but not mandatory in context of criminal proceedings. Electronic signatures are supported in the following areas:</p> <ul style="list-style-type: none">• Authentication for parties / citizens• Signature and validation of documents and applications <p>The major advantage of electronic signatures is high interoperability in technical and legal areas. On the other hand signature creation is time consuming compared to conventional signatures.</p>
 BE	<p>In the public sector in Belgium, the electronic signature is used inter alia in the context of tax-on-web (electronically signing and sending of a tax declaration) and the public service of Social Security (Rijksdienst voor Sociale Zekerheid or RSZ) prioritises the digitisation of its document flow as well. Whereas most social security claims have long been digital, most of its notifications and confirmations are still sent on paper and the RSZ want to change this by using the company's secure e-box.</p>


	<p>With regard to criminal proceedings, the use of the electronic signature (with an e-ID) has not been legalised meaning if someone were to use an electronic signature in this regard, it would have no legal value at all.</p> <p>However, the possibility of a digitised signature used by some police zones (in the context of pilot projects) was allowed when signing their reports, which implies that a 'wet' signature is placed on an external device or on the tablet / laptop screen and copied using an application onto the digital report at the place where the "wet" signature was applied. There is therefore no real signature, but there is a validation and confirmation of the fact that the signature holder has effectively introduced the signature at the moment as indicated.</p> <p>Moving in the direction of electronic signatures provides numerous of benefits for the police and the public prosecution (justice), as a shared server would allow that the information between the involved agencies can be shared completely, including:</p> <ul style="list-style-type: none"> - reading the reports - online examining of pictures and camera images - digitally sending of instructions <p>which will result in an easier way of composing a digital criminal record.</p> <p>However, a 'real' digital criminal record will only be possible when the electronic signature holds effective legal value, as it will assure people of the authenticity and identity of the signatory.</p>
 BG	<p>With the development of information technologies, especially the Internet, the possibility of exchanging electronic statements immediately – without territorial limits and practically for free – has led to transferring the major part of communication between people in the electronic environment. Insofar as the law links some of these statements with legal consequences, the question about methods of identifying authors of e-statements and furthermore methods of securing the remaining functions of the signature – consent, integrity and irrevocability – was raised sharply.</p> <p>In search of a solution, the concept of electronic signatures as an analogue of handwritten signatures in the electronic world was created. In Bulgaria, the validity of e-signatures was sanctioned with the adoption of the Electronic Document and Electronic Signature Act</p>

	<p>(EDESA), prom. SG Issue No. 34 of 6 April 2001, amend. SG Issue No. 112 of 29 December 2001, amend. SG Issue No. 30 of 11 April 2006, amend. SG Issue No. 34 of 25 April 2006, amend. SG Issue No. 38 of 11 May 2007, amend. SG Issue No. 100 of 21 December 2010, suppl. SG Issue No. 101 of 20 December 2016 effective 06.10.2001.</p> <p>This Act settles the electronic document, the electronic signature and the terms and conditions for providing certification services.</p> <p>Here are the legal definitions of the following concepts according to the Act:</p> <p>Electronic statement – a verbal statement presented in digital form by a generally adopted standard of transformation, reading and visual presentation of the information. The electronic statement can also contain non-verbal information.</p> <p>Electronic document – an electronic statement written on a magnetic, optic or other carrier enabling reproduction. The written form shall be considered complied with if an electronic document is compiled.</p> <p>Author of the electronic statement – the individual indicated in the statement as its author.</p> <p>Titular of the electronic statement – the person on whose behalf the electronic statement is made.</p> <p>Addressee of the electronic statement – the addressee of the electronic statement can be a person who, by virtue of a law, is obliged to receive electronic statements or which, on the grounds of unambiguous circumstances, can be considered agreed to receive the statement in electronic form.</p> <p>Mediator of the electronic statement – a person who, by assignment of the titular, the author or the addressee, sends, receives, records or stores an electronic statement or performs other services related to it.</p> <p>Electronic signature – every information in an e-form added or logically related to the electronic statement, to establish the identity of the author.</p>
 HR	No, electronic signatures are not yet in use in public sector in Croatia, nor are digital signatures used in criminal proceedings.

 CY	<p>Yes, we do foresee the use of electronic signatures in the context of criminal proceedings as it will speed up the procedures that are in place now. One of the main advantages in the use of electronic signatures is the security that the system is providing.</p>
 CZ	<p>The question of electronic communication between the courts, law enforcement and individuals involved in both civil and criminal proceedings was the subject of a recent Opinion of the Supreme Court (Opinion of the Supreme Court on Submissions Filed Electronically and on Service of the Court's Electronic Documents through the Public Data Network of 5 January 2017).</p> <p>As for the criminal proceedings the law provides for submission filled by electronic and other on-remote means (Article 59, para 1 of the Criminal Procedural Code). The electronic signature equals to the regular signature and has to be accepted by the state authorities as stipulated by the law (see especially: Law No. 300/2008 Coll. Act. of 17 July 2008 on electronic acts and authorized document conversion; Law No. 297/2016 Coll. Act of August 24, 2016 on trust services for electronic transactions). In case the submission was sent from the data box belonging to a petitioner (to the person filing the submission) the electronic signature is not required. The jurisprudence deems "the authorisation of such a document" implied in the fact it has been sent from the data box of the petitioner.</p> <p>Vice versa the state authorities may serve documents (including decisions in criminal proceedings) on persons concerned using their data boxes. Such electronic service of documents equals to the regular service and has the same effects.</p>
 DK	<p>In Denmark, neither the prosecution service nor the public sector as a whole has implemented or foresees to implement electronic signatures. However, a few years ago a new system called E-post(electronic mail) was introduced in Denmark. The system requires for all citizens and companies to have a digital mailbox in this system. All mail from the authorities to the citizens and companies in Denmark is now sent by this secured electronic mail system. The Danish Prosecution Service uses the system when sending for example letters to accused persons, victims and witnesses. Mail sent by the E-post system is not signed in hand but solely shows the name of the sender.</p> <p>Via this system it is shown which authority the mail is sent from, and the sender is thereby authorized for the receiver – so he/she can be sure of which authority the mail is from. However the system does not give any certainty as to which specific employee at the authority who has sent the mail – despite of the name indicated in the mail.</p>

 EE	In Estonia, electronic signatures are widely used in the public sector and in the criminal proceedings. Use of electronic signatures has made proceedings much more effective and enables fast exchange of information and documents.
 FI	Some authorities (e.g. Police Board) use already electronic signatures at least in administrative matters. Prosecution Services does not at the moment. In context of criminal proceedings and especially in the use of such EU instruments where judicial authority's validation is needed (EIO, future regulation of freezing) sometimes quite urgently, undue delays could be avoided with electronic signatures. Electronic signatures are planned to be in use in the new system of criminal files (AIPA) which is still under development.
 FR	Le ministère de la justice est mobilisé dans le cadre de projets et expérimentations visant à favoriser la dématérialisation des procédures pénales, laquelle ne peut être effective sans la mise en œuvre de la signature électronique. La signature électronique est prévue à l'article 801-1 du code de procédure pénale. A défaut de signature électronique, un document dématérialisé demeure un simple document de travail et ne présente aucune valeur juridique.
 DE	<p>As to the legal framework, the Electronic Signature Directive was implemented into German law by the "Act on outlining Conditions for Electronic Signatures and for the Amendment of further Regulations" which came into force on 22 May 2001. The law defines different kinds of electronic signatures:</p> <p>'Electronic signatures' are "data in electronic form, attached to other electronic data or logically linked to them and which serve for authentication". 'Advanced electronic signatures' are electronic signatures that a) are exclusively assigned to the signature key holder, b) enable the identification of the signature key holder, c) can be generated by means which the signature-holder holds under his sole control, and d) are linked with the data to which they relate, in such a way that a subsequent modification of the data can be recognized. The term 'qualified electronic signatures' means advanced electronic signatures which are based on a qualified certificate valid at the time of their production and which are generated with a secure signature generation unit.</p> <p>Pursuant to Section 41a of the German Criminal Procedures Code, which came into force on 1 April 2005, declarations, applications or reasons given in support thereof, which are addressed to the court or the public prosecution office and are expressly required by this</p>

	<p>statute to be in writing or signed, may be submitted in electronic form if they bear a qualified electronic signature and are suitable for processing by the court or public prosecution office. In addition to the qualified electronic signature, a statutory instrument may provide for the admissibility of a further secure procedure which guarantees the authenticity and the integrity of the electronic document transmitted. An electronic document shall be deemed to have been received as soon as such department of the court or public prosecution office as is designated for receipt has made a record thereof. If the electronic document transmitted is not suitable for processing, the sender is to be notified and informed of the applicable technical requirements without delay. Since this provision only governs the way of the transmission of documents, a file copy of the electronic document is to be printed out without delay.</p> <p>However, currently this form of transmission is not often used. A main reason is that until today the option of using an electronic file has not been introduced in criminal proceedings in Germany; this situation shall change in the years after 2018. On 5 July 2017, a new law was passed on the Federal level, governing the use of an electronic file in the future. The 'e-file' in criminal proceedings shall be possible as of 2018 and obligatory as of 2026 in order to ensure an exhaustive conversion throughout Germany.</p> <p>Thus, right now we only have entered the phase of preparation for the implementation, but are far from having concluded this process. Given that the problems of security and authenticity of the documents are resolved in a satisfying way, with the 'e-file' once in place we expect a smoother working process and facilitated communication, thus enabling speedier proceedings.</p>
 EL	<p>Under Grecian law (Articles 158 and 160 of GCC), it highlights that contracts don't need a handwritten signature to be seen as credible. They are seen as such as long as legal able individuals have reached an agreement (this can be by agreeing verbally, electronically or by physically signing, however sometimes parties will have to provide evidence in court to support).</p> <p>Since July 2016, the eIDAS regulation has meant that all companies in the EU comply with each other's e-Signature regulations, standardising them across Europe.</p> <p>Greece has foreseen the use of electronic signatures in the public sector and particularly in the context of criminal proceedings. According to Greek Code of Criminal Procedure a citizen can also bring a criminal action electronically (Art 42 par. 5 as amended by Act 4055/2012), and the service of Judgements or orders can be sent also electronically (Act 155 par 1 as amended by Act 4267/2014).</p>

	A new software programme will be ready in a few months that will facilitate the implementation of the use of electronic signature in order to accelerate the criminal proceedings.
 HU	<p>According to the existing legal background, in Hungary it is already possible to use electronic signatures in criminal proceedings in the following situations.</p> <p>The electronic document handling by the authorities during the criminal procedure</p> <ol style="list-style-type: none"> 1. The court, the prosecution service, the investigating authority and the penal institution inside their organisation may use electronic form for written communication according to the Act 19 of 1998 on the Code of Criminal Procedure (from now on mentioned as CP) Section 69/A paragraph (1). 2. The court, the prosecution service, the investigating authority and the penal institution between each other may use electronic form for written communication according to CP Section 69/A paragraph (1). 3. The court, the prosecution service and the investigating authority may request information, data or documents using the power described in CP Section 71, if the organisation to whom the request was sent agrees to use electronic communication and displays its contact information on its homepage. In this case, the organisation sends the requested information on an electronic way, except when the volume or the size or form of the paper documents would cause unacceptable difficulties by the digitalisation, or the authority requested the document in its original form for some reason. (CP Section 69/A paragraph (1a)) <p>According to CP Section 69/A. paragraph (2) and (4), in the above mentioned possibilities the participants of the electronic communication must use such a method, which is accepted as secure electronic communication by the Act 222 of 2015 on the general rules for electronic administration and trust services (from now on: ET).</p> <p>All the official documents sent in an electronic format must be delivered via a secure electronic transfer service and the organisations must issue the documents with the use of an electronic signature, advanced electronic signature or validation stamp.</p> <p>In this form all the electronic documents are treated as a public document.</p>

The new Code of Criminal Procedure (Act 110 of 2017, effective from the 1st of July 2018, from now on mentioned as new CP) has a slightly different regulation according to new CP Section 158.

It announces, that the court, prosecution service and the investigating authority issue all the electronically delivered documents with an advanced electronic signature, an electronic signature based on a qualified certificate or with an electronic stamp, which has to meet all the requirements of the relevant governmental order and act. If it is the case, the document issued such a way counts as a public document.

Also, ET Section 1 point 17 and 17a. declares the courts, prosecution services and investigating authorities as entities obliged to follow electronic case handling.

According to ET Section 2 and 58, this means that all the document deliveries between these authorities must be executed via an electronic delivery system and all the document deliveries from these authorities to clients of criminal proceedings (like the defendant or victims/witnesses) must have a similar electronic form with some exceptions.

For example, defense counsels are obliged to use the electronic form according to ET Section 9 paragraph (1) b), while other clients may choose to use the electronic form or the classic paper documents as well, but according to Act 240 of 2013 on the execution of penalties and other measures, persons kept in penal institutes have no rights to use electronic case handling and therefore must use the paper document form in criminal procedures.

The filing of the indictment

According to CP Section 219 Paragraph (1) and (1a), when the prosecution service file the indictment to the court, it must send the indictment and all digitally available documents in an electronic channel too, or if it is not possible, on a digital data storage device.

If the prosecution service use an advanced electronic signature on the indictment filed to the court in electronic an electronic way, and filed it via an electronic delivery system, then the arrival time of the indictment is counted by the arrival of the electronic form of the indictment, not the arrival of the paper form of the indictment.

Questioning the witness

CP Section 85 regulates the questioning of the witness. According to paragraph (5), the court, the prosecutor or the investigating authority

may permit the witness to make a written testimony following or in lieu of the oral questioning, and in such a case, the witness may affix his certified electronic signature on the testimony taken in the form of a computer file.

New CP Section 181 paragraph (1) b) uses the same perquisites for the witness to give a witness statement in an electronic form.

Order to reserve computer data

CP Section 158/A concerns the order to reserve computer data (a regulation based on the article 16 of the cybercrime convention).

Paragraph (1) states that the compulsion to reserve data means the temporary restriction of the right of disposal of a person possessing, processing or managing data recorded by a computer system (hereinafter: computer data) over specific computer data, in order to investigate and prove a criminal offence.

According to paragraph (4), during this procedure the party ordering the reservation of data may affix its advanced electronic signature on the data to be reserved.

New CP Section 316 contains a very similar rule to the one in CP Section 158.

The possible advantages/disadvantages of the use of electronic signatures

The use of electronic signatures in the criminal proceeding can make it easier and faster to handle statements connected to certain persons in the procedure, like filing an appeal against a court decision.




Furthermore, it facilitates the communication between stakeholders in the criminal procedure.


Disadvantages of the electronic signature


It can clearly cause difficulties and obstructions in the procedure when we try to exchange the currently conventional paper based case handling with the general obligation and therefore mass use of electronic signatures.




This is very different from the current paper form case handling the members of the society are accepting and are accustomed to use.



IT could be difficult also to provide validity in mixed cases, where it is important to issue both electronic and paper form documents.

	<p>However, the fact of these initial difficulties do not influence the worth of implementing a better system.</p> <p>Another possible disadvantage is the following. Most of the providers providing electronic signatures are in the private sphere. Using the electronic signature services of private sphere providers means a form of dependency from the part of the authorities, which involves a security risk. This risk arises particularly if the employment of electronic signatures is a general obligation and covers most of the official communication.</p> <p>In that case a cyber attack against the electronic signature provider can influence the functions of the authorities using that provider.</p> <p>It should be mentioned here the DigiNotar case of the Netherlands from year 2011, when the electronic signature provider of the Dutch authorities became victim of a cyber attack and its digital validation system became compromised, rendering the electronic signature of these authorities invalid.</p>
 IE	
 IT	<p>In Italy the digital signature system is governed by the code of the Digital Administration (Legislative decree of March 7, 2005, n. 82) whose principles apply also to the administration of justice. The decree provides for electronic signature and advanced electronic signature. The art. 21 it provides that the computer document, to which an electronic signature is affixed, is freely assessed in the trial, taking into account its objective characteristics of quality, safety, integrity and immutableness. The computer document signed with advanced electronic signature, qualified or digital, formed in compliance with the technical rules referred to in article 20, paragraph 3, which ensure the identification of the author, the integrity and the immutableness of the document, has the efficacy provided for in article 2702 of the Civil Code. The use of the qualified or digital electronic signature device is presumed to be attributable to the holder, unless it proves otherwise.</p>
 LV	<p>In the Republic of Latvia Prosecutors and employees of the Prosecution Office since 1 March 2016 are using the information system of the Prosecution Office, which provides the possibility to send electronically the replies and notifications to the natural and legal persons. If in the application or complaint received in the Prosecution Office is indicated the address of electronic mail, the documents prepared by the official are sent by means electronically signed document. Prosecutors are using the electronically signed documents not only for</p>

	<p>communication with the public institutions, but also for communication with the private persons, including the parties of the criminal proceedings.</p> <p>In the criminal procedures the replies to the complaints are mainly signed electronically. Additionally in the criminal procedures it is possible to sign electronically also different requests for provision of information and other documents, for example, protests against the court rulings. At the same time it should be indicated that currently as of the moment of the instituting of the criminal procedure all documents related with the specific criminal procedure shall be kept all together in the criminal case in hardcopy form, but electronically signed documents a person directing the proceedings (investigator, prosecutor or judge) shall print out and attach to the files of the criminal case.</p>
 LT	<p>In Lithuania, in the criminal proceedings an electronic signature is used by prosecutors, pre-trial judges and pre-trial investigation officers to sign electronic documents drawn up in the Integrated Information System for Criminal Procedure (Lithuanian IBPS).</p> <p>IBPS was installed and has been operating since 1 February 2016. In the course of pre-trial investigation all prosecutors, pre-trial judges and officers working in the pre-trial investigation institutions use this system, i.e. prepare procedural documents and communicate with each other regarding the issues related to the pre-trial investigation. The procedure that has been approved by the Prosecutor General and the Minister of the Interior provides which documents pertaining to the criminal case must be drawn up in an electronic form and signed by electronic signature; these documents mainly are procedural documents regarding opening and closing of a pre-trial investigation, integration and separation of pre-trial investigations and granting a procedural status to a person. Currently most of the procedural documents in the pre-trial investigation are drawn up in electronic form and are signed by electronic signature.</p> <p>Preparation of criminal case documents and signing thereof in an electronic form enable pre-trial investigation officers, prosecutors and courts to maintain expedient communication in the course of pre-trial investigation and ensure a better security of pre-trial investigation documents, because all institutions work in one integrated information system, in a secured network, and prosecutors do not need to file printed documents when applying the court regarding imposition of procedural coercive measures; pre-trial investigation officers and prosecutors communicate with each other in a very similar way.</p> <p>At present an electronic criminal case is formed at the stage of pre-trial investigation only; upon completion of pre-trial investigation, the</p>

	<p>case is handed over to the court for examination in an electronic form, but courts do not have yet possibility to examine criminal cases presented in electronic form, which means that in the transitional period a printed version of electronic criminal case must be made and later, after pre-trial investigation is completed, presented to the court for examination.</p> <p>Despite technical availabilities, most procedural documents in the IBPS are signed by a safe electronic signature, but are not certified by qualified certificate. Therefore, such electronic documents can be presented only to the institutions using the IBPS. When such electronic document is sent to the third parties (lawyers and other parties of the proceedings), it must be printed, its transcript must be certified and the document is then sent by post or email.</p>
 LU	<p>I. Luxembourg has legally recognized electronic signatures since 2000, with the Law on E-commerce dated 14 August 2000 which implements among others EU Directive 1999/93 of 13 December 1999. Furthermore, a Grand-Ducal Regulation of 1 June 2001 stressed out the conditions applying to an electronic signature to be recognized as legal .</p> <p>These legal provisions are considered as two major advances in securing electronic data and transactions conducted online.</p> <p>The electronic signature is now widely used in the public sector via the LuxTrust system which is an electronic certificate in form of a card (or similar products) which allows you to identify yourself within an electronic system. For example, to access an application that accepts LuxTrust products, such as Internet banking, online payment of taxes or governmental applications. The smartcard allows also a person to sign electronically documents or transactions.</p> <p>II. The electronic signature is not used in the context of criminal proceedings <i>stricto sensu</i> in Luxembourg. However, there are ongoing discussions in the context of the processing of requests based on Directive 2014/41/EU of 3 April 2014 regarding the European Investigation Order in criminal matters which could be sent electronically via a secured channel from one Member State to the other.</p> <p>III. The cooperation with the financial intelligence unit of the office of the state prosecutor at the Luxembourg district court is done electronically.</p> <p>Professionals falling under the scope of the Law of 12 November 2004 on the fight against money laundering and terrorist financing (i.a. financial institutions) file all money laundering and terrorist financing related reports electronically. This applies to spontaneous</p>

	disclosures and answers to requests issued by the FIU. This also the case for the exchanges between FIU Luxembourg and FIUs worldwide which are conducted exclusively electronically.
 MT	
 PL	Poland has provided in its legislation the use of electronic signatures in the public sector. The first institution to use electronic signatures successfully in practice is the Social Insurance Institution. The law stipulates that every prosecution office and court is required to set up an electronic mailbox and have at least two electronic signatures. In criminal proceedings electronic signatures are used by courts and penal institutions e.g in connection with release orders of the prisoners. Courts use electronic signatures also in filing of writs and pleadings in the process of electronic civil proceedings.
 PT	<p>The general Portuguese legal framework of the digital signature is Decreto-Lei n.º 290 -D/99, from 2 August, revised by Decreto-Lei n.º 88/2009, from 9 April (please, find attached).</p> <p>According to this Act, on one hand, it is stated that digital documents can be used and have the same value of written documents (Article 3, para 1). On the other hand, this act states that digital signature can be used, in digital documents, including by public authorities (Article 5, para 1).</p> <p>Besides, Decreto-Lei n.º 116 -A/2006, from 16 June, revised by Decreto-Lei n.º 161/2012, from 31 July (please, find attached), provides the regulation of the State Electronic Certification System.</p> <p>Finally, Decreto-Lei n.º 135/99, from 22 April, revised by Decreto-Lei n.º 74/2017, from 21 June, allow public authorities to make use of electronic communications, when addressing citizens. According to Article 26, para 2, this communication will have the same value of a paper communication.</p> <p>This general framework is applicable to the judicial system.</p> <p>Moreover, regarding private parties, Portaria n.º 1178-E/2000, from 15 December, allows the use of electronic communications to deliver</p>

	<p>documents to a judicial service (namely a Civil Court), submitted to the use of digital signature. Within the civil justice, there is a system in place, allowing the practice of acts only in digital format (the CITIUS system).</p> <p>However, there is not a similar system within the criminal justice. Nevertheless currently it is under development the implementation a such a system. Besides, it is becoming each day more expanded the use of the civil system (CITIUS) within the criminal justice.</p> <p>Within CITIUS, decisions by prosecutors and communications between authorities are already using digital format and digital signature.</p>
 RO	<p>According to the Romanian national law (Art. 142 1 , 143, 170, 170 (21) – (25) penal procedure Code, art. 12, Law no. 302/2004, on international judicial co-operation in criminal matters and Law no. 455/2001), the use of electronic signatures in the context of criminal proceedings is possible and allows to better certify authenticity/integrity of data transmitted as such and also the direct use of proofs transmitted/received in this form during criminal prosecution and trials.</p> <p>More precisely, the use of electronic signatures is provided for data resulted from technical surveillance activities/procedures and for communication of computer data, leading to significantly reducing the time of prosecution, being one of the main advantages, together with the safety of transmission. Also, requests for international judicial assistance are to be transmitted/received in such manner.</p>
 SK	<p>I. Legal framework</p> <p>The Slovak legal order assumes the use of an electronic signature by the execution of the public authority. The details of use of the electronic signature and electronic reception (service/delivery) are specified in:</p> <ul style="list-style-type: none"> • Act No. 305/2013 of Coll. on the electronic form of an execution of competence of public authorities and on the change and amendments of certain Acts (Act on e-Government), • Act No. 272/2016 of Coll. on trustworthy services for electronic transactions in the internal market and on the change and amendments of certain Acts (Act on trustworthy services), • Act No. 301/2005 Coll. Code of Criminal Procedure,

- Public Notice of the Ministry of Justice of the Slovak Republic No. 543/2005 of Coll. on the Administration and Office Order for District Courts, Regional Courts, Specialized Criminal Court and Military Courts,
 - Public Notice of the Ministry of Finance of the Slovak Republic No. 75/2014 on the guaranteed conversion,
- And the internal regulations:
- The Order of the Prosecutor General of the Slovak Republic No. 2/2017 of 10 January 2017 on the application of the Act on e-Government,
 - The Instruction 19/2016 of the Ministry of Justice of the Slovak Republic No. 48652/2016/100 on the application of the Act on e-Government within the authority of the Ministry of Justice.

II. Act on e-Government

Section 2 of the Act on e-Government outlines the scope of the act as follows:

“(1) This Act relates to the execution of the public authority electronically in the extent of the competence of the public authority according to separate regulations.

(2) This Act does not apply to

- a) exercise of the public authority electronically and to electronic communication of the public authorities between each other containing classified or sensitive information,
- b) exercise of the public authority electronically by the National Bank of Slovakia,
- c) information systems of the public administration relating to the ensurance of the defense of the Slovak Republic, security of the Slovak Republic or containing classified information,
- d) information systems of the public administration containing data processed for the purpose of providing healthcare and to information systems containing data on the health condition of a person for the purpose of implementing a public healthcare insurance,

	<p>e) information systems created by international organizations or by in accordance with provisions of international law and information systems created by the European Union</p> <p>f) delivery via publication in the official register,</p> <p>g) providing access to information on the basis of a request pursuant to a separate regulation.”</p> <p>Pursuant to Section 3 a) of the Act on e-Government the exercise of the public authority means “ action of the public authority within the scope regulated by separate regulations, related to the the matters of rights, legally protected interests and obligations of natural or legal persons.”</p> <p>Pursuant to Section 17 para 1 of the Act on e-Government the public authority is “obliged to implement electronically the exercise of the public authority according to this Act; whereas such obligation does not apply in relation to actions within proceedings on rights, legally protected interests or obligations of persons,</p> <p>a) on which the separate regulation specifically determines that the public authority executes them exclusively in a sheet form,</p> <p>b) the separate regulation determines or enables to execute them orally, by an implied expression of will or by presenting a matter that has not a sheet or electronic form, or</p> <p>c) those which consist of executing an activity such as oral proceeding, local detection, execution of control or supervision on the spot, inspection, access to files, bringing forward a person and other similar acts taking place outside of the official premises of the public authority.“</p> <p>As regards the authenticator pursuant to Section 21(1) of the Act on e-Government defines (unless Section 22a does not specify differently) that „for the purposes of authentication only such authenticator may be used, which is</p> <p>a) an official authenticator that is an identification card with an electronic chip and a personal security code in accordance with a separate regulation or a document on residence with an electronic chip and a personal security code in accordance with a separate regulation or</p>
--	---

b) an alternative authenticator of unique and final succession of symbols which alone does not have any significance value if it accessible only as a succession of these symbols, as a tool, procedure or its combination. The issue of an identification card with an electronic chip and a personal security code is determined by a separate regulation. The issue of a document on residence with an electronic chip and a personal security code is determined by a separate regulation.“

Subsequently Section 22aa of the Act on e-Government defines the authenticating certificate as „an electronic document presenting the electronic identity of the person it was issued to and is used for the purpose of identification and authentication in the access to the information system or in electronic communication relating to the exercise of public authority or for the purpose of access to the electronic box or for the disposal of the electronic box. The authenticating certificate contains information on its purpose and the identifier informs on the person it was issued to.“

III. Particularities within the Criminal Proceedings

The Code of Criminal Procedure defines in the Section 62 para 1 and Section 66a the use of the electronic signature within the criminal proceedings. Pursuant to Section 62 para 1 of the Code of Criminal Procedure submission is always assessed by its content, even if it is incorrectly marked. It can be made in writing, orally into the protocol, by cable (telegraph), fax or electronic means signed with a qualified electronic signature pursuant to a special Act, or without a qualified electronic signature. Submissions made telegraph, fax or electronic means without a qualified electronic signature must be confirmed in writing or orally into the protocol within three working days, otherwise the submission shall not be handled.

Therefore the Code of Criminal Procedure distinguishes a submission made by electronic means without a qualified electronic signature and the submission made by electronic means signed by a qualified electronic signature. A specific category is the elaboration of Criminal Complaints. According to the internal regulations of the Prosecutor's Office of the Slovak Republic, each prosecutor is obliged to carry out a Criminal Complaint regardless of the fact whether it has been submitted by electronic means signed by a qualified electronic signature or without it. Thereby it is not necessary to wait for its confirmation in a written or oral form into the Protocol while carrying out Criminal Complaints submitted by electronic means without a qualified electronic signature.

Pursuant to Section 66a of the Code of Criminal Procedure „According to this Act the separate regulation on the electronic form of the execution of a competence of public authorities does not apply to the service by electronic means“. Therefore the Act No. 305/2013 Coll. on

the electronic form of competence of public authorities and on the change and amendment of certain Acts is not applicable to the service of documents in criminal proceedings .

The serving of procedural documents in the criminal proceedings is regulated by Section 65 and Section 66 of the Code of Criminal Procedure.

In Section 65 para 8 of the Code of Criminal Procedure the option (not obligation) of serving the documents also by electronic means signed by a qualified electronic signature is regulated for the law enforcement authorities and for the court to serve them to the accused, defence counsel, the victim and their representative, reporting person, legal representatives, participating person and its representative, and to penitentiary and custody institutions.

In order to implement this option the following general legal conditions set up in Section 31 para 2 of the Act on e-Government must be complied with:

„The provisions on the electronic transmission (service) shall not apply and the transmission (service) shall be regulated by the provisions on the transmission (service) according to separate regulations if:

- a) the electronic box of the recipient is not activated,
- b) a separate regulation defines that they shall be served exclusively in a sheet form, or
- c) is served to persons serving the sentence of a deprivation of liberty, in detention, persons placed into institutions executing maintenance and protective education, or to those utilizing diplomatic privileges and immunities.“

IV. The Information System of the Prosecution Service

Despite the stated information, all documents in the information system of the Prosecution service of the Slovak Republic are issued as „an electronic official document“ which must be authorised.

From a technical point of view, the Prosecutiion service operates with the information system PTCA which is in the specified matter adjusted to the required functionality and enables the creation, signature, transmission as well as the reception of electronic decisions

signed by a qualified electronic signature within the Slovak Republic.

An electronic official document which is authorised is the first original of a document. It is possible to execute the authorization pursuant to Section 23 para 1 of the Act on e-Government either by a qualified electronic signature and a mandatory certificate or by a qualified electronic seal with an attached time-stamp.

The authority of the Prosecution service that has issued the electronic official document may issue from it an original counterpart in a sheet form pursuant to Section 31 para 3 of the Act on e-Government or to issue an authorized conversion pursuant to Section 36 of the Act on e-Government. The power of other persons to make the authorized conversion pursuant the Act on e-Government remains untouched.

The original counterpart in a sheet form issued according to the procedure in Section 31 para 3 (the issue of the original counterpart of the electronic document in a sheet form) or to Section 36 (authorized conversion into a sheet form) of the Act on e-Government, shall be signed before being expedited by the person who issued the decision and is responsible for the correctness of the original counterpart. The original counterpart shall be verified by an official stamp if the separate regulations define to do so.

The above-stated regulation of the examination of the documents submitted by electronic means is fully complying and does not cause any problems in the practice of law enforcement authorities. The advantage of this regulation is the progressive implementation of the electronization a informatization into the criminal proceedings. There weren't noted any disadvantages of the use of electronic signature.

Details on applying the Act on e-Government within the Prosecutor's Office are regulated by the cited order of the Prosecutor General.

V. Procedures within the responsibility of the Ministry of Justice

The Instruction of the Ministry of Justice of the Slovak Republic 19/2016 in Art. 2 specifies that the decision, request, statement, opinion or other document issued by the Ministry, District Courts, Regional Courts, Specialized Criminal Court, Judicial Academy of the Slovak Republic, Center for Legal Assistance, General Directorate of Prison and Judicial Guard, bodies for the execution of imprisonment sentence, bodies for the execution of detention and institutes executing the sentence of deprivation of liberty for juveniles and the hospital for the accused and convicted, is issued always as an electronic official document and must be authorized.

However, this Instruction does not pertain to the official communication to the indicated authorities between themselves. If it does not


concern a procedure relating to the regulations of the proceeding before the public authorities, it shall not be used for an official communication between these authorities and other public authorities, if these are not relating to the public authority and the participant of the proceeding and to the matter that does not relate to the Act on e-Government.


In accordance with the Instruction, the electronic official document is authorized by the qualified electronic signature with a mandatory certificate if the separate regulations determine that the document shall be signed by a natural person representing a public authority (e.g. judge) or if the document is issued by a natural person representing a public authority (e.g. the Minister). In other cases the document is authorized by a qualified electronic seal with an attached time-stamp.


Despite the fact that according to the Act on e-Government the electronic transmission (service) does not apply to the criminal proceedings, the Public notice of the Ministry of Justice of the Slovak Republic No. 543/2005 Coll. on the Administration and Office Order for District Courts, Regional Courts, Specialized Criminal Court and the Military Courts assumes the issue of electronic official documents.



In addition the Section 76 of the Statement (Provisions of imposing the execution of the sentence of deprivation of liberty) assesses that:

„The institution for execution of the sentence of deprivation of liberty where the convicted was last located shall without delay submit a notification to the court deciding on the first degree on the transfer of the convicted to another institution for execution of the sentence of deprivation of liberty, on the commencement of a protective treatment, on his escape or arrest, on his death, on the suspension of the execution of the sentence, on a conditional release, as well as in the case the convicted was released as a result of having executed the imposed sentence, was granted a pardon, an amnesty, a conversion of the rest of the sentence of deprivation of liberty to a sentence of house arrest or any other reason. In the case of a conditional release, the institution for the execution of the imprisonment sentence shall notify also the court which issued the decision of the conditional release. In the case of releasing the convicted due to a conversion of the rest of the sentence of deprivation of liberty to a sentence of house arrest, the institution for the execution of the sentence of the deprivation of liberty where the convicted was last located shall immediately notify after having released the convicted the correspondent district court where the house arrest shall be executed; the notification contains information on the time of the release and is served to the court by electronic means.”

 SI	<p>AD1:</p> <p>The Electronic Signature in the Republic of Slovenia is regulated by the Electronic Commerce and Electronic Signature Act (ECESA) and Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. The Act regulates Electronic Commerce between two parties on general basis and it is not limited to regulating commerce between Courts and involved parties.</p> <p>The electronic signature is more extensively regulated in third chapter of ECESA along with the operation of the certification service providers, who represent an inevitable condition for the use of the electronic signatures. ECESA defines the electronic signature very broadly and in general as data in electronic form, which are included or logically linked with other data. Furthermore, it is designed to verify the authenticity of the data and the identification of the signatory:</p> <p>Art. 2(2) of ECESA: advanced electronic signature means an electronic signature, which meets the following requirements:</p> <ul style="list-style-type: none"> • that it is uniquely linked to the signatory; • that it is reliably capable of identifying the signatory; • that it is created using secure signature creation device that the signatory can maintain under his sole control; • that it is linked to the data to which it relates in such a manner that any subsequent change of the data or the connections between the data and the signature are detectable); <p>Electronic commerce was established in procedures first by General Administrative Procedure Act in 2004, followed by Civil Procedure Act three years later. In those procedures electronic signature is widely used. At this point it can be also mentioned that our Ministry of Public Administration manages e-Government portal for electronic services for citizens. User needs qualified digital certificate and signature component for signing the application. Using this portal, it is possible to submit an application for different administrative procedures.</p> <p>It is reported that electronic commerce considerably rationalizes procedures.</p> <p>With reference to the criminal proceedings, Article 76 of Criminal Procedure Act foresees sending submissions in electronic format to the</p>
--	--

	<p>criminal courts that shall be signed by a secure electronic signature, certified by a qualified certificate. The same article also obliges Minister of Justice to lay down the condition and methods for the electronic filing of submissions in an electronic format, the format of writing of these applications, and the organization and operation of the information system of the court. At the moment, only Rules on electronic operations in civil procedures (the Rules) are valid and applicable, but there is an Amendment in preparation that will include also criminal procedures. Currently, The Rules refer to the definition of advanced electronic signature as set in ECESA (along with definitions on terms »time stamp« and »qualified certificate«), and it is expected that this will not change with foreseen Amendment.</p> <p>Considering both, the applicable Rules and the draft Amendment, they regulate:</p> <ul style="list-style-type: none"> • structural organization and operation of information system “e-Sodstvo” (“e-Court”), administrated by Centre for Informatics at Supreme Court of the Republic of Slovenia; • conditions and means of filing digital submissions; • format of digital submissions; • defines secure electronic means for serving documents; • lays down the conditions under which the provider may get an authorization for providing electronic delivery service and • set the tariff for intermediation in delivering to safe electronic. <p>However, at this moment we still operate only with files in physical form although we have legal framework to start operating with digital files. Both, courts and state prosecution service, have already started using their own (different) information systems that are aiming to gradually switch from operating only with physical files to operating exclusively with digital files.</p>
 ES	<p>The electronic signature was introduced in the context of the public sector within the Spanish administration by Law 59/2002 of 19 December on electronic signature, later amended by Law 25/2015 of 28 July which provides legal status to the so called “signature in the cloud” whereby the password to access the signature is not physically in the user’s personal computer but stored in an accessible internet service provider.</p>



	<p>The law makes a distinction between the so called “advanced electronic signature” and “recognised electronic signature”, being the latter equivalent to the signature in writing.</p> <p>Further than that, Royal Decree 3/2010 of 8 January regulates the National Security Scheme within the electronic administration, aimed at establishing the principles and requirements of the security policy for the protection of information, including those related to the electronic signature, electronic certificates, etc. Moreover, Royal Decree 4/2010 on Interoperability National Scheme states that the policy on electronic signature and certificates of the State’s General Administration establishes the interoperability framework for authentication of electronic signature within its scope of competences. This policy can be used by other public administration (regional or local) to define their own electronic signature regulations.</p> <p>At least seven different case management systems coexist in the judicial national system in Spain. The digital signature within the territory under the competence of the Ministry of Justice is being gradually implemented; the implementation will come to an end by July 2018. Some autonomous regions (where the competence for management of resources in the field of Justice Administration have been transferred) have in place their own case management systems. With regard to the Prosecution Service, the implementing plan called Digital Prosecution Service is also being gradually implemented throughout the national territory, mainly in judicial areas other than the criminal one though steps have been taken also in this field. In the autonomous regions (where the competence for management of resources in the field of Justice Administration have been transferred) the situation differs to a considerable extent.</p> <p>In the context of criminal proceedings, the implementation of electronic signature is foreseen by the applicable legislation but its enforcement across the national territory is uneven due to the complexity and fragmentation of the case management systems.</p>
 SE	<p>Swedish prosecutors may file all documents to the court electronically, including the indictment. Almost 100 percent of the indictments are electronically transmitted and electronically structured. If filed electronically, the indictment shall either be signed with an electronic signature or be transmitted in an equally secure manner.</p> <p>A Swedish public prosecutor can order summary imposition of a fine. If the suspect confess the crime in the summary imposition and approve to the imposition, it has the same effect as a court ruling. Today the suspect must approve to a summary imposition by signing a declaration in writing. In a near future, it will also be legally accepted for the suspect to sign the declaration by using an advanced electronic</p>


	<p>signature. However, technical implementation of this new possibility is yet to be planned.</p> <p>The use of electronic signatures has many advantages; it promotes productivity in many aspects and is more environmentally friendly. Technical implementation to support electronic signatures in various digital services and tools might be an initial challenge.</p>
 NL	<p>In the Netherlands electronic signatures have been used in the context of criminal proceedings, for some years. Since December 1, 2016 it is legal to use signatures for all the documents of a criminal case file (art 149a lid 3, 138e and f Criminal Procedure Code). The electronic signature has the same value as the “Blue Ink Signature”.</p> <p>Hence it is legally possible to make use of a “digital ” file in the course of the whole legal procedure (starting from the police, via Public prosecution, the courts and lawyers).</p> <p>Electronic signatures will make the paper file redundant. This is the most important advantage as the electronic dossier enables quicker exchange of documents, neither files nor pages get lost and all authorised participants in the process can access the complete file 24/7.</p> <p>Implementation and use of electronic signatures for the Public Prosecutor Office are being prepared on a national level.</p>
 UK	<p>The United Kingdom has provided for the use of electronic signatures which extends to their use in criminal proceedings. Under the Electronic Communications Act 2000, electronic signatures are admissible in evidence in any legal proceedings. Statements adduced in criminal proceedings need to be signed but an electronic signature can be used.</p> <p>The primary concern is that the signature, whether electronic or a ‘wet signature’ is authentic. If there is a dispute about the authenticity or integrity of a document, an enquiry would need to be made into the provenance of the document, whether the signature was a digital or a ‘wet’ one.</p> <p>Electronic signatures can be presented in a variety of ways, including a graphical digital representation of the witness’s usual signature, a scanned copy of a “wet signature”, by use of a password and by the use of an electronic signature authorised or certified by the maker.</p> <p>A possible, but unlikely, risk of digital signatures is that the contents of a statement could be altered after the witness has signed it. This is</p>




could be addressed by requiring a digitally signed statement to be saved to a non-editable format, which would be time-stamped, with procedures in place to ensure that the correct version of the statement is recorded and monitored.





The ability to transfer a statement with a digital signature from the witness, and then then electronically through the system without the need to copy and scan, is a significant advantage. The retention and storage of hard copies of documents is removed from the process. If additional statements are required, this can be addressed efficiently, irrespective of the geographical location of the witness.


2. To what extent does your Member State make use of digital information exchange in the context of criminal proceedings? Do you see any advantages/disadvantages to such use and/or do you see any margin for further use of digital tools in criminal proceedings?



Member State	Replies and observations
 AT	<p>In Austrian Justice electronic legal communication (ELC) with the authorities of police is established since 2008. Electronic communication among justice organizations (prosecution departments and courts) has proven particularly effective as well. In the future we will focus on the expansion of cognitive knowledge management tools in order to provide better support for increasing complex criminal proceedings. In criminal proceedings a special system has been developed to ensure secure communication with telecom providers. Orders of prosecution services to reveal traffic/subscriber/location data are forwarded by the police authorities to telecom providers and replies from the telecom providers are sent back encrypted and via a secure channel. Access to such data must be recorded in such a way that the log data are protected against alteration to verify and trace the procedure.</p>
 BE	<p>The electronic exchange of reports and documents in criminal proceedings in Belgium is – apart from some projects - still in its infancy and what is possible to this day is still not working optimally or was only partially implemented.</p> <p>The vast majority of interactions in criminal matters (summons, notices of court, ...) are still being done through paper correspondence.</p> <p>Moreover, we do not have a digital criminal record, so that electronic access for lawyers or citizens is still unavailable and they have to displace themselves to take note of a criminal record. The intention was to scan all criminal records in judicial investigations through JustScan, and thus to manage them digitally, but this is not yet automated and is used only in major criminal records.</p> <p>What is currently used is the 'e-Deposit', which allows electronic depositing (uploading) of documents (conclusions, pieces of bundles, ...): documents in a particular file can be deposited at an official body through an application, immediately sending a delivery receipt and</p>

	<p>because e-Deposit works with an e-ID authentication, the system is very reliable. However, this possibility - as far as criminal proceedings are concerned - is currently provided at the level of courts of appeal only (ie not for the police courts and the correctional courts) and, in addition, only lawyers can use e-Deposit.</p> <p>Currently action is being taken to create a central database for judgments (VAJA), and it is the intention that these could be consulted by lawyers and citizens as well.</p> <p>The benefits of digital information exchange include the major simplification of administrative work, time savings allowing those involved to spend their time on more value adding tasks, reduced workload, cost savings, etc. Moreover, as already stated, the demand for further evolution of the use of digital devices in criminal matters is very high.</p>
 BG	<p>In the Republic of Bulgaria, e-signature is widely used in the public sector but is generally related to the civil turnover.</p> <p>Art. 319f of the Criminal Code covers crimes related to the Electronic Document and Electronic Signature Act (EDESA). According to the text: "Where a provider of information services acting in this capacity violates provision of Art. 6, para. 2, sub-paragraph 5 of the Electronic Document and Electronic Signature Act, he/she shall be punished by fine of up to BGN five thousand, unless subject to severer punishment."</p> <p>Subject of the crime are the public relations regulated in the EDESA, related to sending, receiving, recording and storing of electronic statements.</p> <p>It is a formulaic norm and regarding items from the objective part of the criminalization, it makes reference to another regulation – the Electronic Document and Electronic Signature Act.</p> <p>There is a special subject of the crime. Not any criminally responsible person can be the author of this criminal violation.</p> <p>First, it is necessary to provide information services. The content of this activity can be taken from the provisions of Art. 93, i. 23 of the Criminal Code. A "provider of computerized information services" is any individual or entity that provides opportunities for communication by means of a computer system or that processes or stores computer data with regard to the above communication service or its users. When that provider is an entity, the subject of the crime will be the individual responsible for storing the information referred to in Art. 6,</p>

	<p>para. 2, i. 5 of the Electronic Document and Electronic Signature Act, regarding the time and source of submitting the electronic statement.</p> <p>Second, it is necessary that the entity is a mediator of the electronic statement. Pursuant to the provision of Art. 6, para. 1 of the EDESA, mediator of the electronic statement is a person who, by assignment of the titular, sends, receives, records or stores an electronic statement or performs other services related to it. This requirement stems from the fact that the obligation under Art. 6, para. 2, i. 5 of the EDESA - to store the information on the precise determination of the time and source of the transmitted electronic statements for a period of one year – has been assigned under the same Act to the mediator of the electronic statement.</p> <p>Subject of the crime is the information under Art. 6, para. 2, i. 5 of the EDESA.</p> <p>Form of guilt – intention.</p>
 HR	<p>Exchange of digital information in criminal proceedings in Croatia is primarily applied in exchange of information regarding bank accounts, and information between state bodies, e.g. the delivery of requested information from the Anti-Money Laundering Office. The advantage of such information exchange is primarily the speed, which expedites the activity of state bodies.</p>
 CY	<p>Currently only few systems exist that make use of digital information exchange in the context of criminal proceedings. Further developments are in place for the use of digital tools in the Public Sector.</p>
 CZ	<p>There is a uniform information system (The Register of Criminal Proceedings - RCP) used by the law enforcement and prosecution in the Czech Republic. The pilot project was launched in 2004 and has been continually upgraded and developed until today. It serves not only as databases, a statistic and search tool but it is also designed to composition of electronic copies of criminal files.</p> <p>Examples of other RCP functionalities: documents and case management, composition and storage of documents and forms, communication and sending documents through data boxes, statistics, search in central registers, synchronisation between the RCP and other registers, on-remote access to evidence and copy of the criminal file by prosecutors.</p> <p>The RCP is currently being upgraded into ELVIZ system which shall overcome some incompatibilities between the systems of the courts,</p>

	<p>prosecution and the police and should create a fully electronic criminal file which will be equal to its current paper version.</p> <p>Before going forward with other legislative proposals we find it reasonable to define the basic terms like “public”, “cyberspace”, “etc. as well as to answer questions concerning jurisdiction and fundamental rights in the given context.</p>
 DK	<p>In Denmark a project regarding Electronic proceedings in the courts has begun this year. The actual case file is send from the Prosecution Service to the court and to the defence attorneys electronic by secured e-mail. During the court proceedings the case is handled by the Judge(judges), the attorneys and the prosecutor electronic on tablets. Pictures, videos or audio is shown or played in the courtroom on big-screens.</p> <p>This system makes the transport of the case files much more easy for all the parts involved, especially in big cases. Also the electronic handling of the case file during the proceedings has the advantage, that the prosecutor can present the case electronic with all the possibilities it implies.</p>
 EE	<p>In Estonia, the exchange of digital information in criminal proceedings is everyday practise. Almost all documents between parties are exchanged digitally. The criminal files are disclosed to the lawyers also in digital way.</p>
 FI	<p>Investigation authorities such as police, customs, border guard uses digital information exchange (EC3, Siena). Digital tools in criminal proceedings are badly needed. Cases come from police to prosecutor mostly in paper, sometimes the protocol is electronic, but not always. From prosecutor to court the indictment goes electronically and protocols in paper or in cd. For some years now the new system (AIPA) has been under development. In that all material would be forwarded police – prosecutor – court – defence lawyers in electronic form.</p>
 FR	<p>La loi du 3 juin 2016 a modifié l'article 19 du code de procédure pénale afin de prévoir expressément la possibilité pour le procureur de la République d'autoriser que « <i>les procès-verbaux dressés par les OPJ ainsi que les actes et documents y relatifs, lui soient adressés sous forme électronique</i> ».</p>

	<p>La loi du 16 février 2015 relative à la modernisation et à la simplification du droit et des procédures dans les domaines de la justice et des affaires intérieures a modifié l'article 803-1 du code de procédure pénale relatif à la communication électronique en matière pénale, afin de généraliser le recours à la communication électronique au cours de la procédure pénale et d'éviter le recours à des envois postaux. Les justiciables peuvent ainsi être convoqués ou recevoir des avis ou documents par courriels ou SMS.</p> <p>Parallèlement au logiciel de Numérisation des Procédures Pénales (NPP), ont été mises en œuvre des expérimentations de transmissions dématérialisées de procédures pénales par courrier électronique, basées sur l'accord cadre national signé le 11 décembre 2008 entre le ministère de la Justice et la gendarmerie nationale. Les unités de la gendarmerie nationale peuvent depuis lors transmettre aux tribunaux de grande instance, par voie électronique, les procédures donnant lieu à poursuites pénales ou les procédures contre auteurs inconnus.</p> <p>En l'absence de signature électronique, ces pièces - dénommées « équivalents électroniques de procédures » (EEP) - n'ont pas, à ce jour, de valeur légale. Néanmoins, ce dispositif génère des économies de temps, de moyens et permet aux parquets d'assurer un contrôle optimal des enquêtes.</p>
 DE	<p>Digital information plays a major role in criminal proceedings not only pertaining to cyber-crimes, but in almost every field of crime. The increasing importance of digital communication in almost every area of social life entails a growing relevance of digital evidence. Consequently, in Germany the use of digital evidence in the context of criminal proceedings is increasing.</p> <p>In order to facilitate the effectiveness of investigations, prosecution authorities and police exchange information by using digital means. For example, the basic data concerning the perpetrator and the crime as well as parts of the file are scanned and digitally transmitted to other authorities.</p> <p>However, there are still difficulties to guarantee secure ways of transmission. Thus, the authorities still tend to abstain from using electronic transmissions due to the necessity to maintain confidentiality. Furthermore, the authorities have to comply with the relevant provisions of the data protection law.</p> <p>With the 'e-file' at hand, there will be a new situation. Certainly, prosecution offices will benefit from new technical possibilities of communication. Also, there will remain further room to make criminal investigations more effective and to strengthen the close coopera-</p>

	tion between police authorities and prosecution offices, including authorities of other Member States.
 EL	Already Greek Police Cooperation Department operate successfully referring the execution of investigations and European Warrant Arrests as digital information are being exchanged during intranet.
 HU	<p>The currently working digital document exchange system</p> <p>As mentioned in answer 1, in Hungary currently there is no obligation to use electronic communication in the criminal proceedings. It is just a possibility to handle the document exchange between authorities, or the document deliveries to clients in an electronic way.</p> <p>This means currently – apart from the deliveries of indictments to the courts in an electronic channel – the deliveries of physical storage devices (DVD disk, harddrive), which requires a steady financial cost to upkeep. The digital storage devices are sent with the paper form documents together, which means that they are neither faster to arrive, nor safer: the possibility of losing, damaging a storage device during the delivery is similar to the dangers of the damage or destruction of paper form documents.</p> <p>The digital document exchange of the future</p> <p>From the 1st of January 2018, the authorities and certain clients will have an obligation to continue electronic communication. Until 31st of December 2019, this can happen with the delivery of physical storage devices if certain conditions are met.</p> <p>The implementation of a complete electronic document delivery system requires a bigger amount of resources to invest, as this requires the set up a storage for a huge amount of data, and also a solution to send and receive this data, which is only possible through a high bandwidth communication network.</p> <p>After the development of such a network, it will have the certain advantage, that it will be possible to cut the delivery time of the documents to almost zero, and it also eliminates all the risks of losing and damaging/destroying a data storage media during the delivery.</p> <p>During the electronic delivery of the documents, validity can be properly ensured by electronic signatures.</p> <p>It must be taken into consideration however, that the electronic documents are more easily distributable in great numbers. For this reason,</p>

investigations might become more transparent, the defendants and the defence counsels can harmonise their defence tactics more easily, as it is easy to share with each other the testimonies, records on investigative measures, which would otherwise accessible by a few of them.

It is easier also to put a pressure on the investigating authorities with continuously informing the society on the stance of the criminal proceeding and showing it in a disadvantageous aspect.

Yet there are not only disadvantages for the authorities from the digital case handling, their possibilities are also growing.

The authorities can easily inform the society on the status of the proceeding all the same in an electronic way, and the cooperation between authorities can be faster too. One of the good examples is the following.

It is very frequent with crimes committed on the internet, that the crime is not connected to one geographical location like a city or town. For example, an advertisement offering something to sell by a fraudster can victimise anyone around the country, or even someone outside the country. This can cause investigations going parallel to each other, which drains the resources of the authorities without a real reason, as these cases could be handled together more effectively. (The data request to the service provider where the advertisement was uploaded should be asked only once for information, the victim or the suspect can be heard about all facts in one testimony each instead of repeated hearings, etc..)

However, to merge cases continued by different authorities, first the connecting cases are needed to be identified.

This can be executed effectively with electronic communication. It is possible to search the system for similar cases and identify them.

The information exchange between authorities can speed up also the document deliveries between authorities, which can help to make faster the case handling, even if the cases can not be merged for some reason with the similar offences.

The digital evidence handling

The other aspect of the digital information exchange is the field of digital data handling as evidence handling. This involves among others the computer systems and validated copies created from their content, if they are holding the traces of a crime committed.

The digital evidence is currently being handled via physical storage devices (DVD, harddrive) with evidence bags, and hash values to prove that they remained valid and unchanged.

In the society it is very popular to use digital devices: mobile phone, tablet, digital camera, digital security camera, smart watch, electronic fitness equipments, tabletop computers, smart refrigerators, smart TVs, on board computer system of cars, etc.

Such tools are recording and storing an ever growing amount of data, which can be relevant for criminal procedures, and therefore the need arises all the time more frequently to secure such data, examine it and cross-check it with other information, or execute searches in such a database. In a lot of case it is possible to create a “profile” of the user using these devices, like his personal life, behaviour, daily routines, which is similar to the profile creation of homicide cases, where this profile is being used to identify the possible offender.

As the digital storage devices are very diverse, and their storage capacity grows all the time, the resulting big amount of data is very difficult to be properly examined without the help of specific softwares and big capacity computers.

Such properly equipped and staffed “labs” are yet very expensive to upkeep, and for this reason it is not cost effective to create a new lab for all the local level authorities.


Creating a secure electronic communication network can also help to solve this problem, as it will be enough to set up new labs only for certain regions, and all the data required to be examined can be sent in an electronic channel, without any more expenditure.


Digital investigating measures


In the case of investigative measures, like the hearings, it is extremely important to properly record all the circumstances and statements. This can include the behaviour the officials present or, concerning the person being heard, all the information including the facial movements, tone of speech, body language representing some emotion.

In some cases this can be a very important data, especially when there is a need to check if all the procedural rules for the certain investigative measure were obeyed or the evidence should be dismissed because of procedural mistakes. It can be important also, when there is no chance for further evidence to be found and the existing evidence is not enough to easily decide upon.



In similar situations it is possible to record the picture and the sound during the investigative measure. In Hungary there are very detailed



	<p>rules for executing and recording the hearing of minor witnesses under age 14 for example.</p> <p>Creating, storing, sending and using a video capture of the investigative measure is more easy on a digital device. This can make it possible to use detailed recording methods even in small importance cases, instead of minutes simply summarising the events happened during the investigative measure.</p> <p>It is a disadvantage of the electronic information exchange that the electronic data can be easily copied, and the computer systems are vulnerable against cyber attacks, where attackers attempt to gather information about the procedure. It is an easier way to attack a system in the cyberspace, than acquiring the paper form documents of a case delivered by real life officials.</p> <p>It is easier also to distribute copies of digital documents, than those of the paper form documents.</p> <p>Therefore the system containing data on criminal cases should be properly protected, which is an important task and a great challenge.</p> <p>By the electronic information exchange it is a further challenge also to handle the transfer of big volume data. According to the ET Section 108/A. § - 109 §, this can be evaded with transferring physical storage devices until the 31st of December 2019.</p> <p>Until that date, all the authorities has to be prepared to have a solution to directly transfer big amounts of data, including an ever growing number of video and sound records of investigative measures.</p> <p>This means a considerable amount, and it is necessary to find a technical solution to handle this.</p> <p>Connected to this, as a further problem it can be mentioned, that the private persons, as clients of a procedure, cannot be expected to have such broadband internet and storage capacities as an authority, the electronic documents has to be handled to them in such a way, where they can access it with the tools and broadband they have in possession.</p> <p>Therefore the delivery of electronic documents to clients can mean a further difficulty, adding to the difficulty with finding a solution between authorities.</p>
 IE	



 IT	<p>On the organizational level the Italian Ministry of Justice and some Prosecutor's offices are experiencing a system of computer transmission of the news of crime.</p> <p>The experimentation is in advanced phase and is showing many positive aspects on the plan of resource saving and efficiency of data transmission. Privacy issues have been reported in particular regarding judicial data and specifically data on telephone wire tapping.</p> <p>The SCIP- (information system of criminal cognition) fixed an unitary platform of the Registry of the proxies)-now covers all the judicial offices of I grade but is only partially accessible to lawyers. The communications and notifications via the SNT system (telematic notifications System) and PEC Tiap have increased by 50% from 2015 to 2016, 4.6 million in absolute value; Whereas the use of telematic communications has achieved a saving of 67 million . Now the Ministry and judicial offices have completed the plan for the adaptation of the requirements for the safety of personal data, especially with reference to interception operations.</p> <p>The Telematic criminal process is the subject of a specific project by the Italian Ministry of Justice.</p> <p>The legislator began to speak, for the first time, of "telematic" notifications in the criminal field almost six years ago, when the system through which they are carried out, i.e. the Certified e-mail (hereinafter PEC "Certified Electronic Post"), had already found a specific discipline in the D.P.R. 11.02.2005, No. 68 ("Regulation laying down provisions for the use of Certified electronic mail") and had already been chosen for communications and notifications in the civil process.</p> <p>If the rules for the use of the PEC and the C.A.D. date back to 2005, and if the telematic communications had already been established as compulsory in the civil process (in 2008), it is only at the end of 2008 and then between the end of 2009 and the beginning of 2010 that we start to speak, even in the criminal process, of telematic notifications : The PEC, understood as an instrument of telematic transmission of notifications, was in fact introduced by the legislator, for the first time in criminal proceedings, by art. 4 of D.L. 29.12.2009, No. 193, Conv. With conv.in L. 22.02.2010, No. 24. On 14 March 2011 .</p> <p>Art. 74 of the Development Decree, approved by Decree Law 18.10.2012, N. 179 and converted with the law 17.12.2012 n. 221 provides that in civil proceedings, the Registrar's communications and notifications are carried out exclusively by telematic means to the certified e-mail address resulting from public lists, in compliance with the regulations, including regulations, concerning the subscription, transmission and receipt of computer documents. In the same way, the notification shall be carried out by person other than the defendant</p>
---	---


	<p>in accordance with articles 148, paragraph 2-bis, 149, 150 and 151, paragraph 2, of the Code of Criminal Procedure. The notification report shall be drawn up in an automatic form by the computer systems supplied to the registry. The notification or communication containing sensitive data shall be carried out only for extract with contextual provision, on the website identified by the administration, of the Integral Act to which the consignee is accessed by means of the instruments referred to in article 64 of Legislative Decree n. 82 of 7 March 2005 (Code of the Digital administration) .</p> <p>The extraordinary plan for digital justice was launched with the objective of equipping within 12 months all the participating judicial offices of a computer kit. Almost all the judicial offices have joined the plan. On the basis of the order of accession, a deployment plan has been drawn up which groups the judicial offices in 13 batches of intervention for the delivery, installation and implementation of the computer equipment. In the criminal trials the telematics notifications were also recently extended to the proceedings before the Supreme Court .</p> <p>The Italian Ministry of Justice will invest in the near future the resources available (both the European Structural Funds pon and the “Stability Law” 2017) in videoconferencing and computer security of interception infrastructures, buying dedicated servers and preparing a secure network.</p>
 LV	<p>In Latvia currently is planned to develop the project of e-case related with digitalization of the criminal and administrative violations proceedings at all stages of the proceedings in principal institutions dealing with these proceedings – in judicial institutions, Prosecution Office and investigatory bodies, hence increasing the availability of related information in the electronic environment, openness of the proceedings, enhancing the impartialness of the decisions, better reliability and understanding of the society.</p> <p>In general the main tasks of the e-case project includes the following: digitalization of the files of the criminal proceedings and administrative violations proceedings, ensuring that these files are electronically available both to institutions involved into these proceedings and to private persons in the form of electronic services, improving the data storage and exchange according to the actual requirements and trends in the given field. Essential precondition for implementation of the e-case project is undertaking of all involved institutions – the Ministry of Interior (State Police), Prosecutor General’s Office and the Ministry of Justice (The Court Administration) to implement the reform of the investigation, criminal prosecution and court proceedings by replacing the hardcopy documents circulation with electronic one. The development of e-case project of the Prosecution Office is essential step for improving of the quality and efficiency</p>



	<p>of the persons and state rights protection, increasing the portion of the fulfilment of tasks within the competence of Prosecutor in electronic environment.</p> <p>Implementation of e-case project would essentially reduce the spending of administrative resources, simplify the investigation of the criminal offences, decrease the costs of the investigation in the criminal procedures, as well as would ensure the electronic access to the files of e-case to persons mentioned in the Criminal Procedure Law in all stages of the criminal procedure. At the same time it is foreseen to elaborate the amendments in the legislative acts, for example, in the Criminal Procedure Law, Administrative Violations Code. The possibility to certify the electronically made document and its variants will be provided for, for example, electronic signature or biometry, and confidence to the document, prepared by a person directing the proceedings electronically and attached into the system.</p> <p>It is planned to implement the 1st stage of the project program “E-case: improving of the investigation and court proceedings” in cooperation between the Courts Administration of the Ministry of Justice, the Prosecution Office of the Republic of Latvia, the State Probation Service, the Department of the Imprisonment Institutions and the Information Centre of the Ministry of Interior. Within the frameworks of the 1st stage of the e-case program is planned to implement in the Prosecution Office until year 2020 the project “Development of the Prosecution Office Information System” (further referred as “Project”), its aim is to improve the efficiency of the Prosecution Office work and decrease the time of circulation of the documents related with the judicial proceedings by improving, developing and integrating of the Prosecution Office Information System. By the development project of the Prosecution Office Information System (further referred as “ProIS”) the following aims shall be reached:</p> <ul style="list-style-type: none"> • Improving of the Prosecution Office information exchange between the parties in the criminal procedure, the investigatory and judicial institutions. • Integration of the Prosecution Office work procedures into the pre-trial investigation and court proceedings within the context of e-case. • Rational improving of ProIS by means of e-case and public centralized sharing solutions. <p>It is planned that in the result of the project all criminal cases will be lodged with the courts electronically by means of the sharing components of the e-case and e-services “Electronic familiarization with the files of the criminal case within the pre-trial procedure” and</p>
--	---


	“Submission of the procedural documents” will be available.
 LT	<p>At present Prosecutor General’s Office of the Republic of Lithuania and regional prosecutor’s offices send/receive requests for legal assistance to/from other EU Member States by traditional post, sometimes by email (documents are scanned in .pdf format) and fax. Evidence collected while carrying out requests for legal assistance and stored in a digital format (usually in CDs) are sent by post. The average number of CDs sent to other EU Member States is 25, and the average number of received CDs is 30 per year.</p> <p>Digital format of evidence helps to save printing costs and other costs (e.g. storage of printed case material). In order to transfer electronic evidence more effectively and in a shorter time, it would be useful to migrate the communication among Member States in criminal matters to the cyberspace as well.</p> <p>Considering the abovementioned, Prosecutor General’s Office of the Republic of Lithuania takes an active role and represents Lithuania’s position to support (referring to the conclusions of the Council of the European Union made in June 2016 on improving criminal justice in cyberspace) the initiative of the European Commission regarding creation of a safe electronic platform for communication enabling transfer of European investigation orders and electronic evidence (e-Evidence) among Member States. Prosecutor General’s Office of the Republic of Lithuania makes preparations for introduction of e-Evidence system, and together with institutions of other EU Member States has filed a joined application for grant from the European Union funds to finance the project of implementation of e-Evidence system.</p>
 LU	<p>I. Beginning of the year 2017 the Luxembourg prosecutor’s office started issuing digital copies of their files to the lawyers requesting a copy for their pleadings. Upon their request, they receive a link on their official mailbox , where the files may download during a one-month period. Any such download is logged by the prosecutor’s office and finally added to the file itself to keep trace of the files being issued. In addition to the benefit of this paperless transmission which allows the lawyers to print only a selected range of pages required for their pleadings, the same files may be made available again to any other requesting party within minutes upon their request. Discussions are proceeding on an extension of this system to insurance companies in damage cases.</p> <p>In the near future such files may also be used to be transferred digitally from one prosecutor’s office to another prosecutor’s office within</p>



	<p>the EU.</p> <p>II. Further to the implementation of the Luxembourg law of 17 May 2017 , the code of criminal proceedings has been amended to increase the use of digital information exchange.</p> <p>Any case registered at a Police station is, in addition to be transmitted to the prosecutor's office in paper form, transferred electronically and any standard information required by the prosecutor's office, instantly synchronised with their internal system.</p> <p>Any case directly registered at the prosecutor's office and which is not yet digitally available, is being digitalized internally. As a next step, already provided for in the law , it is envisaged to issue the orders of summary punishment digitally through a secure channel, allowing the receiver as well to interact i.e. file for appeal.</p> <p>III. According to article 66-5 of the Criminal Procedure Code, certain disclosure orders issued by an investigation magistrate can be sent to financial institutions in a digitalized way. A secure channel of communication has been set up between the financial institutions, the office of the investigation magistrates and the police (who handles the material execution of said disclosure orders).</p> <p>IV. In MLA matters, all requests to and from the US are transmitted electronically, without further exchange of paper versions. All other requesting countries can send requests electronically and these requests will be executed on basis of the digital version. However, a paper version is still needed at the latest before the return of any execution material to the requesting country. Legislative work on the EIO is currently in process and will allow an electronic transmission of the orders.</p> <p>As regards the second question above, while the advantages of using digital communication channels are widely recognised by the practitioners, further work will be required, together with the EU institutions, to set up systems that allow both an effective and a secure exchange of information.</p>
 MT	
 PL	<p>Prosecution service leading or supervising criminal proceedings, uses the digital exchange of information for the purposes of these proceedings on an ongoing basis. Such exchanges take place on the basis of statutory regulations or internal bilateral agreements between</p>

	<p>institutions. The information obtained from following databases is also successfully used:</p> <ul style="list-style-type: none"> - PESEL - Social Security database - KRS - National Court Register - NKW - Central Database of Land Registry - KRK - The National Criminal Register - CEPIK - Central Register of Vehicles and Drivers - REGON - Register of National Economy
 PT	<p>As said, it is currently under development the implementation of a new system within the criminal justice, expected to be concluded by 2019. This system will aim to digitalize the criminal justice process. Within it, all the acts and decisions will be in electronic format, using digital signature.</p> <p>It is expected that such a system can accelerate the proceeding, contributing to the general efficiency of the judicial system.</p>
 RO	<p>Digital information exchange in the context of criminal proceedings, a very important tool, is not frequently used between the Romanian authorities, or with foreign partners, although it would be extremely useful for speeding up criminal procedures.</p> <p>The main problem is related to the technical support, a secure technical frame and costs of technical equipment to be used for such transmission/ training of personnel, an important financial impact being envisaged. Still, on long term, the costs are optimum and justified because of the more efficient activity, the speed and safety/integrity of procedures being one major advantage.</p> <p>Also other advantages are to be considered, such as the exact identification of the document's issuing authority/person, integrity of content and safety of communication, reducing time for obtaining evidence and avoiding extinction of proofs.</p>

 SK	<p>Pursuant to Section 69 para 1 of the Code of Criminal Procedure the accused, defence counsel, victim and Party to an action, representative, appointed guardian and in proceedings before the court a public prosecutor, probation and mediation officer, high court clerk, court secretary and assistant prosecutor have the right to inspect files, with the exception of the voting record and personal data on the identity of the protected witness, endangered witness, or a witness whose identity is classified, and classified data on the identity of the agent, to take and make notes of them, and to procure copies of the files and their parts at own expense; such expenses shall not be paid by the public prosecutor, the probation and mediation officer, high court clerk, court secretary and assistant prosecutor. The same right applies to the legal representative of the accused, the victim and the party to an action, if such persons are denied their legal capacity or their legal capacity is restricted. Other persons may do so with the consent of the presiding judge and, in the pre-trial stage, with the consent of the law enforcement authority, only if it is necessary to exercise their rights.</p> <p>Pursuant to Section 69 para 3 first sentence of the Code of Criminal Procedure, those persons who have the right to be present in an action cannot be denied access to the protocol of such action.</p> <p>Referring to Section 69 para 1 of the Code of Criminal Procedure, within the criminal proceedings it is possible for an defined group of persons to access files and to procure copies of the files and their parts at their own expense. In the practice of law enforcement authorities it is usual that they provide the investigation file in a digital form (e.g. by a download to the USB storage device), so it is not necessary to provide copies of the file which is time consuming and it improves the efficiency of the criminal proceedings.</p> <p>Referring to Section 69 para 3 of the Code of Criminal Procedure the authorized person directly participating on the investigation action or in a proceeding before a court or other law enforcement authority receives a protocol of this action in an electronic form upon request. This procedure is convenient, because while the competent court or other law enforcement authority may be thoroughly controlling the content of the protocol, the authorized person does not need to wait for the termination of the control. After having finished this control, the protocol may be sent by electronic means to the electronic address to the authorized person.</p> <p>The exchange of the electronically signed decisions is used in the criminal proceedings from 1 November 2016 in accordance with the valid regulations especially relating to courts. At the Police Office the project „electronic investigation file“ is in the state of implementation which shall enable from 1 July 2018 the communication between a prosecutor and a police officer only electronically with the access to the complete investigation file. Subsequently it is foreseen that the charges, or the proposal to approve the agreement on guilt and punishment,</p>
---	--







	<p>including the investigation file, shall be served to the court electronically, which should accelerate the mutual communication within the criminal proceeding as well as the elaboration of the court's or prosecutor's decisions by the electronic signature.</p> <p>In general it may be affirmed that the use of digital tools within the criminal proceedings has its significant advantages because it may often accelerate and shorten the proceeding and therefore also accelerate the implementation of the criminal justice, providing also the elimination of a situation of legal uncertainty of the parties involved in the criminal proceedings.</p> <p>In communication with the citizens the effectivity of the use of digital tools is limited to their readiness and willingness to communicate by electronic means or to use digital tools within specific actions of the criminal proceedings.</p>
 SI	<p>As far as the prosecution service is in question, we have recently started the process of receiving criminal reports when the perpetrators are unknown from the police. The reports in digital form are sent directly to our information system, but they are still followed by the file in physical form. The process is at an early stage and still needs improvements to reach the pivotal aim – rationalization and paperless business.</p> <p>The Republic of Slovenia also supports the project eCODEX but has not a status of a party in the project. However, the Centre for Informatics at Supreme Court of the Republic of Slovenia follows development of the project and uses the same technology and standards for their system. It is expected that eCODEX will be gradually integrated in European portal e-justice in the future, allowing the possibility to exchange documents and data between competent authorities of Member States. There would be no storage warehouse but only safe and direct transmission of data between two information systems.</p> <p>The issue that we see in connection to the system above is difference in levels of protection that different Member States would choose – the exchange would be possible only in case of the same level of protection. When one Member State would choose to operate only electronically, it would be impossible to receive or to send data to authorities of another Member State. In that case the exchange would be completely blocked.</p>
 ES	<p>Law 18/2011 on the use of information technologies and communications in the Justice Administration regulates all the aspects related to digitalisation of the Justice system (use of electronic means by the Justice Administration, legal regime applicable to the electronic Justice</p>






	<p>Administration-, management of electronic files, cooperation among the different competent Administrations, interoperability and security).</p> <p>Pursuant to Article 230 of the Law on the Judiciary, Courts and Prosecution Services must use all electronic means available to them in the exercise of their activities with due respect to the data protection rules; documents issued by electronic means will be considered as originals if their authenticity, integrity and compliance with the procedural laws are granted. Confidentiality and secrecy of the personal data included in the electronic files must be also granted. The different electronic systems used by the Justice Administration should be compatible.</p> <p>Differing national systems with regard to the implementation of electronic tools will obviously hamper judicial cooperation; interoperable national systems within the European Union would definitely boost efficiency in this field.</p> <p>Developing and implementing the eCodex should be prioritised by member States.</p> <p>The use of digital tools within the Justice Administration should be further developed and expanded for the sake of a faster and more secure transfer and management of evidence and other data, in particular in relation with cybercrime.</p>
 SE	<p>Many authorities within the Swedish criminal justice sector, and foremost the Swedish Prosecution Authority, have a well-developed digital information exchange with the other authorities within the justice sector. The development is ongoing and will most likely be intensified in the coming years.</p> <p>There are great advantages with a digital information exchange, such as increased productivity (no need to register the same data twice; automatic registration of actions and received/sent documents; less time spent sending/searching for paper and paper-files, easier access to data and document), better statistics and follow-up as well as easier archiving.</p> <p>Digital information exchange is not easy and takes time to develop and implement. There are often business/operational challenges, juridical challenges, and technical challenges. Lack of understanding of these facts can be frustrating. The lack of understanding of the importance of information security and cyber security might also be a challenge.</p> <p>The margin for further use of digital tools in criminal proceedings is immense. But, there are many exchanges/integrations/development</p>










	activities yet to do, and to wish for.
 NL	<p>Paper files are gradually digitised. This digital copy is then used during the whole process. The electronic signature guarantees the faithfulness of the document in court.</p> <p>The electronic version of the originally paper or physical document is legally considered as the original document. Thus the physical version can eventually be deleted. This will in the future result in a digitalised archive.</p> <p>Draw backs: working digitally requires a change in the organisation, culture and technology which is a complicated and time consuming process.</p>
 UK	<p>In the UK a vast majority of case material is received digitally through an interface between police systems and the CPS Case Management System. Where material is not received through this interface, most of the remainder is received on disc and is uploaded to enable subsequent digital working. Case material is exchanged with other Criminal Justice System (CJS) agencies digitally through the use of interfaces with systems including the Crown Court Digital Case System (CCDCS) and Court Store, or cloud-based sharing systems including Evidence.com and Egress or by e mail. Case material is also presented digitally in court by prosecutors using tablet devices and a bespoke Prosecutor Application.</p> <p>Advantages of using digital tools:</p> <ul style="list-style-type: none"> • All parties involved in a case have access to the same material in the same format that may be accessed from the same system, e.g. CCDCS. • Achieves greater efficiency in the case management and progression process by enabling instant access to material when it is made available, and by all agencies following a consistent process. • Realisable cashable benefits through savings in paper, storage and other ancillary costs associated with managing hard-copy material.




	<ul style="list-style-type: none"> • Enables automation of administrative functions reducing costs of administrative processes • Enables greater control over who has access to case material. <p>Disadvantages of using digital tools:</p> <ul style="list-style-type: none"> • May be initial significant financial outlay for the purchasing/installation of IT software and hardware. • Requires significant cultural change (which cannot be underestimated) across the CJS to achieve the full anticipated benefits of digitalisation <p>Further scope of using digital tools:</p> <ul style="list-style-type: none"> • Development of solutions to digitalise multimedia evidence (MME) will enable all parties in a case to access this type of evidence at a much earlier stage. This will positively impact on case progression. • Development of the Common Platform will result in all CJS agencies utilising one shared system and following the same end to end process to manage all types of criminal cases, thereby achieving consistency and greater efficiency. • A suitable solution to allow self-represented defendants to access and manage cases digitally would assist in achieving greater digitalisation of the CJS.
--	--





3. Have you encountered, in your relations with other EU Member States, any obstacles to judicial cooperation in criminal matters that are related to the use of electronic signatures and/or digital information exchange?


Member State	Replies and observations
 AT	No. The eIDAS regulation creates an appropriate basis for cross-border information exchange also in criminal proceedings.
 BE	<p>We have few experience with incoming requests with digitalized signatures. In those cases that the request was only signed with an identification number we asked the requesting authority to provide us with an identification, because we don't have the equipment to identify this number. This took some time and an explanation to the requesting country. (we had just one case over a one year period, from Spain in a minor traffic offence)</p> <p>In general all the incoming requests are still signed.</p>
 BG	n/a
 HR	No, judicial cooperation in criminal matters is generally not conducted electronically.
 CY	No obstacles.
 CZ	<p>In judicial cooperation in criminal matters communication by e-mail is widely used both by the police, judiciary and contact points of the network (especially the EJN, ECJN and others). Request for mutual legal assistance in their electronic forms are accepted and their execution is ordered without delays.</p> <p>Electronic signatures are neither used nor required in judicial cooperation in criminal matters which implies the lack of identifiable problems.</p>

 DK	No, not to my knowledge.
 EE	We have experienced that most of the Member States prefer paper documents, ordinary mail, and don't use digital signature. Only in urgent cases, the digital requests are accepted but usually there is need to send original request via ordinary mail and in paper afterwards. Still, the exchange of mutual legal requests between Estonia and Finland is paper free and done via digital way and because of that, it is very fast.
 FI	No. As stated before EIO would benefit from electronic signatures in member states where the issuing authority needs judicial authority's validation.
 FR	<p>Des développements ont été entrepris afin de permettre aux utilisateurs (juges d'instruction, JIRS, parquets) de renseigner directement dans Cassiopée des événements dits « européens » avec les données du dossier pré-renseignées. Une nouvelle entité a été créée : le Bureau National Français, et ce dernier pourra accéder directement aux données avec des identifiants Cassiopée propres. Par ailleurs, depuis le 1er mars 2026, les magistrats disposent sur l'applcatif de l'intégralité du formulaire de saisine d'EUROJUST.</p> <p>Un développement est actuellement programmé aux fins de mise en œuvre, en 2018, d'une alimentation automatisée du système de gestion de procédures (CMS) d'Eurojust, par des données de Cassiopée.</p>
 DE	<p>With regard to the exchange of data on the international level, Germany signed the Con-vention on the stepping up of cross-border cooperation, particularly in combating ter-rorism, cross-border crime and illegal migration (also referred to as 'Prüm Convention') on 27 May 2005. The treaty is open to all members of the European Union, 14 of which are currently parties. Core elements of the convention were picked up by the EU 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. The treaty is aimed at signifi-cantly enhancing information exchange for the purpose of the prevention and prosecution of crimes between the signatory states. As a major innovation, the treaty stipulates that the participating states will grant each another automated access to their DNA and finger-print data and to vehicle registration databases. In case the stored data matches DNA traces or finger prints, states submit the personal data of the sought person through mutual legal assistance.</p> <p>Concerning the digital exchange by judicial authorities except for transmissions to EJM-contact points we still lack a secure way of data transmission. Particularly, we miss com-mon standards of encryption. Consequently, this way of communication is hardly been used. A</p>

	<p>positive example is the cooperation of the authorities of North-Rhine-Westfalia with prosecution offices and courts in Belgium and the Netherlands, including means of direct communication between the police and prosecution offices (e-CODEX pilot EURE-gio).</p> <p>Besides that, another obstacle relates to the submission of large volumes of data. It has been necessary in several cases in the past to hand over the respective hardware instead of submitting the digital information via electronic channels.</p>
 EL	At last we have not encountered in our relationship with other EU Member States any obstacles to judicial cooperation.
 HU	We haven't encountered any problems in this field. The main obstacle in this area is the fact that digital information exchange doesn't work.
 IE	
 IT	In Italy they work very well the system of contact points 24/24 provided by the Convention on Cybercrime in Budapest in 2001 attuned by law n. 48 /2008 which are based on an immediate and unformalised computer communication on data preservation . The problems encountered concern above all the technical standards of digital documents .
 LV	Electronic signature currently is not used in the international cooperation within the criminal justice matters.
 LT	Considering that at present only evidence in a digital format are exchanged, in practice Prosecution Service of Lithuania does not face any major problems in communicating with other Member States regarding criminal matters and in exchanging electronic information.
 LU	We do not have any information about a case where the use of electronic signature and/or digital information exchange has led to significant problems in the cooperation with other Member States.
 MT	
 PL	We are unable to answer that question as we do not conduct such statistics.

 PT	As now, there is no experience at this respect.
 RO	<p>Requests for international judicial assistance may be transmitted/received through the use of electronic signatures and/or digital information exchange, if the authenticity and confidentiality of requests and the credibility of data included in such requests are guaranteed.</p> <p>During practice, electronic mail or the support of Eurojust are frequently used for transmitting/receiving requests or various data/information necessary to executing requests, or the results of executing the requests, however without the use of electronic signatures.</p> <p>One difficulty might consist in the necessity of means to promptly verify the authenticity of the source of request (a contact point network being an advantage in this respect) or of the electronic signature (owning the devices/app-s to verify the certificate and the provider).</p> <p>Also, transmitting responses to international judicial assistance requests might raise problems, related to the size/volume of data to be transmitted. Both authorities involved must own technical equipment to a certain standard –speed of loading/unloading, capacity and place of storage and security of communication channel.</p>
 SK	<p>As we weren't yet confronted with the use of electronic signature within the international judicial cooperation in criminal matters, we do not register any obstacles in this field. The main reason is that currently the standards of the use of electronic signature are not unified within the EU (an upcoming change is foreseen in 2019).</p> <p>The issues of the electronic signature within the international judicial cooperation in criminal matters between Member States of EU is currently a matter examined by the European Commission (particularly the legal aspects) in the context of the preparatory works related to a creation of a platform for the transmission of European investigation orders and electronic evidence (the query was initiated by the Slovak Republic as the current legal framework does not regulate the possibility of use of the electronic signature within the European investigation order system and there is no valid and effective regulation at the level of EU that could've been applied). Cross-border digital transmission of information requires, taking into account a non-public nature of the pretrial stage of criminal proceedings as well as the new legislation in the field of data protection, the security of the exchange of digital information. These issues are also in the centre of</p>

	<p>discussion in the process of creating the platform.</p> <p>We are not aware of any obstacles relating to the transmission of different requests (issued without the electronic signature, e.g. scanned requests, requests sent by electronic mail etc.) by electronic means as long as they are issued in conformity with the existing legal mechanisms.</p>
 SI	<p>We do not have legal provisions that would allow us to share our digital evidence with foreign authorities by means of digital information exchange. The practical reason is lack of secured connections for e-evidence exchange.</p>
 ES	<p>A distinction should be made between digital information in general and the particularities related to judicial cooperation the fight against cybercrime where data stored in information systems is requested. In relation to the former, no particular issues have been identified with regard to the exchange of digital information that we are aware of; as for the latter, some of the main remaining issues that can be listed are: volatility of data, loss of location, different approaches to the concept of jurisdiction in this field, difficulties in identifying the competent jurisdiction or the jurisdiction where to address a MLA request, the need to find alternatives to traditional MLA requests, production order for subscriber information, confidentiality and disclosure or differing approaches to the possibility of trans-border access to stored computer data, among others.</p> <p>The activities and permanent exchange of information (including digital information) in the context of a joint investigation team would definitely be enhanced and facilitated if the Justice systems of the participating member States would be interoperable.</p>
 SE	<p>No, not to our knowledge at this stage. In the former communication between Swedish prosecutors and Eurojust (a long, long time ago), there were some difficulties to understand the standards and security levels (the Swedish Prosecution Authority did not understand Eurojust). As a result, Sweden connected a VPN to the Swedish desk, using encrypted communication between the Swedish desk at Eurojust and the Swedish Prosecution Authority.</p>
 NL	<p>The Netherlands, Belgium and Germany collaborate in the e- CODEX pilot project on “Mutual Legal Assistance in Criminal Matters” . In this pilot Mutual Legal Assistance requests are exchanged in a digital form between The Netherlands and North Rhine Westphalia.</p>

	No use is made of electronic signatures (the form, containing a blue ink signature, is scanned and uploaded back into the system).
 UK	The European Investigation Order (EIO) was implemented into UK law on 31 July 2017 by The Criminal Justice (European Investigation Order) Regulations (the Regs) 2017. The UK's early experience of the EIO has been that one MS so far will not accept a court issued EIO without a wet signature. An EIO was issued by the UK court and a Judge had granted the application and provided an electronic signature. The EIO was transmitted to the relevant MS but was returned by the prosecutor who requested that the UK Judge would need to provide a wet signature or a court stamp in order for the EIO to be recognised. The EIO was stamped by the UK court but again was returned by the MS who a wet signature from the issuing Judge.