ELECTRONIC LEGAL ACTS AND COMMUNICATIONS

8 November 2024

Hosted by Vyskočil, Krošlák a partneři

VK&

Table of Contents

SUMMARY OF THE MEETING

On 8 December 2024, another TELFA Associates Meeting was held in Prague, during which a very important topic of **Electronic Legal Acts and Communications** was discussed.

The aim of the meeting was to share knowledge and experience in the areas of electronic signing, identification and electronic communication. Although this area of law is significantly influenced by directly applicable EU legislation, as the Meeting eventually demonstrated, practice can and does differ in many respects.

The Meeting provided many useful and enriching insights into the legal practice across different jurisdictions as well as the approach to the issues mentioned. As part of the preparation for the Meeting, a questionnaire was sent out to each partner law firm to provide an initial introduction and overview of the specifics of Electronic Legal Acts and Communications applied in that jurisdiction.

As we operate in a globalised world in which knowledge and awareness of cross-border legal regimes is often inevitable, we found it useful to disseminate the answers to the questions in the questionnaire in this comprehensive form. Although this does not represent an exhaustive coverage of the topic, we believe that this summary can potentially assist you when dealing with specific issues involving persons and entities from the countries involved.

Last but not least, we would like to thank all the participating law firms who contributed both to the Meeting itself and provided answers to the initial questionnaire, thus contributing to the creation of this comparative summary.

AUSTRIA

Oberhammer

1. Electronic Legal Acts and Signatures

1. What are the requirements for a written legal act executed by electronic means to be valid? *(e.g. signature, identification of the person acting, capture of its content...)*

A qualified electronic signature is required to fulfil the legal requirement of a "written document". E-mails (unless carrying a qualified electronic signature) or copied signatures do not fulfil this requirement.

2. How does judicial practice view electronic legal acts? In practice, what evidence is required and/or accepted by the courts?

Where the Austrian law does not require a written document to constitute a binding obligation, also E-mails or Text messages are accepted by courts to consitute legal act. E.g. agreements for the sale of good on P2P-online platforms. E-Mails are widely used and accepted as evidence in court rooms.

3. Does the national legislation differ in any respect from the EU Regulation No. 910/2014 (eIDAS)? If so, in which areas?

Not to a degree notable in daily practice.

4. Does your jurisdiction recognise other types of electronic signatures than those regulated by the Regulation eIDAS?

In some instances courts have rules that a faxed signatures also qualify as handwritten signatures (which usually only qualified electronic signatures do).

5. Is it possible for a Notary Public (or another person/entity) to officially verify a signature that has been made by electronic means? If so, in which cases and under what conditions?

Yes, in such case the electronic signature has to be given in front of the notary, which is usually done in an Online-Video-Conference.

6. Which type of electronic signature is required when interacting with courts and public authorities? Is this practice uniform across all public bodies and authorities?

Qualified electronic signatures are required by courts for lawyers. For documents submitted by the parties themselves in some instances scanned signatures are accepted, especially when it comes to family law. However, the justice system also operates a system where one may login with their Austrian ID (governmental electronic ID also providing qualified electronic signatures) and submit documents to the courts. The usage of this system is favoured by courts.

7. In practice, do public authorities effectively recognise the use of signing tools *(e.g. Adobe Sign, DocuSign)* when interacting with them?

Usually only where qualified electronic signatures are used. However, some courts are starting to accept DocuSign documents for less sensitive documents ,e.g. related to the commercial register.

2. Electronic Identification

1. What means can be used to prove an individual´s identity electronically in your jurisdiction? Do electronic ID cards work *(e.g. in the form of mobile app)*?

Yes. The digital government app has the functionality to display an electronic copy of the driver's licence.

2. Are there any means of electronic identification of legal entities in your jurisdiction?

Yes. There is the USP (Unternehmensservicportal = company service portal), which is the central platform for communication between companies and authorities in Austria. A natural person has to log in with its ID Austria and may file applications and similar with the authority if that person is linked to a legal entity.

3. Are there any electronic identification means provided by private entities in your jurisdiction *(e.g. Bank ID)?* Do they provide sufficient proof of identity when interacting with all public authorities or are there any limitations?

A-Trust, the operator of ID Austria is a private entity, that also operates other technical solutions for electronic identification. To our knowledge, there is no other private provider of such solutions.

4. Is there only one/multiple electronic identification means offered directly by the state in your jurisdiction?

There is one: ID Austria.

3. Electronic Communications

1. What means of electronic communication with public authorities are used in your jurisdiction?

E-Mail, data boxes, individual masks for certain areas.

2. Are there any state-guaranteed means of electronic communication that can be used to communicate with the public authorities? If so, can individuals and legal entities also communicate with each other through this/these means?

By state guaranteed means we mean electronic communications means that come from and are operated by the state/state institutions themselves.

FinanzOnline and USP are platforms for communication between entities and (a) the financial authority and (b) various other authorities that also may be used for electronic communication.

3. In your jurisdiction, is the use of data boxes in communication with courts and public authorities common? If so, are there any exceptions when a data box cannot be used?

**** Data box is an electronic documents delivery system that enables individuals and legal entities to send/receive electronic documents to/from public authorities free of charge. It works similarly to an email box, except that the identity of the owner of the data box is officially verified. Individuals and legal entities can also communicate electronically with each other using the data box, but for a fee.***

While a data box is provided by the government, it is based on an opt-in model and in our perception, it is not used intensively.

4. Are there any specific formalities that must be met when communicating with public authorities *(e.g. document format, signatures, attachments etc.)*?

This depends strongly on the public authority involved. Most authorities accept E-Mails and most common attachment types. For the communication between lawyers and courts stricter rules apply.

5. Are there any legal fictions/presumptions associated with electronic service of documents in your jurisdiction *(e.g. service by fiction)*?

Yes, for most use cases it is the first business day after either the electronic notification or the first business day after the document was made available.

6. In your jurisdiction, is it possible to communicate electronically with all public authorities? If not, which ones cannot?

Yes, at least E-Mail/fax are accepted as means of electronic communication by all authorities. This is, however, not a legal requirement, thus for some specific authorities this possibility might not exist.

7. Is there an obligation to communicate with some public authorities/on certain matters only electronically?

Yes, e.g. for lawyers when communicating with the courts. Same might be true for the representation in tax or other matters.

BELGIUM

DELSOL Avocats Belgium

1. Electronic Legal Acts and Signatures

1. What are the requirements for a written legal act executed by electronic means to be valid? *(e.g. signature, identification of the person acting, capture of its content...)*

It depends on the kind of act and the usage thereof, there are 3 categories of digital signatures (regular, advanced, qualified), the more important the act, the higher level required, etc..

2. How does judicial practice view electronic legal acts? In practice, what evidence is required and/or accepted by the courts?

In court, (generally speaking) judges don't make a big fuzz, however the clerks do when it comes to registering or publishing (printed versions are not allowed etc).

3. Does the national legislation differ in any respect from the EU Regulation No. 910/2014 (eIDAS)? If so, in which areas?

No.

4. Does your jurisdiction recognise other types of electronic signatures than those regulated by the Regulation eIDAS?

Not to our knowledge.

5. Is it possible for a Notary Public (or another person/entity) to officially verify a signature that has been made by electronic means? If so, in which cases and under what conditions?

We have a very slow digitalisation process. For years signing from distance was done by giving a digital proxy to an employee of the notary, it's not until this year that some (excluding e.g. testaments/wills, etc) acts can be signed directly via the Identity Card.

6. Which type of electronic signature is required when interacting with courts and public authorities? Is this practice uniform across all public bodies and authorities?

We have eID and itsMe, linked with our personal identity card (or lawyer card) which is used to login and sign on the platforms of the courts/public authorities.

7. In practice, do public authorities effectively recognise the use of signing tools *(e.g. Adobe Sign, DocuSign)* when interacting with them?

Mixed, we do not have that much digitalisation, but overall yes.

2. Electronic Identification

1. What means can be used to prove an individual´s identity electronically in your jurisdiction? Do electronic ID cards work *(e.g. in the form of mobile app)*?

In Belgium, several banks founded itsMe, which is a monopolist on logging in with your ID card from the app. Otherwise you can also plug-in the ID card in a reader and use the local log-in method.

2. Are there any means of electronic identification of legal entities in your jurisdiction?

A platform to check companies: KBO/BCE (state-run), company web, others (private).

3. Are there any electronic identification means provided by private entities in your jurisdiction *(e.g. Bank ID)?* Do they provide sufficient proof of identity when interacting with all public authorities or are there any limitations?

See earlier, itsMe was founded by banks and is now the method in Belgium to interact with almost all public authorities. There is apparently competition from SmartID

4. Is there only one/multiple electronic identification means offered directly by the state in your jurisdiction?

Yes, the state just accepts the identity card (+ pin code) via a reader, the applications (itsme, smartid etc are all private).

3. Electronic Communications

1. What means of electronic communication with public authorities are used in your jurisdiction?

E-mail, website, deposit-platform.

2. Are there any state-guaranteed means of electronic communication that can be used to communicate with the public authorities? If so, can individuals and legal entities also communicate with each other through this/these means?

By state guaranteed means we mean electronic communications means that come from and are operated by the state/state institutions themselves.

Communication that is „guaranteed“ is via the website. No.

3. In your jurisdiction, is the use of data boxes in communication with courts and public authorities common? If so, are there any exceptions when a data box cannot be used?

**** Data box is an electronic documents delivery system that enables individuals and legal entities to send/receive electronic documents to/from public authorities free of charge. It works similarly to an email box, except that the identity of the owner of the data box is officially verified. Individuals and legal entities can also communicate electronically with each other using the data box, but for a fee.***

It is common for the courts: there is DPA (private platform started by the bars in Belgium, paid deposits) and e-deposit (started by the courts, free of charge), no real limitations to our knowledge besides 20mb per file size.

Public authorities have a data box but it is more rarely used (if the size of the files is too big for mailing).

4. Are there any specific formalities that must be met when communicating with public authorities *(e.g. document format, signatures, attachments etc.)*?

Not to our knowledge.

5. Are there any legal fictions/presumptions associated with electronic service of documents in your jurisdiction *(e.g. service by fiction)*?

Not with electronic service of documents.

6. In your jurisdiction, is it possible to communicate electronically with <u>all</u> public authorities? If not, which ones cannot?

Yes, to our knowledge.

7. Is there an obligation to communicate with some public authorities/on certain matters only electronically?

Tax administrations limited since COVID to communicate only electronically and only make an appointment if necessary.

CZECH REPUBLIC

Vyskočil, Krošlák a partneři s.r.o., advokátní kancelář

1. Electronic Legal Acts and Signatures

1. What are the requirements for a written legal act executed by electronic means to be valid? *(e.g. signature, identification of the person acting, capture of its content...)*

According to Sec. 562 of the Civil Code (Act. No. 89/2012 Coll.), in order to preserve the validity of a written legal act made by electronic means, such legal act must satisfy two conditions:

1) <u>The content of the legal act is captured</u>
   The legal act must allow for reproduction of its content and reacquaintance with the information, i.e. t<u>he ability to preserve the informational value of certain data.</u>

2) Identification of the person(s) acting
   It does not require proof of identity, but only its identifiability – thus, identification must be possible, NOT necessarily always successful. It is not bound to any qualified form of authentication – a simple password login, SMS key, fingerprint etc. is sufficient.

If these conditions are met, a legal act executed by electronic means has the same effect as a "paper" legal act. Special laws may provide otherwise, e.g. client identification under the AML Act.

In theory, the legal act executed by electronic means does not have to be signed – provided, of course, that both above-mentioned conditions are met. However, in practice, without any signature, it can be challenging to prove the intent to be bound by the legal act before the courts, as well as to prove the identification of the person acting. Unfortunately, the Czech courts still often require a signature, even though it is not strictly required under the current legislation.

2. How does judicial practice view electronic legal acts? In practice, what evidence is required and/or accepted by the courts?

The Czech courts generally accept legal acts executed by electronic means, as well as electronic signatures. Where the courts are failing short, however, is in their assessment of the requirements for electronic signatures, where there is inconsistent interpretation of the eIDAS Regulation, as well as domestic implementing laws, across the court system.

Czech courts, especially the lower courts, require a higher class of electronic signatures (usually advanced, sometimes also qualified) as a validity requirement for ordinary private legal acts (e.g. purchase contracts), even though according to the current legislation a simple electronic signature should be sufficient (unless the parties agree otherwise). The rationale for this is that courts lack identification of the person acting when using simple electronic signatures.

As far as evidence is concerned, Czech law is based on the rule that all means of establishing the state of the case may be used as evidence. It is therefore up to the court to decide what credibility it will give to specific means of evidence. Czech courts generally accept electronic evidence, however, simple electronic evidence (e.g. emails, electronic copies of documents) can be challenged quite easily. Thus, in practice, the use of electronic time stamps, seals or, if possible, the attachment of source code is recommended in a given case.

3. Does the national legislation differ in any respect from the EU Regulation No. 910/2014 (eIDAS)? If so, in which areas?

Czech law is largely in line with the eIDAS Regulation. Even new laws have been adopted to implement it – mainly the Act No 297/2016 Coll., on trust services for electronic transactions; and the Act No. 25/2017 Coll., on electronic identification. These acts supplement some of the issues not addressed by the Eidas Regulation (e.g. when, against whom, to use which electronic signature…).

The Czech regulation of electronic legal acts and electronic signatures contains one major deviation, namely when it introduces a fourth type of electronic signature (see question below.)

4. Does your jurisdiction recognise other types of electronic signatures than those regulated by the Regulation eIDAS?

The Czech legislator has introduced another type of electronic signature called advanced electronic signature based on a qualified certificate.

It stands somewhere between an advanced and qualified electronic signature (according to the eIDAS Regulation) in terms of the security and identification of the person acting. The difference between this signature and QES is that this signature does not require any hardware (no qualified electronic signature creation device) - practically, the certificate is stored in the computer. The purpose was to introduce an electronic signature based on a qualified certificate, but due to the lack of the need to own a token, its acquisition costs would be lower and it would be easier to use.

For this signature and the QES, the legislator also introduced the legislative abbreviation „recognized electronic signature" - it does not represent a separate type of electronic signature, but a differentiation of signatures that must be used if one is to act towards courts and public authorities.

The use of a data box for signing is also a specific feature of the Czech legal system. If a person who is the owner of the data box sends a document from that data box, it is considered to be made in writing and signed by that person (even though the document is not signed). This legal fiction of signature when sending a document via a data box is probably the most common way of „signing" at present.

5. Is it possible for a Notary Public (or another person/entity) to officially verify a signature that has been made by electronic means? If so, in which cases and under what conditions?

Official verification (legalization) of electronic signatures is possible in the Czech legal system from 1 July 2022.

In theory, legalization of an electronic signature is possible in 3 different ways:

1) verification by an authorised person (by their QES)

- Notary Public, attorney or an employee of the public administration contact point (CzechPoint).

The Notary Public must always verify the identity of the person signing (in person or via video conference with simultaneous use of one of the means for electronic identification). Verification by an attorney is not yet possible in practice due to the lack of technical support.

This method of verification is not used much in practice so far, mainly because notaries have not yet got used to it and do not like to verify electronic signatures.

2) verification by the public administration information system

This is a method where an electronic equivalent of an officially verified signature is created. This is subject to prior trustworthy verification of the identity of the signatory (only on the basis of a qualified electronic identification system with a high level of assurance – now *only eID card, Moje ID service, Starcos chip card*). Legalization is then automated.

Unfortunately, this method is not yet very useful in practice. The primary reason for this is the lack of the necessary functionality on the part of public administration information systems. Another obstacle to more widespread use is the overall insufficient number of electronic identification devices with a high level of assurance.

3) verification using a recognised electronic signature (see above)

This method is based on the fact that if the person acting signs a document using a recognised electronic signature, it is considered to be an officially verified signature. The condition is that the signatory has entered the details of the qualified certificate (serial number etc.) in the Register of Residents.

This method is the simples in practice and works reliably. However, you must have an electronic signature based on a qualified certificate.

6. Which type of electronic signature is required when interacting with courts and public authorities? Is this practice uniform across all public bodies and authorities?

1) Public signatory = QES

2) Legal act towards the public authorities = recognized electronic signature (QES or advanced electronic signature based on a qualified certificate) or data box

3) Other, namely private sector = any electronic signature (e.g. simple electronic signature)

The practice ad 1) and 2) is uniform, however, the courts in particular take a different approach to the use of only a simple electronic signature in the private sector in private legal acts. Some of them require a higher level of signature in order for the legal act to be considered valid.

7. In practice, do public authorities effectively recognise the use of signing tools *(e.g. Adobe Sign, DocuSign)* when interacting with them?

As mentioned above, the public authorities are rather sceptical about the use of these tools when they are used for simple electronic signing of e.g. contracts. This is thus essentially a matter of randomness as to how any given judge will approach the validity of a legal act signed through one of these services.

However, in practice, some registry courts (maintaining the Business Registers) accept documents signed by these services (namely DocuSign) as duly signed.

2. Electronic Identification

1. What means can be used to prove an individual´s identity electronically in your jurisdiction? Do electronic ID cards work *(e.g. in the form of mobile app)*?

There are currently many ways and means of electronic identification:

1) ID card with an activated electronic contact chip – *assurance level high*

2) NIA ID – based on a combination of name, password and SMS code – assurance *level substantial*

3) Mobile eGovernment Key – login without the need to enter additional authentication codes (mobile app) - *assurance level substantial*

4) Chip card Starcos – assurance *level high*

5) Bank ID – currently the most used and accessible mean – assurance *level substantial*

6) MojeID – use of a login, password and token - assurance *level high*

2. Are there any means of electronic identification of legal entities in your jurisdiction?

There are currently no means of electronic identification for legal entities. In practice, only the person authorized or entitled to act for and on behalf of the legal entity (e.g. the directors) can identify.

3. Are there any electronic identification means provided by private entities in your jurisdiction *(e.g. Bank ID)?* Do they provide sufficient proof of identity when interacting with all public authorities or are there any limitations?

Yes, there are the following means:

1) Bank ID

2) Chip card Starcos

3) Moje ID

Of these means, only the Bank ID is the one that provide the assurance level substantial (the other provide assurance level high). Even then, however, the Bank ID is sufficient to access all government services.

4. Is there only one/multiple electronic identification means offered directly by the state in your jurisdiction?

There are three electronic identification means offered directly by the state:

1) ID card with an activated electronic contact chip – *assurance level high*

2) NIA ID – based on a combination of name, password and SMS code – assurance *level substantial*

3) Mobile eGovernment Key – login without the need to enter additional authentication codes (mobile app) - *assurance level substantial*

3. Electronic Communications

1. What means of electronic communication with public authorities are used in your jurisdiction?

The most used and primary channel are data boxes, through which both public authorities communicate to citizens and vice versa. All public authorities are obliged to set up a data box, so in this sense it is the simplest channel.

Of course, it is also possible to communicate via e-mail. Certain specialised government work is then done through special platforms, where it is possible to both fill in the submission and then send it directly via the platform - e.g. *portál Moje Daně* (tax platform) or *Portál občana*.

2. Are there any state-guaranteed means of electronic communication that can be used to communicate with the public authorities? If so, can individuals and legal entities also communicate with each other through this/these means?

By state guaranteed means we mean electronic communications means that come from and are operated by the state/state institutions themselves.

Yes, data boxes are established and managed by the Ministry of the Interior of the Czech Republic in cooperation with the Czech Post (state enterprise), which is the operator of the data box information system.

Furthermore, the state (through its individual organisational units) operate several online platforms through which specific state administration agendas can be communicated (e.g. tax platform *portál Moje Daně*, or *Portál občana* which is a centralized platform allowing access to public administration services, such as requests for extracts from criminal record etc.).

3. In your jurisdiction, is the use of data boxes in communication with courts and public authorities common? If so, are there any exceptions when a data box cannot be used?

**** Data box is an electronic documents delivery system that enables individuals and legal entities to send/receive electronic documents to/from public authorities free of charge. It works similarly to an email box, except that the identity of the owner of the data box is officially verified. Individuals and legal entities can also communicate electronically with each other using the data box, but for a fee.***

Data boxes are the most widely used tool for electronic communication and identification in the Czech Republic and play an absolutely crucial role in the Czech digitalisation.

All public authorities are obliged to set up a data box and receive documents in it. Legal entities, lawyers, self-employed persons, tax advisors, auditors (and others) are also obliged to have a data box. The data box addresses are publicly listed. Other persons may set one up voluntarily.

However, the state and its authorities are obliged to communicate and send documents via data box to the persons who have set up a data box. Legal entities and natural persons can still use different means of communications, i.e. using data box for sending documents is not mandatory for them.

Those having a data box may communicate with public authorities via data box free of charge. Communication via data box between private persons is also possible, however, it is a paid service.

4. Are there any specific formalities that must be met when communicating with public authorities *(e.g. document format, signatures, attachments etc.)*?

If using a data box, there are some requirements on the documents format and their size.

The total size of all attached documents must not exceed 100 MB per message. The data box information system support various document formats, e.g. *doc, jpeg, pdf, pptx, html, xml, zip*. It can be said that there is not really a format that the system would not support. The system checks the document format and the corresponding content before sending.

Documents sent via a data box do not have to be signed if they are „written“ by the person sending them from his/her data box – the legal fiction of signature applies.

However, when communicating with the public authorities via email, such documents must bear a recognized electronic signature.

5. Are there any legal fictions/presumptions associated with electronic service of documents in your jurisdiction *(e.g. service by fiction)*?

When using a data box, there is a fiction of service of the document.

Every document that is received is considered served after 10 days, even when the addressee did not log in and read the message. This is a statutory fiction of service.

Normally, the message sent via the data box is received at the moment when the user with permission to log in that data box logs in (i.e. even before opening and reading the message in question). If this does not happen, the message is considered delivered on the 10th day after the message is delivered to the data box (fiction of service).

6. In your jurisdiction, is it possible to communicate electronically with all public authorities? If not, which ones cannot?

It is in principle possible to communicate with all public authorities and bodies electronically. It is precisely because of the mandatory existence of data boxes that all public authorities are obliged to accept documents and submissions electronically.

7. Is there an obligation to communicate with some public authorities/on certain matters only electronically?

There are cases and situations where electronic communication is mandatory:

1) Tax returns – entities and persons with mandatory data box must file their tax returns (and possibly other tax related submissions) electronically.

2) UBO – proposal for entry or change of entry in the Register of Ultimate Beneficial Owners has to be done electronically for business corporations

3) Insolvency – entities and persons with mandatory data box have to file motions and proposal in the insolvency proceedings electronically.

DENMARK

Lund Elmer Sandager

1. Electronic Legal Acts and Signatures

1. What are the requirements for a written legal act executed by electronic means to be valid? *(e.g. signature, identification of the person acting, capture of its content...)*

Overall, there are no formal requirements for validity. It is merely a question of whether it can be proven that the signature was actually executed.

2. How does judicial practice view electronic legal acts? In practice, what evidence is required and/or accepted by the courts?

There is free assessment of evidence, so it is up to the court to determine the weight that should be given to a particular piece of evidence.

3. Does the national legislation differ in any respect from the EU Regulation No. 910/2014 (eIDAS)? If so, in which areas?

Danish legislation aligns with the EU Regulation No. 910/2014 (eIDAS) but has some national adaptations in certain areas to fit its legal system.

The main points of difference include:

1) Use of NemID and MitID: Denmark has implemented NemID (and more recently, MitID) as its national electronic identification scheme, which functions within the eIDAS framework. However, these systems have specific national characteristics and requirements adapted to Danish public and private sector needs.

2) Level of Assurance: Danish legislation has defined specific assurance levels for electronic signatures and electronic identification that align with, but also interpret, the eIDAS requirements to suit Danish standards for high-security applications. This is particularly relevant for governmental services and secure communication within Denmark.

3) Public Sector Exceptions: While eIDAS promotes mutual recognition of electronic IDs across EU member states, Denmark has certain exceptions in public sector applications, where only Danish eIDs are accepted. This is a limited deviation and usually does not affect cross-border transactions but applies to some internal administrative processes.

4) Consumer Protects Danish consumer rights and Contract Law: Danish law has incorporated additional protections for consumers in electronic transactions that supplement eIDAS regulations, ensuring that electronic signatures and identities are used in a manner that rts. These areas demonstrate Denmark's efforts to balance EU-wide eIDAS regulations with specific national needs and practices.

4. Does your jurisdiction recognise other types of electronic signatures than those regulated by the Regulation eIDAS?

Danish legislation does not recognize other types of electronic signatures beyond those defined by eIDAS.

5. Is it possible for a Notary Public (or another person/entity) to officially verify a signature that has been made by electronic means? If so, in which cases and under what conditions?

In Denmark, a Notary Public can officially verify a signature made by electronic means under specific conditions. This process, known as notarization, involves the Notary Public confirming the identity of the signatory and the authenticity of the signature. For electronic signatures, the Notary Public may require the signatory to appear in person and provide valid identification to verify their identity.

Additionally, the Notary Public may need to confirm that the electronic signature meets certain technical standards to ensure its validity. It's important to note that not all electronic signatures may be eligible for notarization, and the specific requirements may vary depending on the type of document and the intended use.

6. Which type of electronic signature is required when interacting with courts and public authorities? Is this practice uniform across all public bodies and authorities?

Generally, the Danish national electronic identification systems, NemID and its successor MitID, are widely used for authentication and signing purposes. These systems comply with the eIDAS regulation and are recognized as providing a high level of assurance.

7. In practice, do public authorities effectively recognise the use of signing tools *(e.g. Adobe Sign, DocuSign)* when interacting with them?

Overall, yes. See the answer to question 1 and question 9.

2. Electronic Identification

1. What means can be used to prove an individual´s identity electronically in your jurisdiction? Do electronic ID cards work *(e.g. in the form of mobile app)*?

The Danish national electronic identification systems, NemID and its successor MitID, are widely used for authentication and signing purposes.

2. Are there any means of electronic identification of legal entities in your jurisdiction?

Yes, Denmark provides electronic identification mechanisms for legal entities through systems like NemID and its successor, MitID. These platforms facilitate secure digital interactions between businesses and public authorities. Legal entities can obtain a NemID or MitID employee signature, enabling representatives to authenticate and sign documents on behalf of the organization. This ensures that electronic transactions are conducted securely and that the identities of the entities involved are verified.

3. Are there any electronic identification means provided by private entities in your jurisdiction *(e.g. Bank ID)?* Do they provide sufficient proof of identity when interacting with all public authorities or are there any limitations?

In Denmark, MitID serves as the national electronic identification (eID) system, developed through a public-private partnership between the Danish government and the banking sector. This collaboration ensures that MitID is widely accepted across both public and private sectors.

While MitID is the primary eID, some private entities, such as banks, may offer their own identification solutions. However, these are typically designed for specific services and may not be universally accepted by all public authorities.

4. Is there only one/multiple electronic identification means offered directly by the state in your jurisdiction?

Yes, MitID is the only one.

3. Electronic Communications

1. What means of electronic communication with public authorities are used in your jurisdiction?

Depends on the situation. It could be by e-mail, or by the solution called Digital Post that the public authorities use as the standard solution for sending letters etc.

2. Are there any state-guaranteed means of electronic communication that can be used to communicate with the public authorities? If so, can individuals and legal entities also communicate with each other through this/these means?

By state guaranteed means we mean electronic communications means that come from and are operated by the state/state institutions themselves.

Yes, Digital Post. No, individuals and legal entities cannot communicate with each other through this.

3. In your jurisdiction, is the use of data boxes in communication with courts and public authorities common? If so, are there any exceptions when a data box cannot be used?

**** Data box is an electronic documents delivery system that enables individuals and legal entities to send/receive electronic documents to/from public authorities free of charge. It works similarly to an email box, except that the identity of the owner of the data box is officially verified. Individuals and legal entities can also communicate electronically with each other using the data box, but for a fee.***

Yes, we use Digital Post in general. When communicating with the courts about an ongoing case, this takes place on the platform minretssag.dk, where all messages about the case is exchanged.

4. Are there any specific formalities that must be met when communicating with public authorities *(e.g. document format, signatures, attachments etc.)*?

No, not in general, but some communication requires the use of Digital Post.

5. Are there any legal fictions/presumptions associated with electronic service of documents in your jurisdiction *(e.g. service by fiction)*?

In Denmark, electronic communication with public authorities is standard practice, and the use of digital post-boxes, such as Digital Post, is mandatory for both individuals and businesses.

When a document is sent to a recipient's Digital Post, it is legally presumed to have been received once it becomes accessible in the recipient's digital mailbox. This presumption means that the sender does not need to prove actual receipt; the mere availability of the document in the digital mailbox suffices.

However, this presumption can be challenged if the recipient can demonstrate that they were unable to access their Digital Post due to circumstances beyond their control. It's important to note that while this presumption applies to communications with public authorities, different rules may govern electronic service of documents in private legal matters.

6. In your jurisdiction, is it possible to communicate electronically with <u>all</u> public authorities? If not, which ones cannot?

Yes, it is.

7. Is there an obligation to communicate with some public authorities/on certain matters only electronically?

This depends on the situation, but in some cases it is required.

ESTONIA

WIDEN Estonia

1. Electronic Legal Acts and Signatures

1. What are the requirements for a written legal act executed by electronic means to be valid? *(e.g. signature, identification of the person acting, capture of its content...)*

The requirements for a written legal act executed by electronic means to be valid Estonia are as follows:

- The act must be made in a manner allowing permanent reproduction;

- It must contain the names of the persons making the act;

- It must be electronically signed by the persons making the act.

The signature must be given in a way that allows linking the signature to:

- The content of the act;

- The person making the act;

- The time when the act was made.

A digital signature is also considered a qualified electronic signature under EU Regulation 910/2014 according to Estonian law.

2. How does judicial practice view electronic legal acts? In practice, what evidence is required and/or accepted by the courts?

Estonian courts accept electronic signatures, particularly those that meet the criteria set by the eIDAS Regulation. Qualified Electronic Signatures (QES) are considered equivalent to handwritten signatures and are widely accepted in legal proceedings. As a digital signature is legally equated to a qualified electronic signature in Estonia, the identity of the signatory is verifiable and thus accepted by the courts.

3. Does the national legislation differ in any respect from the EU Regulation No. 910/2014 (eIDAS)? If so, in which areas?

Estonia's national legislation primarily complements the eIDAS Regulation rather than differing from it. The key areas where the Estonian law provides additional specifications are as follows:

Insurance Requirements:

- Qualified trust service providers must maintain liability insurance or comparable guarantee with minimum coverage of:

- €1 million per incident

- €1 million total for all incidents annually

Documentation Requirements:

- Trust service providers must document their operations and maintain activity logs for 10 years

- They must have an up-to-date termination plan with specific requirements for notification, data preservation, and hardware destruction

Identity Verification:

- Specific requirements for identity verification before issuing qualified certificates

- Documents that can be used for verification are specified

- Identity verification evidence must be retained for 10 years after certificate expiration

Licensing Period:

- Licenses for qualified trust service providers are valid for 2 years

Non-qualified Trust Services:

- Estonia allows non-qualified trust service providers to be included in the trust list

- These providers must meet specific requirements and undergo conformity assessment every 2 years

eID System Assessment:

- Detailed procedure for assessing the equivalence of electronic identification systems

- Assessment decisions are valid for up to 3 years

4. Does your jurisdiction recognise other types of electronic signatures than those regulated by the Regulation eIDAS?

Yes, Estonian jurisdiction recognizes other types of electronic signatures besides those regulated by the eIDAS Regulation, but signatures other than QES standard are not equal to handwritten signatures. This can be concluded from the Act on the General Part of the Civil Code. As long as the electronic signatures besides those regulated by the eIDAS Regulation are compliant with the following requirements, they are recognized in Estonian jurisdiction.

- The act must be made in a manner allowing permanent reproduction;

- It must contain the names of the persons making the act;

- It must be electronically signed by the persons making the act.

The signature must be given in a way that allows linking the signature to:

- The content of the act;

- The person making the act;

- The time when the act was made.

5. Is it possible for a Notary Public (or another person/entity) to officially verify a signature that has been made by electronic means? If so, in which cases and under what conditions?

Yes. The digital signature (QES signature) can be verified with the Notary Public. However, for digital signatures that were not made in the presence of the notary, the notary can only verify the validity of the digital signature. The Notary Public in Estonia primarily verifies the validity of existing digital signatures rather than authenticating the act of signing itself electronically, unless the signing takes place in their presence.

6. Which type of electronic signature is required when interacting with courts and public authorities? Is this practice uniform across all public bodies and authorities?

In practice, everybody uses the Estonian digital signature with meets the QES standard. This practice is uniform.

7. In practice, do public authorities effectively recognise the use of signing tools *(e.g. Adobe Sign, DocuSign)* when interacting with them?

No, as signing tools such as Adobe Sign and DocuSign do not meet the qualified electronic signature requirements under EU Regulation 910/2014 and therefore are not in practice accepted by the public authorities.

2. Electronic Identification

1. What means can be used to prove an individual´s identity electronically in your jurisdiction? Do electronic ID cards work *(e.g. in the form of mobile app)*?

ID Card, Mobile-ID, Smart-ID (the last two are in mobile).

2. Are there any means of electronic identification of legal entities in your jurisdiction?

Yes, of course. There are qualified electronic seals for legal entities, which are regulated by Article 38 of the EU Regulation 910/2014 (eIDAS). Documents submitted to the E-Business Register can be electronically certified, and in such cases, a qualified electronic signature or a qualified electronic seal can replace the name, signature, and stamp of the certifying person or institution.

3. Are there any electronic identification means provided by private entities in your jurisdiction *(e.g. Bank ID)?* Do they provide sufficient proof of identity when interacting with all public authorities or are there any limitations?

Yes, for example, Smart-ID is provided by a private entity. This is sufficient proof of entity when interacting with public authorities.

4. Is there only one/multiple electronic identification means offered directly by the state in your jurisdiction?

Two – ID card and mobile-ID.

3. Electronic Communications

1. What means of electronic communication with public authorities are used in your jurisdiction?

All public authorities have webpages and functioning electronic communications systems.

X-Road: This is the backbone of e-Estonia, enabling secure data exchange between different information systems. It allows public and private sector databases to link up and operate in harmony, providing a seamless flow of information.

e-Tax Board: This platform allows individuals and businesses to file their taxes online, access tax records, and communicate with the tax authorities electronically.

e-Business Register: This service enables the electronic registration of businesses, submission of annual reports, and other business-related activities.

e-Residency: Estonia offers e-Residency, a digital identity that allows non-residents to access Estonian e-services, including company formation, banking, and tax filing.

i-Voting: Estonia is one of the few countries in the world that allows its citizens to vote online in national elections. This system ensures secure and transparent voting processes.

e-Health: The e-Health system allows citizens to access their medical records, book appointments, and communicate with healthcare providers electronically.

e-School: This platform facilitates communication between schools, students, and parents. It provides access to grades, attendance records, and other educational information.

e-Police: This service allows citizens to report crimes, request information, and communicate with the police electronically.

2. Are there any state-guaranteed means of electronic communication that can be used to communicate with the public authorities? If so, can individuals and legal entities also communicate with each other through this/these means?

By state guaranteed means we mean electronic communications means that come from and are operated by the state/state institutions themselves.

Yes, all of the aforementioned electronic communication systems are state guaranteed. These state-guaranteed means of electronic communication are not only used for interactions with public authorities but also enable individuals and legal entities to communicate with each other. For example, the X-Road infrastructure supports secure data exchange between private sector

entities, and e-Residency allows non-residents to engage in business activities with Estonian companies.

3. In your jurisdiction, is the use of data boxes in communication with courts and public authorities common? If so, are there any exceptions when a data box cannot be used?

**** Data box is an electronic documents delivery system that enables individuals and legal entities to send/receive electronic documents to/from public authorities free of charge. It works similarly to an email box, except that the identity of the owner of the data box is officially verified. Individuals and legal entities can also communicate electronically with each other using the data box, but for a fee.***

Yes. But they are not typically used tor people communicating with each other.

4. Are there any specific formalities that must be met when communicating with public authorities *(e.g. document format, signatures, attachments etc.)*?

QES digital signature.

5. Are there any legal fictions/presumptions associated with electronic service of documents in your jurisdiction *(e.g. service by fiction)*?

**** Data box is an electronic documents delivery system that enables individuals and legal entities to send/receive electronic documents to/from public authorities free of charge. It works similarly to an email box, except that the identity of the owner of the data box is officially verified. Individuals and legal entities can also communicate electronically with each other using the data box, but for a fee.***

The concept of "data boxes" as used in some other jurisdictions is not specifically mentioned in the Estonian context. Instead, Estonia relies on several key digital tools and platforms for communication:

X-Road: This is the backbone of Estonia's e-governance system, enabling secure data exchange between different information systems. It allows public and private sector databases to link up and operate in harmony, providing a seamless flow of information.

e-File: This system connects courts to other information systems and stores data that all the systems use. It is part of the digital court files system and facilitates the electronic filing and management of cases.

Court Information System (CIS): This is a comprehensive system used by the courts to manage case information and facilitate communication with parties involved in legal proceedings.

Public e-File: This platform allows the public to access information about court cases and communicate with the courts electronically.

4. Are there any specific formalities that must be met when communicating with public authorities *(e.g. document format, signatures, attachments etc.)*?

QES digital signature. Identification, which can be done using electronic identification methods such as Smart-ID, Mobile-ID, or the ID-card.

5. Are there any legal fictions/presumptions associated with electronic service of documents in your jurisdiction *(e.g. service by fiction)*?

For Administrative Proceedings:

- A document is deemed served when the relevant information system has registered the opening or receipt of the document;

- When the addressee has electronically confirmed receipt;

- When the document or notice has been sent to a company's registered email address;

- When sent to the registered or published email address of public legal persons, attorneys, auditors, notaries, bailiffs, trustees in bankruptcy, patent attorneys, or sworn translators. For Civil Court Proceedings:

Documents sent through the designated information system are deemed served when:

- The recipient opens it in the system;

- Confirms receipt without opening;

- Another person whom the recipient has allowed to view documents in the system opens it;

- For business entities, documents sent to the registered email address are deemed served after five working days from sending, without requiring confirmation of receipt;

- When documents have been previously served in the same court proceedings, subsequent documents sent to the same address or communication device are deemed served after three working days;

- For documents sent to foreign countries by postal service, they are deemed served after 30 days from sending.

The law also includes an enforcement mechanism: if a person fails to accept documents within the prescribed period, their access to certain information systems (e-land register, e-file system, e-commercial register) may be temporarily restricted until the document is served.

6. In your jurisdiction, is it possible to communicate electronically with <u>all</u> public authorities? If not, which ones cannot?

Yes.

7. Is there an obligation to communicate with some public authorities/on certain matters only electronically?

In practice, yes.

FINLAND

Lexia Attorneys Ltd

1. Electronic Legal Acts and Signatures

1. What are the requirements for a written legal act executed by electronic means to be valid? *(e.g. signature, identification of the person acting, capture of its content...)*

In private legal acts, the principle of form freedom applies, meaning that there are no written form requirements for the legal act. Thus, for example, even an email can be considered a valid legal act as long as the identities of the parties can be verified. However, certain legal acts, such as real estate transactions and wills, have specific form requirements set by law.

Electronic legal acts between private individuals and authorities are more strictly regulated. The person executing the legal act must be properly identified. This can be done through the use of electronic identification systems that comply with European regulations. The act can be signed electronically with an advanced electronic signature or otherwise in a manner that ensures the authenticity and integrity of the document. The electronic document must remain unaltered and archived in a manner that allows later verification of its originality and integrity.

2. How does judicial practice view electronic legal acts? In practice, what evidence is required and/or accepted by the courts?

In Finland, judicial practice generally views electronic legal acts as valid and enforceable, provided they comply with the legal requirements. Courts assess electronic evidence based on its ability to reliably demonstrate authenticity, integrity, and the identity of the signatory.

3. Does the national legislation differ in any respect from the EU Regulation No. 910/2014 (eIDAS)? If so, in which areas?

Finland's national legislation largely aligns with the EU Regulation No. 910/2014 (eIDAS).

4. Does your jurisdiction recognise other types of electronic signatures than those regulated by the Regulation eIDAS?

No.

5. Is it possible for a Notary Public (or another person/entity) to officially verify a signature that has been made by electronic means? If so, in which cases and under what conditions?

No.

6. Which type of electronic signature is required when interacting with courts and public authorities? Is this practice uniform across all public bodies and authorities?

Regarding a document received by an authority, the type of electronic signature is not regulated by law, but most authorities require an advanced electronic signature. An electronic document received by an authority does not need to be supplemented with a signature if the document contains information about the sender and there is no reason to doubt the authenticity or integrity of the document.

A statement of claim, a summons, as well as a court document and other legal documents sent as an electronic message, can be signed mechanically. A mechanical signature means that instead of a physical signature, the name of the relevant person is written on the document using a word processing program. A decision document can also be signed electronically. However, the decision document must be signed with an advanced electronic signature that meets the requirements of the eIDAS Regulation or otherwise in a manner that ensures the authenticity and integrity of the document.

7. In practice, do public authorities effectively recognise the use of signing tools *(e.g. Adobe Sign, DocuSign)* when interacting with them?

Yes.

2. Electronic Identification

1. What means can be used to prove an individual´s identity electronically in your jurisdiction? Do electronic ID cards work *(e.g. in the form of mobile app)*?

In Finland, electronic identification services include:

- online banking codes provided by banks;
- mobile certificates issued by telecommunications operators;

- the Digital and Population Data Services Agency's Citizen Certificate stored on an identity card issued by the police and certain other identification certificates on various organisation cards; and
- registered identification broker services.

The most common of these are mobile certificates and identification using online banking credentials from banks.

2. Are there any means of electronic identification of legal entities in your jurisdiction?

In Finland, there are currently no specific means of electronic identification for legal entities. In practice, only the person authorized or entitled to act on behalf of the legal entity (e.g., directors) can be identified electronically.

3. Are there any electronic identification means provided by private entities in your jurisdiction *(e.g. Bank ID)?* Do they provide sufficient proof of identity when interacting with all public authorities or are there any limitations?

Yes, there are electronic identification means provided by private entities in Finland. These include online banking codes provided by banks and mobile certificates issued by telecommunications operators. These identification means are generally sufficient for proving identity when interacting with public authorities in Finland and the National Cyber Security Centre Finland (NCSC-FI) monitors and supervises compliance with the requirements for strong electronic identification services. However, the assurance level of a strong electronic identification service may vary, and some authorities may have specific requirements for certain transactions.

4. Is there only one/multiple electronic identification means offered directly by the state in your jurisdiction?

There is only one, the citizen certificate. The citizen certificate is available on the ID card's chip and can be used to log in to official e-services or make electronic signatures. The ID card applications are submitted to the police.

3. Electronic Communications

1. What means of electronic communication with public authorities are used in your jurisdiction?

In Finland it is possible to communicate electronically with all public authorities and bodies and the Finnish government is gradually shifting to making digital services the primary channel for accessing the services of public authorities.

The means of communication vary depending on the authority, but most communication is done via electronic platforms and email.

2. Are there any state-guaranteed means of electronic communication that can be used to communicate with the public authorities? If so, can individuals and legal entities also communicate with each other through this/these means?

By state guaranteed means we mean electronic communications means that come from and are operated by the state/state institutions themselves.

Yes, there are various state-guaranteed means of electronic communication, such as the suomi.fi -service and the Business Information System. Suomi.fi is a comprehensive online service portal that provides access to various public services and information for citizens, businesses, and organizations. It includes services related to health, education, employment, social security, and more. The Business Information System is a Finnish government service jointly maintained by the Finnish Patent and Registration Office and the Finnish Tax Administration. It provides access to the Finnish Trade Register and the Finnish Register of Foundations, allowing users to file information for both agencies.

3. In your jurisdiction, is the use of data boxes in communication with courts and public authorities common? If so, are there any exceptions when a data box cannot be used?

**** Data box is an electronic documents delivery system that enables individuals and legal entities to send/receive electronic documents to/from public authorities free of charge. It works similarly to an email box, except that the identity of the owner of the data box is officially verified. Individuals and legal entities can also communicate electronically with each other using the data box, but for a fee.***

The concept of a data box, as described, is not implemented in Finland. Instead, Finland relies on other electronic communication methods, such as the Suomi.fi service and various electronic identification means provided by private entities like online banking credentials and mobile certificates to send and receive secure emails.

4. Are there any specific formalities that must be met when communicating with public authorities *(e.g. document format, signatures, attachments etc.)*?

It is common for authorities to specify the acceptable document format, which is commonly PDF.

5. Are there any legal fictions/presumptions associated with electronic service of documents in your jurisdiction *(e.g. service by fiction)*?

The electronic service of documents is legislated in Finland. The responsibility for ensuring that an electronically delivered message reaches its destination lies with the sender. A

message is considered received when it is available to the receiver in a receiving device or information system in such a way that it can be processed, such as read or its file format changed.

6. In your jurisdiction, is it possible to communicate electronically with all public authorities? If not, which ones cannot?

In Finland, it is possible to communicate electronically with all public authorities.

7. Is there an obligation to communicate with some public authorities/on certain matters only electronically?

No, although in many cases the primary form of communication is digital.

FRANCE

DELSOL Avocats France

1. Electronic Legal Acts and Signatures

1. What are the requirements for a written legal act executed by electronic means to be valid? *(e.g. signature, identification of the person acting, capture of its content...)*

For a written legal document produced by electronic means to be valid in France, a number of conditions must be met:

Reliable electronic signature: The document must be signed electronically, and this signature must enable the signatory to be reliably identified. According to article 1367 of the French Civil Code, an electronic signature "consists of the use of a reliable identification process guaranteeing its link with the document to which it is attached".

Identification of the Signatory: The system used must ensure certain identification of the person signing. This can be achieved using electronic certificates, secure access codes or other strong authentication methods.

Integrity of the document: The content of the document must be preserved in such a way as to guarantee its integrity. It must not be possible to alter it after it has been signed without this being detectable.

Compliance with Legal Requirements: The electronic document must comply with the same legal requirements as its paper version. Some transactions, such as notarial deeds, may require a particular form that is not compatible with an electronic medium.

2. How does judicial practice view electronic legal acts? In practice, what evidence is required and/or accepted by the courts?

In practice, French courts accept electronic legal documents and electronic evidence, provided that the mechanisms for identifying the signatory and guaranteeing the integrity of the document are reliable. The use of qualified electronic signatures and compliance with the eIDAS regulation strengthen the evidential value of electronic documents before the courts. The courts apply this principle of functional equivalence, accepting electronic writing as evidence as long as these conditions are met (1366 Code civil). The parties must prove that the deed has not been altered since its creation. This can be established by electronic time stamps, digital certificates or electronic seals. The courts have confirmed the validity of electronic documents in a number of rulings, provided that the legal requirements are met (Cass. Civ. 1ère, 6 mai 2010, n°09-13.591).

3. Does the national legislation differ in any respect from the EU Regulation No. 910/2014 (eIDAS)? If so, in which areas?

France retains certain legislative specificities. These differences can be seen mainly in the additional requirements for certain types of legal act (Public notary legal acts where the physical presence of signatories is sometimes required), the national standards for trust service providers (France has a national electronic identity, independent from eIDAS , and additional rules imposed by the Agence nationale de la sécurité des systèmes d'information (ANSSI)), and the rules on archiving and electronic evidence.

It is therefore important for practitioners and businesses to take account of both the eIDAS regulation and the relevant French legislation to ensure legal compliance.

4. Does your jurisdiction recognise other types of electronic signatures than those regulated by the Regulation eIDAS?

French law takes a more flexible approach to electronic signatures than the eIDAS regulation. It recognises the validity of any electronic signature provided that it is based on a reliable process for identifying the signatory and that it expresses his or her consent to the obligations arising from the document, in accordance with article 1367 of the Civil Code. In France, therefore, electronic signatures that do not comply with the standards of the eIDAS regulation may be legally valid.

5. Is it possible for a Notary Public (or another person/entity) to officially verify a signature that has been made by electronic means? If so, in which cases and under what conditions?

A notary public can officially verify an electronic signature in France, mainly in the context of electronic authentic instruments or the certification of signatures on private documents. This

verification must comply with the legal conditions relating to the identification of the signatory, the use of qualified electronic signatures and the guarantee of the integrity of the document.

Some notarial deeds in France still require the physical presence of the signatories:

- Inter vivos donations (excluding manual donations);
- Authentic wills;
- Marriage contracts;
- Acts of notoriety establishing filiation or possession of status;
- Acts of notoriety establishing filiation or possession of status.

6. Which type of electronic signature is required when interacting with courts and public authorities? Is this practice uniform across all public bodies and authorities?

The type of electronic signature required when dealing with the courts and public authorities in France varies depending on the organisation involved and the nature of the procedure. Although a qualified electronic signature is often required for acts of high legal importance, some administrations accept an advanced electronic signature for less sensitive procedures. Practice is not uniform, and it is essential to refer to the specific requirements of each body or procedure to determine the type of electronic signature required.

7. In practice, do public authorities effectively recognise the use of signing tools *(e.g. Adobe Sign, DocuSign)* when interacting with them?

French public authorities accept the use of electronic signature tools such as Adobe Sign or DocuSign, provided that the signatures meet the legal requirements in terms of reliability, identification of the signatory and link with the document signed. However, practice differs greatly depending on the administration concerned. Some administration do not even request a signing tool, a scanned copy of a signed document being enough (creation of an association, documents sent to the commercial register). Other will require the original signed copy of a deed (Civil status, social services).

2. Electronic Identification

1. What means can be used to prove an individual´s identity electronically in your jurisdiction? Do electronic ID cards work *(e.g. in the form of mobile app)*?

In France, electronic proof of identity is based on secure systems governed by law. These include

- The Carte Nationale d'Identité Électronique (CNIe), which can be used via the "France Identité" mobile application, offering a modern solution for proving identity online.

- The FranceConnect platform, which centralises authentication for many public services.

- La Poste's qualified electronic certificates and digital identity, providing secure identification for specific procedures. These tools meet the requirements of the eIDAS regulation and guarantee the legal recognition of electronic identification in France.

2. Are there any means of electronic identification of legal entities in your jurisdiction?

In France, electronic identification methods for legal entities include qualified electronic certificates, FranceConnect Entreprise, and La Poste's digital identity for businesses. These systems guarantee reliable, secure and legally recognised authentication, making administrative and commercial procedures easier for businesses.

3. Are there any electronic identification means provided by private entities in your jurisdiction *(e.g. Bank ID)?* Do they provide sufficient proof of identity when interacting with all public authorities or are there any limitations?

In France, only certain means of electronic identification provided by approved private entities are accepted by the public authorities. La Poste's digital identity and qualified electronic certificates from ANSSI-approved service providers are the only recognised options for certain administrative procedures.

Bank identifications, on the other hand, do not yet allow direct interaction with the public authorities. The limitations often depend on the level of security required by the authorities and the accreditation of service providers on platforms such as FranceConnect.

4. Is there only one/multiple electronic identification means offered directly by the state in your jurisdiction?

France offers several means of electronic identification directly provided by the government, including FranceConnect for the general public, the Carte Nationale d'Identité Électronique (CNIe) with the France Identité application, and the Système d'Authentification Sécurisée (SAS) for public servants.

These solutions are tailored to different levels of security and administrative needs, with FranceConnect being the main solution and widely used for day-to-day procedures.

3. Electronic Communications

1. What means of electronic communication with public authorities are used in your jurisdiction?

In France, the means of electronic communication with public authorities are varied and include centralised platforms such as FranceConnect, specialised systems for courts and billing, and secure messaging.

2. Are there any state-guaranteed means of electronic communication that can be used to communicate with the public authorities? If so, can individuals and legal entities also communicate with each other through this/these means?

By state guaranteed means we mean electronic communications means that come from and are operated by the state/state institutions themselves.

1. FranceConnect portal

Overview: FranceConnect is a centralised authentication service that enables citizens to access a wide range of online public services with a single identifier.

Use: By connecting via FranceConnect, users can access public service portals such as Impots.gouv.fr, Ameli (health insurance), CAF (family allowances), and Service-Public.fr for administrative procedures.

2. Télérecours and Télérecours Citoyens

Overview: Télérecours and TélérecoursCitoyens are electronic communication platforms for exchanges between litigants, lawyers and administrative courts.

How to use: - *Télérecours*: for lawyers and public authorities to manage cases before administrative courts. - *Télérecours Citoyens* : Suitable for individuals not represented by a lawyer wishing to lodge administrative appeals online.

Advantages: These platforms make it possible to file applications, consult case documents and receive court decisions electronically, thus guaranteeing traceability and simplified access to administrative justice services.

3. Secure messaging from Assurance Maladie and CAF

Overview: Users can communicate with Assurance Maladie (via Ameli) and CAF (Caisse d'allocations familiales) via secure messaging integrated into their respective online spaces.

How to use: Policy holders can ask questions, send supporting documents and track their requests via these messaging systems.

4. ChorusPro portal for electronic invoicing

Presentation: Chorus Pro is the national electronic invoicing portal for companies that invoice public administrations for services.

Use: Companies subject to electronic invoicing can submit their invoices to the portal, which are then forwarded to the public bodies concerned.

5. E-barreau/RPVA (Réseau Privé Virtuel des Avocats)

Presentation: E-barreau or RPVA is the secure network used by lawyers to communicate with civil courts.

Use: Lawyers can file documents, consult their clients' files and communicate with the courts via this network.

6. Démarches-Simplifiées.fr

Overview: Démarches-Simplifiées.fr is a platform that enables a wide range of administrative procedures to be carried out online, simply and securely.

Use: Citizens can submit applications, forms or documents for various administrative procedures (e.g. grants, authorisations).

7. Email and secure messaging

Common use: In some cases, administrations accept e-mail communications, although secure systems are preferred.

Secure messaging: Some administrations provide secure-email addresses for sending sensitive documents, but the use of platforms such as FranceConnect is generally encouraged for security reasons.

8. SMS and notifications to track procedures

Overview: Several administrations send notifications by SMS to inform citizens of the progress of their procedures (e.g. status of identity card or passport applications).

3. In your jurisdiction, is the use of data boxes in communication with courts and public authorities common? If so, are there any exceptions when a data box cannot be used?

**** Data box is an electronic documents delivery system that enables individuals and legal entities to send/receive electronic documents to/from public authorities free of charge. It works similarly to an email box, except that the identity of the owner of the data box is officially verified. Individuals and legal entities can also communicate electronically with each other using the data box, but for a fee.***

Data boxes are commonly used in communications with the courts and certain public authorities, but their use is not compulsory in all situations or for all audiences. Systems such as RPVA/e-Barreau, Télérecours and Chorus Pro are widely used, particularly by professionals (lawyers, businesses). However, for private individuals and procedures requiring a physical presence, alternatives such as postal mail or hand-delivery remain available.

4. Are there any specific formalities that must be met when communicating with public authorities *(e.g. document format, signatures, attachments etc.)*?

The specific formalities for communicating with the French public authorities include requirements in terms of document format (PDF mostly), electronic (qualified or advanced electronic signature - use of FranceConnect) or handwritten signatures, supporting documents and submission protocol. Failure to comply with these formalities may result in delays or refusal of the application, so it is essential to check the requirements carefully on the administrative platforms or with the authority concerned.

5. Are there any legal fictions/presumptions associated with electronic service of documents in your jurisdiction *(e.g. service by fiction)*?

In France, electronic notification of documents is often governed by legal presumptions that make it easier to take them into account in administrative, tax and legal proceedings.

A presumption of receipt generally applies: a document is deemed to have been received by the recipient as soon as it is made available on a secure platform (for example, Télérecours for the administrative courts or the impots.gouv.fr tax portal), whether the recipient has consulted it. This presumption is intended to ensure the continuity of proceedings and avoid delays caused by failure to consult the platform.

Some electronic notifications are also based on a fiction of notification: the notification is legally valid as soon as it is put online, even if the recipient has not read it. This principle is common in systems such as the Virtual Private Network for Lawyers (VPN). However, the addressee may contest the notification in the event of force majeure or technical difficulties that have prevented it from being consulted. These electronic notification rules guarantee the legal security of exchanges, although appeals are possible in limited cases.

6. In your jurisdiction, is it possible to communicate electronically with all public authorities? If not, which ones cannot?

In France, although electronic communication with the public authorities is widely developed, it is not yet available for all procedures. Online services enable many procedures to be carried out, but some authorities, such as town halls for civil status documents (birth, marriage, death) and notaries for authentic instruments, still require a physical presence. These procedures often involve legal obligations that require you to appear in person to guarantee authenticity and consent.

In addition, certain procedures at consulates (such as passport or identity card applications) and courts for criminal hearings cannot be carried out exclusively electronically. Although digital tools such as Télérecours and the RPVA facilitate exchanges in civil and administrative courts, some legal proceedings are still limited to face-to-face communications. Electronic communication is now widespread, but some procedures still require physical interaction for reasons of security or legal validation.

7. Is there an obligation to communicate with some public authorities/on certain matters only electronically?

In France, certain administrative and legal procedures require communication to be carried out exclusively by electronic means, for reasons of security and simplification. In the area of public procurement, companies have been required to send their invoices to the authorities via the Chorus Pro platform since 2020, and this electronic invoicing obligation will be extended to transactions between companies from 2024.

Similarly, companies' tax and social security returns, such as VAT, corporation tax and social security contributions (DSN), must be filed online, in particular via the impots.gouv.fr and Net-

entreprises portals. In the legal sector, electronic communication is mandatory for lawyers in civil and administrative cases. Lawyers are required to use the RPVA (RéseauPrivé Virtuel des Avocats) to communicate with civil courts and Télérecours for administrative courts.

These secure platforms guarantee the confidentiality and speed of procedural exchanges. Dematerialisation is now an obligation in certain key areas in France, aimed at securing and streamlining exchanges with public authorities.

GERMANY

Buse

1. Electronic Legal Acts and Signatures

1. What are the requirements for a written legal act executed by electronic means to be valid? *(e.g. signature, identification of the person acting, capture of its content...)*

Section 126a - German Civil Code:

> (1) If electronic form is to replace the written form prescribed by statute, the issuer of the declaration must add their name to it and provide the electronic document with a qualified electronic signature.
>
> (2) In the case of a contract, the parties must each provide a counterpart with an electronic signature as described in subsection (1).

2. How does judicial practice view electronic legal acts? In practice, what evidence is required and/or accepted by the courts?

Prima facie evidence for its authenticity / can be challenged by expert opinions

3. Does the national legislation differ in any respect from the EU Regulation No. 910/2014 (eIDAS)? If so, in which areas?

The implementation of eIDAS 2.0 is still in progress.

4. Does your jurisdiction recognise other types of electronic signatures than those regulated by the Regulation eIDAS?

No.

5. Is it possible for a Notary Public (or another person/entity) to officially verify a signature that has been made by electronic means? If so, in which cases and under what conditions?

Yes, as attorneys. When interacting with courts and attorneys.

6. Which type of electronic signature is required when interacting with courts and public authorities? Is this practice uniform across all public bodies and authorities?

Advanced electronic signature.

7. In practice, do public authorities effectively recognise the use of signing tools *(e.g. Adobe Sign, DocuSign)* when interacting with them?

Yes, when e-mail or fax is accepted.

2. Electronic Identification

1. What means can be used to prove an individual´s identity electronically in your jurisdiction? Do electronic ID cards work *(e.g. in the form of mobile app)*?

N/A

2. Are there any means of electronic identification of legal entities in your jurisdiction?

Yes.

3. Are there any electronic identification means provided by private entities in your jurisdiction *(e.g. Bank ID)?* Do they provide sufficient proof of identity when interacting with all public authorities or are there any limitations?

Yes, few certified providers, e.g. Docusign.

4. Is there only one/multiple electronic identification means offered directly by the state in your jurisdiction?

Yes, multiple, e.g. beA.

3. Electronic Communications

1. What means of electronic communication with public authorities are used in your jurisdiction?

BeA.

2. Are there any state-guaranteed means of electronic communication that can be used to communicate with the public authorities? If so, can individuals and legal entities also communicate with each other through this/these means?

By state guaranteed means we mean electronic communications means that come from and are operated by the state/state institutions themselves.

Yes, beA – but only for attorneys.

3. In your jurisdiction, is the use of data boxes in communication with courts and public authorities common? If so, are there any exceptions when a data box cannot be used?

**** Data box is an electronic documents delivery system that enables individuals and legal entities to send/receive electronic documents to/from public authorities free of charge. It works similarly to an email box, except that the identity of the owner of the data box is officially verified. Individuals and legal entities can also communicate electronically with each other using the data box, but for a fee.***

Yes, for tax purposes, e.g. Elstar, and for communication, e.g. DE-Mail.

4. Are there any specific formalities that must be met when communicating with public authorities *(e.g. document format, signatures, attachments etc.)*?

Yes, specific format and searchable (PDF-A), embedded font.

5. Are there any legal fictions/presumptions associated with electronic service of documents in your jurisdiction *(e.g. service by fiction)*?

Yes, Art. 173 of the Code of Civil Procedure.

6. In your jurisdiction, is it possible to communicate electronically with all public authorities? If not, which ones cannot?

Not with all, e.g. patent authorities.

7. Is there an obligation to communicate with some public authorities/on certain matters only electronically?

Yes, with all kinds of courts.

GREECE

Corina Fassouli-Grafanaki & Associates Law Firm (CFG&A law firm)

1. Electronic Legal Acts and Signatures

1. What are the requirements for a written legal act executed by electronic means to be valid? *(e.g. signature, identification of the person acting, capture of its content...)*

It depends whether the legal act requires a certain document type or procedure. According to the Greek Civil Procedure Code and the relevant case law, legal acts that have no requirements may be executed even via email.

Regarding the signatures, legal acts may be executed with physical signatures, digital signatures or via gov.gr (using government credentials).

2. How does judicial practice view electronic legal acts? In practice, what evidence is required and/or accepted by the courts?

It depends whether the legal act requires a certain document type or procedure. According to the Greek Civil Procedure Code and the relevant case law, legal acts that have no requirements may be executed even via email and as such accepted by the courts.

3. Does the national legislation differ in any respect from the EU Regulation No. 910/2014 (eIDAS)? If so, in which areas?

It does not.

4. Does your jurisdiction recognise other types of electronic signatures than those regulated by the Regulation eIDAS?

Yes. Gov.gr.

5. Is it possible for a Notary Public (or another person/entity) to officially verify a signature that has been made by electronic means? If so, in which cases and under what conditions?

Any public official may proceed in verification of physical signatures with the identification of the person acting present. Digital signatures are accepted erga omnes without any added procedure. The most common is via gov.gr (using government credentials).

6. Which type of electronic signature is required when interacting with courts and public authorities? Is this practice uniform across all public bodies and authorities?

Gov.gr is the most common. It is uniformly accepted by all public bodies and authorities by law.

7. In practice, do public authorities effectively recognise the use of signing tools *(e.g. Adobe Sign, DocuSign)* when interacting with them?

Not all the times due to misinformation. This is why gov.gr is the most effective, because it is uniformly accepted by law.

2. Electronic Identification

1. What means can be used to prove an individual´s identity electronically in your jurisdiction? Do electronic ID cards work *(e.g. in the form of mobile app)*?

Mobile app + Public communication registry (gov.gr).

2. Are there any means of electronic identification of legal entities in your jurisdiction?

Mobile app + Public communication registry (gov.gr).

3. Are there any electronic identification means provided by private entities in your jurisdiction *(e.g. Bank ID)?* Do they provide sufficient proof of identity when interacting with all public authorities or are there any limitations?

The crosschecking possess may involve bank IDs as well, to verify the info registered in the Public communication registry (gov.gr)

4. Is there only one/multiple electronic identification means offered directly by the state in your jurisdiction?

One (gov.gr).

3. Electronic Communications

1. What means of electronic communication with public authorities are used in your jurisdiction?

E-mails + fax (not anymore) + gov.gr platform.

2. Are there any state-guaranteed means of electronic communication that can be used to communicate with the public authorities? If so, can individuals and legal entities also communicate with each other through this/these means?

By state guaranteed means we mean electronic communications means that come from and are operated by the state/state institutions themselves.

Yes, gov.gr. Individuals and legal entities may not communicate with each other through this platform.

3. In your jurisdiction, is the use of data boxes in communication with courts and public authorities common? If so, are there any exceptions when a data box cannot be used?

**** Data box is an electronic documents delivery system that enables individuals and legal entities to send/receive electronic documents to/from public authorities free of charge. It works similarly to an email box, except that the identity of the owner of the data box is officially verified. Individuals and legal entities can also communicate electronically with each other using the data box, but for a fee.***

Data boxes may be used in communication with courts and public authorities (opt in).

4. Are there any specific formalities that must be met when communicating with public authorities *(e.g. document format, signatures, attachments etc.)*?

In some cases.

5. Are there any legal fictions/presumptions associated with electronic service of documents in your jurisdiction *(e.g. service by fiction)*?

Yes. Opt-in required.

6. In your jurisdiction, is it possible to communicate electronically with all public authorities? If not, which ones cannot?

It should according to the current law. Not all authorities have reliable platforms or are integrated to the gov.gr platform.

7. Is there an obligation to communicate with some public authorities/on certain matters only electronically?

Yes, if there is a law preventing the physical communication, or requirements to pre-register before the physical communication.

ITALY

RPLT - RP legalitax

1. Electronic Legal Acts and Signatures

1. What are the requirements for a written legal act executed by electronic means to be valid? *(e.g. signature, identification of the person acting, capture of its content...)*

Under Italian law, specifically the Digital Administration Code (Codice dell'Amministrazione Digitale – CAD), the requirements for a legally valid written legal act executed by electronic means include the following:

1. Identification of the Parties: The parties involved must be clearly identified within the document. This can be done through the use of electronic identification systems that comply with European regulations (eIDAS – electronic IDentification, Authentication and trust Services).

2. Integrity of Content: The content of the document must remain unchanged after signing. This is typically ensured through cryptographic methods that protect the document from unauthorized alterations.

3. Electronic Signature: The document must be signed using a qualified electronic signature (QES), which provides the same legal value as a handwritten signature. The QES must be created using a secure signature creation device and based on a qualified certificate issued by a trusted certification authority.

4. Timestamp: For certain acts, a qualified timestamp may be necessary to prove when the document was signed. This provides additional assurance regarding the timing of the signing and the validity of the document.

5. Storage and Retrieval: The electronic document must be stored in a manner that ensures its integrity, confidentiality, and accessibility over time. This often involves using systems that adhere to specific standards for electronic document management.

2. How does judicial practice view electronic legal acts? In practice, what evidence is required and/or accepted by the courts?

In Italy, judicial practice generally recognizes electronic legal acts as valid, provided they meet the legal requirements specified for electronic signatures and document integrity. Courts assess electronic evidence based on its ability to reliably demonstrate authenticity, integrity, and the identity of the signatory.

Here's how electronic legal acts are typically viewed and what evidence may be required or accepted by Italian courts:

1. Type of Electronic Signature: The type and level of the electronic signature used play a significant role. A Qualified Electronic Signature (QES) is presumed to meet all the requirements of a handwritten signature and is generally accepted as valid without additional evidence. Simple electronic signatures might require additional proof of authenticity in court.

2. Certificate of Authenticity: For signatures like QES, the corresponding certificate issued by a trusted certification authority serves as evidence of the signer's identity and is crucial in court proceedings. This certificate must be valid at the time the document was signed.

3. Audit Trail and Logs: Systems that capture electronic signatures (for example Go Sign or dike) maintain an audit trail and logs that can be presented as evidence to show the process followed, including timestamps and IP addresses, which help establish the circumstances under which the act was executed.

4. Expert Witnesses: In some cases, technical experts may be required to testify about the security and procedures involved in the electronic signing process, especially if the authenticity or integrity of the document is challenged.

5. Metadata: Metadata associated with electronic documents (such as timestamps, document history, and secure hash values) can be critical in proving that the document has not been altered since it was signed.

3. Does the national legislation differ in any respect from the EU Regulation No. 910/2014 (eIDAS)? If so, in which areas?

Italian legislation regarding electronic identification and trust services is largely aligned with EU Regulation No. 910/2014.

However, there are areas where Italian law provides additional details or specific practices. For example, while eIDAS sets the overarching principles and requirements, Italian legislation through the Digital Administration Code (Codice dell'Amministrazione Digitale, CAD) provides

specific implementation details for how these principles are applied within the Italian context, particularly regarding public administration processes and digital transformation.

Secondly, Italy has developed its national digital identity system, SPID (Sistema Pubblico di Identità Digitale, “SPID”), which operates within the framework of eIDAS but includes specific procedures and technical requirements tailored to Italian citizens and businesses.

Moreover, Italian legislation includes guidelines that are specific to certain sectors, like healthcare or finance, which incorporate eIDAS principles but are adapted to meet national sectoral needs, ensuring integration with Italy’s existing regulatory environment. These additional guidelines ensure that electronic transactions meet the specific needs and compliance requirements of each sector while aligning with the broader framework set by eIDAS.

These sector-specific guidelines are disseminated through regulatory bodies such as local health authorities for healthcare or financial supervisory authorities for finance. Here are some examples:

- In healthcare, the use of electronic signatures and digital records must comply with both national health regulations and EU directives, which emphasize privacy, data protection, and secure data exchange. The Italian Health Ministry and regional health authorities often issue specific guidelines on how electronic identification and records should be handled. The National Electronic Health Record (Fascicolo Sanitario Elettronico, FSE) serves as a central system for managing health data, which includes strict guidelines for accessing and sharing health information using electronic means.

- In the financial sector, regulations around electronic transactions focus on anti-money laundering (AML) and know-your-customer (KYC) requirements. The Bank of Italy and the Italian Ministry of Economy and Finance provide regulations and guidelines that include provisions for electronic transactions and digital identity verification.

4. Does your jurisdiction recognise other types of electronic signatures than those regulated by the Regulation eIDAS?

The Agency for Digital Italy on April 23, 2020, implemented a new form of electronic signature, through the national digital identity system, (Sistema Pubblico di Identità Digitale, “SPID”). The measure is particularly important because the new method of signing can be used for all acts and contracts for which the use of only the digital signature is not mandatory, and therefore, it could apply to a significant number of documents.

5. Is it possible for a Notary Public (or another person/entity) to officially verify a signature that has been made by electronic means? If so, in which cases and under what conditions?

Yes, it is possible for an Italian Notary Public or another authorized entity to officially verify a signature made by electronic means. A notary can verify a QES by checking the validity of the certificate associated with the signature. This typically involves ensuring that the signature is created using a certificate issued by a recognized certification authority and that the certificate

is valid and not revoked. Notaries in Italy are empowered to verify the identity of signatories and ensure the integrity and authenticity of electronic documents.

They use secure systems to access and verify electronic signatures and usually, they log this verification process to provide an audit trail. If the signature is linked to the SPID (Sistema Pubblico di Identità Digitale), which is Italy's Public Digital Identity System, it can provide an additional layer of verification as it is a government-approved means of digital identity. A notary can use SPID to confirm the identity of the signatory if the electronic signature process supports this form of verification.

For signatures that are not QES but are considered advanced electronic signatures, a notary might verify these if they comply with certain standards ensuring the signatory's identity is uniquely linked and that the signature can identify the signatory, created using means that the signatory can maintain under their sole control.

Some notaries use dedicated electronic systems that interface with national ID databases or certified providers to conduct these verifications officially. These systems help ensure that notaries can uphold the rigorous standards required for electronic transactions. These verifications are generally used when there is a legal or practical requirement to ensure the utmost reliability of a signature, such as in the transfer of property, company set up, or other formal legal agreements where authenticity and integrity are critical.

6. Which type of electronic signature is required when interacting with courts and public authorities? Is this practice uniform across all public bodies and authorities?

In Italy, when interacting with courts and public authorities, the type of electronic signature typically required is a Qualified Electronic Signature (QES). While the use of QES is widespread and generally the standard for formal interactions across public bodies, there might be variations in acceptance levels for less formal processes.

Some public administrations might accept an Advanced Electronic Signature (AES) or, in less formal interactions, a Simple Electronic Signature (SES), provided it meets the necessary authentication and integrity criteria for the specific transaction and complies with internal regulations of the specific authority.

In addition to electronic signatures, Certified Electronic Mail (PEC) is commonly used in Italy for official communications with authorities. PEC provides legal proof of sending and receiving an email, akin to traditional registered mail, which further complements electronic signature practices. Therefore, while a QES is the general standard, the requirements may vary depending on the specific public body or the type of document being processed.

7. In practice, do public authorities effectively recognise the use of signing tools *(e.g. Adobe Sign, DocuSign)* when interacting with them?

Italian public authorities primarily require electronic signatures that meet the standards set by the EU Regulation No. 910/2014 (eIDAS). This means the signatures should be Advanced Electronic Signatures (AES) or, ideally, Qualified Electronic Signatures (QES). In essence, while tools like Adobe Sign and DocuSign can be utilized for interacting with Italian public

authorities, they must generate signatures that meet regulatory requirements, primarily QES, to ensure they are accepted.

2. Electronic Identification

1. What means can be used to prove an individual´s identity electronically in your jurisdiction? Do electronic ID cards work *(e.g. in the form of mobile app)*?

The means used to prove an individual´s identity electronically are the following:

- CIE ("Carta d'Identità Elettronica"): is an electronic identity card where with citizens can access to online services with CIE credentials through 3 increasing security levels of identification:

  • 1°: access with username and password;

  • 2°: in addition to credentials above, you need to have another authentication level which demonstrates having the device (e.g. OTP or QR code)

  • 3°: you need to have a device or smartphone with Near Field Communication ("NFC") to recognise the CIE.

  In addition, the CIE can be used with CieSign app as an advanced electronic signature (FEA) tool, allowing citizens to easily sign electronic documents.

- SPID ("Sistema Pubblico di Identità Digitale"): is the key for simply, fast and secure access to the digital services of local and central administrations.

- CNS ("Carta Nazionale dei Servizi"): is a digital smart card or Token USB to access to the digital services of local and central administrations.

2. Are there any means of electronic identification of legal entities in your jurisdiction?

No, means of electronic identification are used only by individuals.

Nevertheless, a Public System for Professional Digital Identity (SPID for professional use by legal entities, also known as SPID for Legal Entities or Type 4 SPID) exists, which is a specific type of Digital Identity granted to an individual with the approval of the legal entity. The SPID Business Digital Identity includes both the individual's data and the associated legal entity's data. This version of SPID requires the use of additional credentials issued to individuals authorized to act on behalf of the legal entity.

3. Are there any electronic identification means provided by private entities in your jurisdiction *(e.g. Bank ID)?* Do they provide sufficient proof of identity when interacting with all public authorities or are there any limitations?

No, you need to have username and password to access to account of private entities. Regarding identification means provided by private entities, Italy does not have an equivalent to systems like the Nordic BankID, which is entirely private and used widely across sectors. SPID, CIE, and CNS are the main systems used for interactions with public authorities, and these are sufficiently recognized due to their standardization and government backing.

4. Is there only one/multiple electronic identification means offered directly by the state in your jurisdiction?

Please see the answer above (SPID, CIE and CNS).

3. Electronic Communications

1. What means of electronic communication with public authorities are used in your jurisdiction?

Please see the answer above (E-Mail and Pec).

2. Are there any state-guaranteed means of electronic communication that can be used to communicate with the public authorities? If so, can individuals and legal entities also communicate with each other through this/these means?

By state guaranteed means we mean electronic communications means that come from and are operated by the state/state institutions themselves.

There are some procedures within specific public authorities that can only be handled through the submission of electronic applications. To access these platforms, it is necessary to identify oneself using digital identification tools such as the electronic ID card (CIE) or SPID.

3. In your jurisdiction, is the use of data boxes in communication with courts and public authorities common? If so, are there any exceptions when a data box cannot be used?

**** Data box is an electronic documents delivery system that enables individuals and legal entities to send/receive electronic documents to/from public authorities free of charge. It works similarly to an email box, except that the identity of the owner of the data box is officially verified. Individuals and legal entities can also communicate electronically with each other using the data box, but for a fee.***

Yes, it's frequent. In civil, criminal, and tax proceedings, lawyers communicate with the courts through their own identification device and using their certified email (PEC). As for public administrations, after the introduction of SPID, more and more activities can be carried out electronically.

4. Are there any specific formalities that must be met when communicating with public authorities *(e.g. document format, signatures, attachments etc.)*?

No. When documents are submitted to the Court, for example in the case of legal proceedings, some documents attached must be in PDF/A format and therefore native PDFs. Others must necessarily be electronically signed, such as the power of attorney for litigation. Attachments can also simply be scanned documents.

5. Are there any legal fictions/presumptions associated with electronic service of documents in your jurisdiction *(e.g. service by fiction)*?

In the Italian system, when a document is served electronically, the proof of it correct delivery is provided by two confirmation receipts (so called the receipt of acceptance and delivery confirmations). These receipts are sent to the lawyer's certified email inbox.

6. In your jurisdiction, is it possible to communicate electronically with <u>all</u> public authorities? If not, which ones cannot?

In Italy, digital communication with Public Administrations (PA) is widespread, thanks to regulations like the Digital Administration Code and tools such as SPID, PEC, and PagoPA.

However, exceptions remain, particularly in smaller municipalities, technical or health offices, law enforcement, and sectors with complex bureaucracy, where in-person presence or paper documents may still be required. Although the push for full digitalization is ongoing, these barriers persist in some areas.

7. Is there an obligation to communicate with some public authorities/on certain matters only electronically?

Yes, in Italy there is an increasing obligation to communicate with certain public authorities and on specific matters only electronically. This push towards digital communication is part of the broader effort to enhance efficiency and accessibility within public administration.

Yes, for example, in civil, criminal, and tax proceedings, the transition to electronic procedures began in 2014, and today legal professionals are required to file documents electronically when interacting with the civil court system. This includes filing lawsuits, motions, and other legal documents through the dedicated online platform. Moreover, participation in public tenders generally requires the use of online platforms to submit bids and communicate with contracting authorities.

LATVIA

WIDEN Latvia

1. Electronic Legal Acts and Signatures

1. What are the requirements for a written legal act executed by electronic means to be valid? *(e.g. signature, identification of the person acting, capture of its content...)*

An electronic document shall be considered to have been signed by hand if it has a secure electronic signature. An electronic document shall be considered to have been signed by hand also in such cases where it has an electronic signature, and the parties have agreed in writing regarding the signing of electronic documents with an electronic signature. In such case, the written agreement shall be drawn up and signed on paper or electronically with a secure electronic signature.

2. How does judicial practice view electronic legal acts? In practice, what evidence is required and/or accepted by the courts?

Courts accept electronic documents signed with a qualified electronic signature (QES), as it provides a high level of authenticity and is legally equivalent to a handwritten signature.

3. Does the national legislation differ in any respect from the EU Regulation No. 910/2014 (eIDAS)? If so, in which areas?

No.

4. Does your jurisdiction recognise other types of electronic signatures than those regulated by the Regulation eIDAS?

No.

5. Is it possible for a Notary Public (or another person/entity) to officially verify a signature that has been made by electronic means? If so, in which cases and under what conditions?

If the document is signed while the parties are on a video conference in the presence of a notary, then yes.

6. Which type of electronic signature is required when interacting with courts and public authorities? Is this practice uniform across all public bodies and authorities?

The electronic document shall be signed if it has a secure electronic signature and time stamp.

7. In practice, do public authorities effectively recognise the use of signing tools *(e.g. Adobe Sign, DocuSign)* when interacting with them?

No.

2. Electronic Identification

1. What means can be used to prove an individual´s identity electronically in your jurisdiction? Do electronic ID cards work *(e.g. in the form of mobile app)*?

Electronic ID (eID) Cards, eParaksts Mobile (eSignature Mobile), Smart-ID, Banking Authentication (BankLink): Latvian banks offer digital identity verification through BankLink, an authentication service used for online banking. This method allows users to log into various online platforms using their banking credentials and is sometimes accepted as proof of identity in cases where advanced security levels aren't necessary.

2. Are there any means of electronic identification of legal entities in your jurisdiction?

Yes.

3. Are there any electronic identification means provided by private entities in your jurisdiction *(e.g. Bank ID)?* Do they provide sufficient proof of identity when interacting with all public authorities or are there any limitations?

Yes, Bank ID, Smart ID.

4. Is there only one/multiple electronic identification means offered directly by the state in your jurisdiction?

eID Card and eParaksts Mobile.

3. Electronic Communications

1. What means of electronic communication with public authorities are used in your jurisdiction?

E-address, e-mail, specially designed systems, for example, the State Revenue Service has its own system (EDS).

2. Are there any state-guaranteed means of electronic communication that can be used to communicate with the public authorities? If so, can individuals and legal entities also communicate with each other through this/these means?

By state guaranteed means we mean electronic communications means that come from and are operated by the state/state institutions themselves.

Yes, e-address (Data box as indicated in the next question). Not used for communication between individuals.

3. In your jurisdiction, is the use of data boxes in communication with courts and public authorities common? If so, are there any exceptions when a data box cannot be used?

**** Data box is an electronic documents delivery system that enables individuals and legal entities to send/receive electronic documents to/from public authorities free of charge. It works similarly to an email box, except that the identity of the owner of the data box is officially verified. Individuals and legal entities can also communicate electronically with each other using the data box, but for a fee.***

The use of data boxes is mandatory for legal entities from January 1, 2023, (a legal entity has to have an e-address). Given that it is a relatively recent tool, the most common way in communication with courts and public authorities is using e-mail.

4. Are there any specific formalities that must be met when communicating with public authorities *(e.g. document format, signatures, attachments etc.)*?

Yes, the documents have to be signed with qualified electronic signature (QES). Also, the courts state that when adding files to the e-case portal, the size of the file to be added must not exceed 10 MB. Allowed formats: *.pdf, *.doc, *.docx,*.odt, *.txt, *.rtf, *.jpg, *.tif, *.edoc.

5. Are there any legal fictions/presumptions associated with electronic service of documents in your jurisdiction *(e.g. service by fiction)*?

The document shall be notified to the official electronic address in the cases and according to the procedures laid down in the Law on the Official Electronic Address, if the addressee has an activated official electronic address account.

A document which has been sent to the official electronic address shall be deemed notified on the second working day after sending thereof. A document shall be notified via electronic mail,

using a secure electronic signature. The legal norms governing the circulation of electronic documents shall be applied to such notification of a document.

A document may be notified via electronic mail, without using a secure electronic signature, if the addressee has expressed a wish in writing to receive the document in the relevant way or such possibility has been provided for in a regulatory enactment. The document shall be notified to the electronic mail address indicated by the person. A document which has been sent via electronic mail shall be deemed notified on the second working day after sending thereof.

6. In your jurisdiction, is it possible to communicate electronically with <u>all</u> public authorities? If not, which ones cannot?

Have not come across a public authority that could not be contacted electronically.

7. Is there an obligation to communicate with some public authorities/on certain matters only electronically?

Yes, all reports to be submitted to the State Revenue Service, except annual report, must be submitted electronically, also the legal entities have the obligation to register an e-address, then the state will send all the notifications to the address, and it's presumed that the recipient has received it. The recipient can answer by mail (not use the e-address).

NETHERLANDS

Dirkzwager legal & tax

1. Electronic Legal Acts and Signatures

1. What are the requirements for a written legal act executed by electronic means to be valid? *(e.g. signature, identification of the person acting, capture of its content...)*

Under Dutch law, the principle is that legal acts can be performed without formality. In some cases, however, the law or the parties do impose specific requirements, such as the requirements of writing and signing. For example, Article 6:227a BW provides for the written form requirements for contracts performed electronically, and Article 3:15a BW governs the method of electronic signing.

2. How does judicial practice view electronic legal acts? In practice, what evidence is required and/or accepted by the courts?

In civil procedures in the Netherlands, evidence can be provided by all means, unless the law stipulates otherwise (Article 152 of the Dutch Code of Civil Procedure, Rv). This means that the court will, in principle, admit electronic evidence, unless the law prohibits it. Evidence based on email correspondence, WhatsApp messages, or SMS messages is, therefore, generally admissible.

According to Article 150 Rv, the rule is that the party asserting a claim — for example, someone relying on a particular clause of a contract — bears the burden of proving that claim.

3. Does the national legislation differ in any respect from the EU Regulation No. 910/2014 (eIDAS)? If so, in which areas?

The Dutch legal system has been fully harmonized with this regulation. There are no provisions that conflict with the rules derived from the eIDAS Regulation.

4. Does your jurisdiction recognise other types of electronic signatures than those regulated by the Regulation eIDAS?

No.

5. Is it possible for a Notary Public (or another person/entity) to officially verify a signature that has been made by electronic means? If so, in which cases and under what conditions?

Since the notary cannot verify the electronical technical aspects, it is required that the person whose signature is being legalized signs the document personally in the presence of the notary with a wet signature.

6. Which type of electronic signature is required when interacting with courts and public authorities? Is this practice uniform across all public bodies and authorities?

In case of court proceedings, a wet signature is obliged (of the attorney). However, there are several governmental proceedings which includes an electronic proceeding, whereby a wet signature is not applicable. In those situations, you have to log in with a certified (official) account.

7. In practice, do public authorities effectively recognise the use of signing tools *(e.g. Adobe Sign, DocuSign)* when interacting with them?

The public authorities do recognize electronical signatures (such as DocuSign), however they do not use them in their own electronic systems.

2. Electronic Identification

1. What means can be used to prove an individual´s identity electronically in your jurisdiction? Do electronic ID cards work *(e.g. in the form of mobile app)*?

In the Netherlands, there are various means by which individuals can electronically verify their identity, particularly in digital interactions with governmental institutions and private organizations.

The primary methods include:

1. DigiD: this is the most widely used system for electronic identification in the Netherlands. With DigiD, citizens can authenticate themselves online with government bodies, healthcare institutions, pension funds, and other organizations connected to the system.

2. eHerkenning: this is a digital identification system designed for businesses and organizations. It is similar to DigiD but is aimed at corporate users who need to log in to government services or other businesses.

3. iDIN: this is a digital identification service developed by Dutch banks. It allows users to verify their identity for online services using their bank credentials, similar to internet banking. iDIN is widely used for identification with non-governmental services such as online stores and insurers, but it also has applications within the public sector.

4. Dutch Passport or Identity Card with NFC Chip: since 2021, the Dutch identity card includes an NFC chip that allows users to verify their identity digitally, for example, when applying for official documents. The NFC function can be used in combination with the DigiD app and a smartphone to verify one's identity remotely.

5. European eIDASRegulation: this regulation allows citizens to identify themselves electronically in other EU member states. Various national electronic identification systems, such as DigiD, can be recognized in other EU countries under eIDAS. In the Netherlands, it is possible to log in to various institutions, especially those government-related, using an 'eIDAS passport'.

Are mobile apps used as electronic identity cards?

Mobile apps such as the DigiD app and iDIN (as verification in banking apps) are already widely used in the Netherlands as electronic identity verification methods. These apps are generally accepted for both government and private services, provided they meet the appropriate security standards.

2. Are there any means of electronic identification of legal entities in your jurisdiction?

Yes, there are several means of electronic identification of legal entities in the Netherlands. These are mainly intended to enable companies, foundations, associations and other legal entities to do business securely with the government and other organisations.

The most commonly used form is eHerkeninng. Other examples of means that can be used include iDIN for Legal Entities, PKIoverheid certificates, SBR (Standard Business Reporting) and eIDAS identification.

3. Are there any electronic identification means provided by private entities in your jurisdiction *(e.g. Bank ID)?* Do they provide sufficient proof of identity when interacting with all public authorities or are there any limitations?

Yes, there are electronic identifiers offered by private entities in the Dutch jurisdiction, such as iDIN and eHerkenning. These private identifiers are playing an increasingly important role in the Netherlands, although there are some limitations.

iDIN: this is an electronic identification method offered by banks in the Netherlands. iDIN uses banks' login methods to identify you online with third parties, such as online shops or insurance companies. So it is mainly intended for use in the private sector.

> Use with public authorities: iDIN is accepted by the government to a limited extent. It is not possible to log in via iDIN to, for example, the Tax Office or other public services. For interaction with public authorities, DigiD is still considered the standard.

eHerkenning: eHerkenning is an identifier specially developed for business users. It allows companies and entrepreneurs to do business digitally with governments and businesses. It is basically a kind of business DigiD and is provided by a number of commercial providers. - Use with public authorities: eHerkenning is widely accepted by government bodies. Entrepreneurs can use eHerkenning to, for example, submit tax returns to the Tax and Customs Administration or arrange matters with other government organisations. For citizens, however, eHerkenning is not relevant; they use DigiD.

DigiD: Although DigiD is a service offered by the government; it is important to note that DigiD is the most commonly used electronic identifier for citizens to log in to government organisations. DigiD is linked to various government services such as the Tax Office, the UWV, healthcare providers, and municipalities.

4. Is there only one/multiple electronic identification means offered directly by the state in your jurisdiction?

In the Netherlands, the state mainly offers DigiD as the official electronic identifier for citizens. Although other private options and systems such as eHerkenning for companies also exist, DigiD is the only mean offered directly by the government and widely recognised among public authorities.

3. Electronic Communications

1. What means of electronic communication with public authorities are used in your jurisdiction?

A wide range of electronic communication means are used in the Netherlands to facilitate interaction between citizens, businesses and public authorities. Important digital platforms used by the government include: MijnOverheid, MijnBelastingdienst, MijnUWV, MijnSVB, and MijnDuo. Besides these Internet platforms, the government also uses other digital solutions such as e-mail, SMS-texts, mobile apps, and sometimes even chat services.

2. Are there any state-guaranteed means of electronic communication that can be used to communicate with the public authorities? If so, can individuals and legal entities also communicate with each other through this/these means?

By state guaranteed means we mean electronic communications means that come from and are operated by the state/state institutions themselves.

In the Netherlands, there are state-guaranteed means of electronic communication for secure communication with the government, such as MijnOverheid's'berichtenbox' (= 'message inbox'), MijnBelastingdienst, MijnDUO, and other government portals.

These portals can be logged into via DigiD and eHerkenning (for business users). However, these tools are specifically intended for communication between citizens, businesses and the government. They cannot be used for direct communication between citizens and businesses without government intervention.

To ensure the security of electronic communications, we have PKIoverheid (Public Key Infrastructure Overheid) in the Netherlands. This is a digital infrastructure set up by the Dutch government to enable secure and reliable communication over the internet. It provides a system for issuing, managing and verifying digital certificates, enabling public authorities, businesses and citizens to communicate securely with each other.

3. In your jurisdiction, is the use of data boxes in communication with courts and public authorities common? If so, are there any exceptions when a data box cannot be used?

**** Data box is an electronic documents delivery system that enables individuals and legal entities to send/receive electronic documents to/from public authorities free of charge. It works similarly to an email box, except that the identity of the owner of the data box is officially verified. Individuals and legal entities can also communicate electronically with each other using the data box, but for a fee.***

Electronic communication with public authorities and courts is mainly done through systems such as MijnOverheid, MijnBelastingdienst and MijnRechtspraak/Zivver.

In some cases, it is also possible through these platforms to upload certain documents in secure ways. For example, tax returns can be filed through MijnBelastingdienst and certain

documents can be uploaded for this purpose. DigiD, and for companies eHerkenning, are the login methods onthese platforms. These systems allow individuals and companies to communicate securely with the government and judicial authorities, officially verifying the user's identity.

For communication with courts, Mijn Rechtspraak is used, where litigants, lawyers and businesses can follow their case and submit/inspect documents regarding their case. E-mail communications take place through a secured e-mail called Zivver.

4. Are there any specific formalities that must be met when communicating with public authorities *(e.g. document format, signatures, attachments etc.)*?

Yes, specific formalities apply in the Netherlands when communicating with public authorities, especially when it comes to legal or official documents.

Important requirements when communicating with the government are:

Document format: many public authorities accept electronic documents in standard formats such as PDF. This format is often required because it ensures an immutable and uniform representation of documents. Also often applies a maximum number of MB's.

Electronic Signature/Identification:

- Ordinary electronic signature: This can be a simple typed name or a scanned signature. For many non-essentials, this is sufficient.

- Advanced or qualified electronic signature: For important or legal documents, an advanced or qualified electronic signature is often required. These signatures meet strict legal requirements and are verified via DigiD or eHerkenning, for example.

Submission on 'secure channels': many public authorities and courts require documents to be submitted through secure and official digital channels, such as MijnOverheid (for communication with government bodies) and Mijn Rechtspraak (for legal proceedings).

Original documents/legalisation: in some cases, for example when submitting official documents such as diplomas or deeds, legalised copies of original documents may be required. This is especially common when communicating internationally or submitting foreign documents.

5. Are there any legal fictions/presumptions associated with electronic service of documents in your jurisdiction *(e.g. service by fiction)*?

In the Netherlands, the principle applies that an electronically sent document is deemed to have been received by the addressee at the moment the document is made accessible to him. This is evident, for example, with regard to the electronic conclusion of contracts, from Art. 6:227c (3) BW.

In the context of civil procedural law, electronic service is permitted, provided the rules of that court show that it is possible. Article 33 'Wetboek van BurgerlijkeRechtsvordering' (Rv)

contains rules on electronic filing and service of documents. The ‘Besluit elektronisch procederen’ provides specific rules on electronic procedure in civil and administrative law.

6. In your jurisdiction, is it possible to communicate electronically with all public authorities? If not, which ones cannot?

In the Netherlands, it is possible to communicate electronically with many public authorities, but it is not yet mandatory or fully possible for all government bodies. The digitisation of government services has been strongly stimulated by legislation such as the ‘Wet modernisering elektronisch bestuurlijk verkeer’ (which has not yet fully entered into force) and the ‘Wet digitale overheid’. Much of this national legislation is the result of European Union legislation.

In the Netherlands, a citizen or company has in principle the right to communicate electronically with the government, provided the authority makes this technically possible. The government must ensure this, but is not yet fully obliged to accept electronic communication in all cases. The ‘Wet modernisering elektronischbestuurlijk verkeer’ stipulates that public authorities must accept communication electronically, unless this is not reasonably possible. The biggest part of this act will come into force 1 January 2026. Especially in criminal and some civil proceedings, with some small public authorities and in specific emergency situations, electronic communication is not yet always possible or mandatory.

7. Is there an obligation to communicate with some public authorities/on certain matters only electronically?

In the Netherlands, electronic communication is mandatory for certain public authorities, especially on certain matters for companies and professional parties. Some common examples are:

Tax authorities: Companies must submit tax returns (VAT, payroll taxes, corporate income tax) digitally.

Judiciary: Lawyers have to litigate electronically in some civil and administrative law cases via ‘Mijn Rechtspraak’.

UWV: Employers must submit sick reports and benefit applications digitally via ‘MijnUWV’.

DUO: Students arrange study financing and loan repayments electronically via ‘MijnDUO’.

KvK: Companies have to submit registrations and changes digitally.

However, if a company requests to send documents on paper, most of the time this will still be allowed, but the option will not be mentioned (main rule is electronic). Citizens are often not required to communicate electronically, but this is encouraged.

POLAND

GWW

1. Electronic Legal Acts and Signatures

1. What are the requirements for a written legal act executed by electronic means to be valid? *(e.g. signature, identification of the person acting, capture of its content…)*

In order to be legally valid, a written legal act executed by electronic means must, as a general rule, comply with the requirements set forth in Article 78^1 of the Polish Civil Code, i.e. the act must contain a qualified electronic signature. This provision also states that any legal act that meets this requirement has the same evidentiary value as a contract with a handwritten signature. In Poland, the basic requirements for electronic signatures are based on the eIDAS regulation.

2. How does judicial practice view electronic legal acts? In practice, what evidence is required and/or accepted by the courts?

In Poland, electronic legal acts are accepted by the courts and are admissible as evidence in legal proceedings. As mentioned above, legal acts bearing a qualified electronic signature have the same evidentiary value as non-electronic acts bearing a traditional handwritten signature.

Article 245 of the Polish Code of Civil Procedure states that "a private document in written or electronic form is evidence that the person who signed it made the statement contained in the document". In addition, Article 46 of the eIDAS Regulation obliges courts to recognise electronic documents.

3. Does the national legislation differ in any respect from the EU Regulation No. 910/2014 (eIDAS)? If so, in which areas?

No, the national legislation fully implements the eIDAS Regulation, but Poland also has additional solutions.

4. Does your jurisdiction recognise other types of electronic signatures than those regulated by the Regulation eIDAS?

In addition to signatures covered by the eIDAS Regulation, Poland also has the institution of the Polish Trusted Profile ("*Profil Zaufany*") and the Polish Trusted Signature ("*Podpis Zaufany*"). These allow people to deal with official matters online by confirming their identity and signing electronic documents.

The Polish Trusted Signature is an integral part of the Polish Trusted Profile, dedicated to the electronic signing of documents. It can be used to sign almost all documents, however its use is narrower than that of the Qualified Electronic Signature, because in many situations where it is possible to sign a document electronically, Polish law requires it to be a QES.

5. Is it possible for a Notary Public (or another person/entity) to officially verify a signature that has been made by electronic means? If so, in which cases and under what conditions?

A notary can verify the legality of a document signed with such a signature, however does not technically verify electronic signatures. In Poland electronic signatures are verified by trust service providers (approved by the relevant minister), which have their own verification tools (usually appropriate software). They operate in accordance with the Act on Trust Services and Electronic Identification (*Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektornicznej*) and the eIDAS Regulation.

6. Which type of electronic signature is required when interacting with courts and public authorities? Is this practice uniform across all public bodies and authorities?

1. The Polish Trusted Signature is most often used in public administration. Article 20ae (2) of the Act on Informatisation of the Activities of Entities Performing Public Tasks (*Ustawa z dnia 17 lutego 2005 roku o informatyzacji działalności podmiotów realizujących zadania publiczne*) states that data in electronic form signed with the Polish Trusted Signature shall be equivalent in legal effect to a document bearing a handwritten signature, unless otherwise specified.

2. In court proceedings there are few possibilities (according to article 126 § 5 of the Polish Civil Procedure Code), however a qualified electronic signature is the most secure and always accepted, as it is equivalent to a handwritten signature.

7. In practice, do public authorities effectively recognise the use of signing tools *(e.g. Adobe Sign, DocuSign)* when interacting with them?

In general, public authorities do not accept such signatures, but in these platforms a qualified electronic signature can be linked (in this case, a document signed with QES using one of these platforms will be recognised).

2. Electronic Identification

1. What means can be used to prove an individual´s identity electronically in your jurisdiction? Do electronic ID cards work *(e.g. in the form of mobile app)*?

1. mObywatel app - official application of the Ministry of Digitalisation containing an electronic identity confirmation function (mID-*mDowód*). It's a digital identity document equivalent to a physical plastic ID card. All entities authorised to verify identity in Poland are obliged to respect the mDowód, similar to a regular ID card. The application is mainly used for the electronic version of an ID card, but it also offers the possibility of issuing electronic versions of other documents, e.g. your driving licence.

2. Polish Trusted Profile (*Profil zaufany*) - This is a free tool that allows a person to confirm his or her identity in electronic administrative systems, among other things. The Polish Trusted Profile is used exclusively for communication with the public administration (offices, ministries) and enables the handling of administrative matters online, e.g. applying for documents, registering a company, applying for state benefits, handling tax matters. Once issued, it's valid for three years (with the possibility of renewal).

3. E-ID (E-dowód) - an ID card equipped with an electronic layer (chip) that, in addition to its traditional function as an ID document, enables the use of advanced digital services. It has been issued in Poland from 2019. An integral part of the e-ID is the Personal Profile (Profil Osobisty), which allows electronic authentication of the user's identity when logging into public administration systems (e.g. ePUAP) or commercial systems.

2. Are there any means of electronic identification of legal entities in your jurisdiction?

In compliance to eIDAS - electronic seals.

3. Are there any electronic identification means provided by private entities in your jurisdiction *(e.g. Bank ID)?* Do they provide sufficient proof of identity when interacting with all public authorities or are there any limitations?

MyID (*MojeID*) is a remote identity verification service based on bank details offered by the National Clearing House (*Krajowa Izba Rozliczeniowa - KIR*). It is accepted in some public administration services and in the private sector. In situations where myID is available to confirm someone's identity, the user is redirected to the bank where, after logging in to the account, a confirmation is sent that the bank has forwarded certain information to the institution.

4. Is there only one/multiple electronic identification means offered directly by the state in your jurisdiction?

No, only the ones listed in question 2.1, i.e.:

A) E-ID (*E-dowód*) – can be used both in private and public sector
B) mObywatel App – everyday use form of identification
C) Polish Trusted Profile (*Profil Zaufany*) – official, used in contact with public authorities

3. Electronic Communications

1. What means of electronic communication with public authorities are used in your jurisdiction?

In Poland, there are a variety of platforms used for communication with public administration and courts.

When it comes to electronic communication with public authorities in Poland, the main government platform is ePUAP. The Electronic Platform of Public Administration Services (*Elektroniczna Platforma Usług Administracji Publicznej*) - ePUAP - is a system that enables citizens and businesses to deal with official matters online. However, it's important to note that there are still some situations where a particular matter cannot be dealt with electronically, such as the issuing of a passport. Moreover, its functions are now gradually being transferred to other systems, e.g. e-Delivery.

In addition, there are a number of smaller platforms designed for specific types of issues, such as the Internet Patient Account (*Internetowe Konto Pacjenta*), which provides information on past, current or planned treatment, electronic prescriptions or vaccines received.

Electronic communication with the courts is conducted through The Court Information Portal (*Portal Informacyjny Sądów Powszechnych*) that provides information on the status of cases, documents filed and actions taken. An application for an account can be filed by professional lawyers as well as by the parties themselves.

The ultimate platform for communication with the courts and public administration will be e-Delivery (*e-Doręczenia*). It is the electronic equivalent of a registered letter with confirmation of delivery. Correspondence via e-Delivery platform is legally equivalent to traditional registered mail with proof of receipt. From January 2025, some public entities and legal professionals are required to have an e-Delivery address. The process of implementing this platform will continue until 2029. In the long term, all public entities, businesses and legal professions will be obliged to have an electronic delivery address and to conduct correspondence by electronic delivery.

2. Are there any state-guaranteed means of electronic communication that can be used to communicate with the public authorities? If so, can individuals and legal entities also communicate with each other through this/these means?

By state guaranteed means we mean electronic communications means that come from and are operated by the state/state institutions themselves.

In general, all the means offered are those provided by the State. Lawyers are able to communicate with each other through e-Delivery systems as from 2025 they are obliged to have an electronic address on this platform.

3. In your jurisdiction, is the use of data boxes in communication with courts and public authorities common? If so, are there any exceptions when a data box cannot be used?

**** Data box is an electronic documents delivery system that enables individuals and legal entities to send/receive electronic documents to/from public authorities free of charge. It works similarly to an email box, except that the identity of the owner of the data box is officially verified. Individuals and legal entities can also communicate electronically with each other using the data box, but for a fee.***

This is popular and is used by many courts. There are several dedicated portals where the user has an individual data box. The most commonly used are those mentioned above - e-Delivery and The Court's Information Portal. Logging in to the e-Delivery platform is done by means of verification with a qualified signature or a Polish Trusted Profile, and in the case of the Court's Information Portal, it is necessary to provide the PESEL number and the assigned password. As mentioned above, from 2025 all legal professionals are obliged to use the e-Delivery system.

4. Are there any specific formalities that must be met when communicating with public authorities *(e.g. document format, signatures, attachments etc.)*?

It is essential that the document is delivered to the person's dedicated data box with verified identity. Other requirements vary depending on the platform, but in general, the file and attachments should be in PDF format or a dedicated form filled in by the platforms. Attachments, if they are copies of official letters, often require a qualified signature (as proof of authenticity).

5. Are there any legal fictions/presumptions associated with electronic service of documents in your jurisdiction *(e.g. service by fiction)*?

In Poland, there is a separate law on electronic delivery (*Ustawa z dnia 18 listopada 2020 r. O doręczeniach elektronicznych*), according to which, if a user's address has been entered into the electronic address database, this is considered equivalent to a request for delivery of correspondence by public entities to that address. Furthermore,

if a non-public entity has not collected the correspondence within 14 days of receipt then, on the next day, the correspondence shall be deemed to have been delivered correctly.

In civil proceedings, the provision of Article 131[1]§ 2 of the Polish Code of Civil Procedure applies, which states, similarly to the above, that in the case of electronic delivery, the letter is deemed to have been delivered at the time indicated in the electronic proof of receipt. In the absence of such proof, electronic delivery shall be deemed successful 14 days after the date on which the document was entered into the system.

6. In your jurisdiction, is it possible to communicate electronically with all public authorities? If not, which ones cannot?

No, in Poland not all public authorities allow full electronic communication. Law enforcement agencies and secret services often require a personal appearance or traditional correspondence, as well as matters concerning changes in civil status (e.g. marriage, change of surname). Some matters require a personal signature, e.g. most notarial deeds require a physical form. Most public authorities allow electronic communication, but there are still some matters that can only be dealt with in the traditional way.

7. Is there an obligation to communicate with some public authorities/on certain matters only electronically?

Yes, there are matters in which communication with certain public authorities must be conducted exclusively by electronic means, and decisions in such matters will be made only by electronic means. For example, as of 2021, the registration of a limited liability company in the court register will only be possible through a dedicated court system, and paper applications will not be accepted. Furthermore, pursuant to Article 131[1] § 1 of the Polish Code of Civil Procedure, the court shall deliver documents through an electronic communication system if the recipient has submitted a document through such a system or has chosen to submit documents in this way.

SERBIA

Vukovic & Partners

1. Electronic Legal Acts and Signatures

1. What are the requirements for a written legal act executed by electronic means to be valid? *(e.g. signature, identification of the person acting, capture of its content...)*

The qualified electronic signature in the Republic of Serbia is regulated and defined under the Law on Electronic Documents, Electronic Identification, and Trust Services in Electronic Business (Zakon o elektronskom dokumentu, elektronskoj identifikaciji i uslugama od poverenja u elektronskom poslovanju, in further text: the Law).

A qualified electronic signature comprises a set of data in electronic form that is associated with, and logically linked to, other digital data with the aim to:

1. Confirm the true identity and authenticity of the signatory,
2. Establish the validity of signed data and ensure its protection during transfer,
3. Verify the accuracy of electronic documents, and
4. Prevent denial of responsibility regarding documents that have already been signed.

For an electronic signature to be deemed qualified and valid, it must contain all legally prescribed information about the signatory. In Serbia, there are five registered certification authorities authorised to issue qualified electronic signatures: the Ministry of Internal Affairs of the Republic of Serbia, the Post of Serbia, the Chamber of Commerce of Serbia, Halcom, and E-Smart Systems.

Each certification authority has its own procedure for obtaining certificates, and while these procedures are generally similar, they are not entirely identical. Furthermore, each authority sets its own fee structure for the services provided, with the exception of the Ministry of Internal Affairs, where certificate issuance is free of charge.

An electronic signature or seal must be unambiguously associated with the signatory or sealer, meeting specific conditions:

- It must allow for the identification of the signatory or sealer.
- It should be created using signature creation data that the signatory can use under their exclusive control, with a high degree of reliability.
- It should be linked to the signed data in a way that enables the detection of any subsequent alteration.

Additionally, digitalized documents possess the same evidentiary value as original documents, provided that certain cumulative conditions are met: the digitalization is conducted under the supervision of legally authorized persons, and the equivalence between the digitalized document and the original is confirmed by a qualified electronic seal or signature by these authorized persons.

Serbia aligns with the European Union's requirements for advanced electronic signatures, ensuring the same standards for data security and verification.

2. How does judicial practice view electronic legal acts? In practice, what evidence is required and/or accepted by the courts?

Court practice regarding electronic legal instruments in Serbia is still evolving and currently lacks consistency. To ensure legal certainty, a qualified electronic signature or seal is required. At present, only the Commercial Court accepts electronically signed submissions.

In practice, some institutions, such as the Republic Geodetic Authority (Real Estate Cadastre), The Intellectual Property Office of Republic of Serbia and the Serbian Business Registers Agency (APR), more readily accept electronic documents and signatures due to advancements in digitalization. Enforcement officers also accept electronic documents.

In all cases, courts require that the identity of the signatory be clearly established, with electronic signatures and seals verified according to statutory regulations. In banking law, credit agreements and contracts related to payment services may be signed using two-factor authentication, and this practice is recognized by the courts.

3. Does the national legislation differ in any respect from the EU Regulation No. 910/2014 (eIDAS)? If so, in which areas?

In 2016, the EU introduced the eIDAS (Electronic Identification, Authentication, and Trust Services) Regulation, which established common standards for electronic signatures and electronic documents. In 2017, following the EU's example, Serbia adopted its own Law on Electronic Documents, Electronic Identification, and Trust Services in Electronic Business, aligning its regulations with EU standards on electronic transactions and digital trust.

However, the Law outlines three categories of legal transactions concerning the use of qualified electronic signatures: Transactions for which a **qualified electronic signature is prohibited:** These include legal actions involving the transfer of real property ownership or other real rights in immovable property, inheritance and family law agreements, marital property agreements, and agreements involving persons who lack legal capacity.

Transactions for which a **qualified electronic signature is optional:** For instance, in eGovernment services, such as filing tax returns, applying for e-permits in construction, accessing electronic registers, handling legal procedures with the Customs Administration, and submitting reports for securities issuers, a qualified electronic signature is convenient but not mandatory.

Transactions for which a **qualified electronic signature is mandatory**: Financial statements, mandatory since 2015, must be electronically submitted to the Business Registers Agency (APR) using a qualified electronic signature from a company's legal representative. Similarly, for registering a company's beneficial owner or submitting specific tax applications for business entities through the e-Taxes portal, a qualified electronic certificate is required.

It can be concluded from this that the main difference would be that the Law is still not aligned with the EU Directive, as it is stated in Article 25(2) of eIDAS that "a qualified electronic signature shall have the equivalent legal effect of a handwritten signature", which should mean

that it can be used in all circumstances, thus facilitating broader recognition and application of electronic signatures in legal transactions.

Furthermore, Serbia's national legislation varies from eIDAS in two more aspects:

Recognition of foreign electronic signatures: Serbia currently does not accept qualified electronic signatures issued in other countries, which may pose barriers to cross-border transactions. Under Article 40 of the Law, qualified trust services from foreign countries may be recognized in Serbia only if reciprocity is established through a ratified international agreement. Consequently, qualified certificates from countries with which Serbia does not have reciprocity agreements are not valid in Serbia.

Use of physical documents: Physical documents continue to be widely accepted, reflecting the ongoing digitalization process.

4. Does your jurisdiction recognise other types of electronic signatures than those regulated by the Regulation eIDAS?

No.

5. Is it possible for a Notary Public (or another person/entity) to officially verify a signature that has been made by electronic means? If so, in which cases and under what conditions?

In theory, notaries in Serbia are permitted to certify electronic signatures; however, this is not yet practiced. According to Article 29 of the Rulebook on Notarial Practices, a notarized document created in electronic form is considered valid if both the notary and the parties possess registered and deposited electronic signatures in compliance with the law.

Additionally, the document must fulfil other legal requirements and be composed in an electronic format specified by the relevant ministry through a special act. Practically, though, notaries can only sign documents electronically themselves, but they are currently unable to certify third-party electronic signatures. Copies, however, should theoretically be capable of being certified under this framework, but full implementation of these provisions is limited.

6. Which type of electronic signature is required when interacting with courts and public authorities? Is this practice uniform across all public bodies and authorities?

When interacting with courts and public authorities in Serbia, a qualified electronic signature is required to ensure that all legal acts and documents are valid and possess legal force.

7. In practice, do public authorities effectively recognise the use of signing tools *(e.g. Adobe Sign, DocuSign)* when interacting with them?

In Serbia, Adobe Sign is widely used for electronic signatures. These tools are increasingly accepted across various sectors, but it is advisable to verify specific requirements or limitations with the relevant institution beforehand.

As of March 2022, the Business Registers Agency has facilitated the use of electronic signatures in the cloud, allowing signatories to sign documents electronically without being tied to additional devices. To utilize this service, users only need to download the ConsentID mobile application. The qualified electronic certificate in the cloud is issued free of charge by the Office for IT and e-Government.

If you are using software like DocuSign with ID verification, Adobe Sign with authentication, or similar applications, it is important to note that they are classified as advanced electronic signatures. These solutions meet the necessary characteristics for ensuring the validity.

2. Electronic Identification

1. What means can be used to prove an individual´s identity electronically in your jurisdiction? Do electronic ID cards work *(e.g. in the form of mobile app)*?

In Serbia, qualified electronic identification methods include electronic ID cards with embedded electronic certificates, such as those provided by the Ministry of Internal Affairs. Mobile applications like ConsentID, used in conjunction with the electronic ID card do exist but it is not commonly.

2. Are there any means of electronic identification of legal entities in your jurisdiction?

Yes, legal entities in Serbia can be electronically identified through qualified certificates issued by authorized certification authorities, but the information there refers to the legal representative of the legal entity.

3. Are there any electronic identification means provided by private entities in your jurisdiction *(e.g. Bank ID)?* Do they provide sufficient proof of identity when interacting with all public authorities or are there any limitations?

Private entities in Serbia offer electronic identification solutions, such as advanced electronic signatures through banking apps. However, these do not qualify as legally sufficient for all public authorities; only qualified certificates issued by registered certification bodies are universally accepted for official purposes.

4. Is there only one/multiple electronic identification means offered directly by the state in your jurisdiction?

In Serbia, the state offers multiple electronic identification options, primarily through the Ministry of Internal Affairs and other public entities. These options include eID cards and cloud-based solutions provided by the Office for IT and e-Government. Both private and legal entities are able access this type of electronic identification. There is a growing effort to digitalize administrative procedures involving government authorities.

3. Electronic Communications

1. What means of electronic communication with public authorities are used in your jurisdiction?

In Serbia, public authorities primarily use the eGovernment Portal (*eUprava*), which facilitates electronic submission of documents, applications, and communication with government bodies.

Other means include email communication with verified electronic signatures, document submission through the Business Registers Agency (APR) portal, and direct online submissions to agencies like the Real Estate Cadastre.

2. Are there any state-guaranteed means of electronic communication that can be used to communicate with the public authorities? If so, can individuals and legal entities also communicate with each other through this/these means?

By state guaranteed means we mean electronic communications means that come from and are operated by the state/state institutions themselves.

Yes, Serbia provides state-guaranteed electronic communication through the eGovernment Portal, which allows individuals and legal entities to communicate with state institutions. However, direct communication between private parties (such as individuals or companies) is generally handled outside this system, typically through private platforms and digital signature tools certified by the Serbian government for official validity.

3. In your jurisdiction, is the use of data boxes in communication with courts and public authorities common? If so, are there any exceptions when a data box cannot be used?

**** Data box is an electronic documents delivery system that enables individuals and legal entities to send/receive electronic documents to/from public authorities free of charge. It works similarly to an email box, except that the identity of the owner of the data box is officially verified. Individuals and legal entities can also communicate electronically with each other using the data box, but for a fee.***

The use of "data boxes" as seen in some jurisdictions is not a standard practice in Serbia. Instead, secure electronic document submissions are managed through the eGovernment Portal or specific online submission platforms, such as the APR portal for business

registrations. Currently, only certain courts, like the Commercial Court in Belgrade, accept electronically signed documents.

4. Are there any specific formalities that must be met when communicating with public authorities *(e.g. document format, signatures, attachments etc.)*?

Yes, communication with Serbian public authorities electronically requires that documents follow specific formats, commonly PDF or XML, and may need to be accompanied by a qualified electronic signature.

For filings like business registration and tax declarations, verification of identity may be required via ConsentID or another qualified electronic identification method.

5. Are there any legal fictions/presumptions associated with electronic service of documents in your jurisdiction *(e.g. service by fiction)*?

It can happen in practice, but as everything connected to electronic documents is still in transition, there is not a general answer.

6. In your jurisdiction, is it possible to communicate electronically with all public authorities? If not, which ones cannot?

Even within a single institution, it happens that some tasks can be performed electronically while others cannot. There is no limited list of what can or cannot be done electronically.

7. Is there an obligation to communicate with some public authorities/on certain matters only electronically?

Yes, certain submissions, such as filing financial statements with the Business Registers Agency (APR) and submitting specific tax declarations, must be done electronically with a qualified electronic signature. This requirement is part of Serbia's digitalization efforts to align with EU eIDAS standards and improve administrative efficiency.

SLOVAKIA

alianciaadvokátov ak, s.r.o.

1. Electronic Legal Acts and Signatures

1. What are the requirements for a written legal act executed by electronic means to be valid? *(e.g. signature, identification of the person acting, capture of its content...)*

For the electronic execution of legal acts which require a written form and handwritten signature, a qualified electronic signature may be used to replace the written form of a handwritten signature. There is required a qualified certificate in ID Card issued to the person at the Police department – Document Issuing Department.

2. How does judicial practice view electronic legal acts? In practice, what evidence is required and/or accepted by the courts?

A scan is sufficient for most documents, even if notarised, but a power of attorney must be in the form of guaranteed conversion except for submissions to the commercial register (there is no need to provide guaranteed conversion). Guaranteed conversion of writs of execution is also required.

3. Does the national legislation differ in any respect from the EU Regulation No. 910/2014 (eIDAS)? If so, in which areas?

The Slovak jurisdiction accept only "qualified electronic signature", while eIDAS recognizes three types of electronic signatures. This means that if an electronic document is signed only with a qualified electronic signature, it has the same legal effects as if a written document is signed with a handwritten signature.

4. Does your jurisdiction recognise other types of electronic signatures than those regulated by the Regulation eIDAS?

No.

5. Is it possible for a Notary Public (or another person/entity) to officially verify a signature that has been made by electronic means? If so, in which cases and under what conditions?

No, it is not possible in Slovak jurisdiction.

6. Which type of electronic signature is required when interacting with courts and public authorities? Is this practice uniform across all public bodies and authorities?

There is required „qualified electronic signature". This practice is uniform across all public bodies and authorities.

7. In practice, do public authorities effectively recognise the use of signing tools *(e.g. Adobe Sign, DocuSign)* when interacting with them?

No, public authorities do not recognise Adobe Sign, DocuSign. Public authorities recognise only qualified electronic signature.

The most used signing tool for qualified electronic signature is DSigner. Client applications for qualified electronic signature (D.Signer/XAdES, D.Viewer, D.Signer Tools) are available for MSWindows (.NET and Java), GNU/Linux (Java only) and Mac OS (Java only) operating systems.

2. Electronic Identification

1. What means can be used to prove an individual´s identity electronically in your jurisdiction? Do electronic ID cards work *(e.g. in the form of mobile app)*?

To prove an individual's identity electronically, a person needs to have an ID card with chip (eID card). This identification is only possible through specific public web administration portals - slovensko.sk and eŽaloby.

2. Are there any means of electronic identification of legal entities in your jurisdiction?

Any legal entity has activated an electronic mailbox and subsequently communicate with public administration authorities electronically. The legal entity is also able to electronically sign documents as long as the person authorised to act on behalf of the company has eID card.

3. Are there any electronic identification means provided by private entities in your jurisdiction *(e.g. Bank ID)?* Do they provide sufficient proof of identity when interacting with all public authorities or are there any limitations?

No, there are no such electronic identification means provided by private entities when interacting with public authorities.

4. Is there only one/multiple electronic identification means offered directly by the state in your jurisdiction?

The only means of electronic identification offered by the state in the framework of electronic communication with the public administration is authentication by means of eID.

3. Electronic Communications

1. What means of electronic communication with public authorities are used in your jurisdiction?

Authentication by means of eID. For using of eID, each person has its own security side code (ZEP PIN and BOK code), which allows secure authentication and unambiguous identification of the person.

2. Are there any state-guaranteed means of electronic communication that can be used to communicate with the public authorities? If so, can individuals and legal entities also communicate with each other through this/these means?

By state guaranteed means we mean electronic communications means that come from and are operated by the state/state institutions themselves.

There are two state-guaranteed means of electronic communications – slovensko.sk and eŽaloby for communication.

The individuals and legal entities can communicate with each other through slovensko.sk but they need to know the number of electrical data box.

3. In your jurisdiction, is the use of data boxes in communication with courts and public authorities common? If so, are there any exceptions when a data box cannot be used?

**** Data box is an electronic documents delivery system that enables individuals and legal entities to send/receive electronic documents to/from public authorities free of charge. It works similarly to an email box, except that the identity of the owner of the data box is officially verified. Individuals and legal entities can also communicate electronically with each other using the data box, but for a fee.***

This type of communication is the most common way for attorneys and legal entities, while communicating with courts and public authorities is through the data box. The law provides for certain cases where it is necessary to serve documents physically – for example, the obligation to serve on the court the original of a promissory note for a promissory note action.

4. Are there any specific formalities that must be met when communicating with public authorities *(e.g. document format, signatures, attachments etc.)*?

In general, the only acceptable format while communicating with public authorities is PDF format, in case that documents must be signed by qualified electronical signature. Certain documents – for example power of attorney must be in “guaranteed conversion” which means they must be attached in a side format. Some evidence that does not need to be signed like pictures can be also in jpg format.

5. Are there any legal fictions/presumptions associated with electronic service of documents in your jurisdiction *(e.g. service by fiction)*?

Yes, in case a person does not accept the document from data box within the specified period of e.g. 15 days, after the expiry of the last day for acceptance the fiction of delivery occurs, whereby the document is deemed to have been delivered.

6. In your jurisdiction, is it possible to communicate electronically with all public authorities? If not, which ones cannot?

Yes, it is possible to communicate electronically with all public authorities in Slovak Republic.

7. Is there an obligation to communicate with some public authorities/on certain matters only electronically?

1. The attorneys are obliged to communicate with public authorities exclusively electronically. In case the fail to do so, the administrative fees are increased by 50%.

2. Also, there is a specific "Dunning procedure" (Upomínacie konanie) in which the claimant is obliged to communicate only electronically.

SPAIN

Adarve Abogados

1. Electronic Legal Acts and Signatures

1. What are the requirements for a written legal act executed by electronic means to be valid? *(e.g. signature, identification of the person acting, capture of its content...)*

To be legally valid, a written legal act executed by electronic means generally needs to meet the following requirements:

Authentication: The electronic signature must be:

(i) Uniquely linked to the signatory;

(ii) Capable of identifying the signatory;

(iii) Created using means under the signatory's sole control;

(iv) Linked to the signed data in a way that any subsequent changes are detectable.

Consent and Intent: The parties must agree to conduct the transaction electronically and show clear intent to sign.

Integrity of the document

Disclosure and Accessibility: The signer must be:

(i) Informed of the option to receive a non-electronic version;

(ii) Notified of the right to withdraw consent;

(iii) Made aware of any hardware/software requirements

(iv) Able to access and retain a copy of the signed document.

Record Retention: Signed electronic documents must be retained in a form that:

(i) accurately reflects the agreement;

(ii) can be reproduced as needed.

Legal Recognition: The law must recognize electronic signatures as legally valid. In the EU, this is established by the eIDAS Regulation.

2. How does judicial practice view electronic legal acts? In practice, what evidence is required and/or accepted by the courts?

Judicial practice generally views electronic legal acts and electronic signatures as valid and admissible in court. Courts across jurisdictions generally accept electronic signatures and documents as admissible evidence. The eIDAS regulation in Europe establishes that electronic signatures should not be denied legal effect solely due to their electronic nature.

To prove the validity of an electronic signature in court, the following types of evidence are typically accepted and valued:

(i) Audit trails (Timestamps of key events; IP addresses of signers; Geolocation data);

(ii) Authentication methods (Entry of personal information (e.g.last 4 digits of SSN; Use of official email addresses; Utilization of trusted eID systems);

(iii)Technical security measures;

(iv) Expert testimony.

3. Does the national legislation differ in any respect from the EU Regulation No. 910/2014 (eIDAS)? If so, in which areas?

The Spanish legislation largely follows the EU Regulation No. 910/2014; however, Spain has included national laws to regulate and complement areas that have not been contemplated by the EU Regulation, through Law 6/2020, (Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza).

Trust Services Providers: Spanish legislation provides:

(i) specific obligations for these providers;

(ii) specific control mechanism for good performance and;

(iii) penalties for infringement;

Spanish authorities:

(i) certain public authorities require a Qualified Electronic Signatures (QES) created by a specific entity (e.g. Fábrica Nacional de Moneda y Timbre) for certain proceedings;

(ii) there is the obligation to interact electronically with certain public authorities and professionals.

4. Does your jurisdiction recognise other types of electronic signatures than those regulated by the Regulation eIDAS?

Spain recognizes and accepts other types of electronic signatures beyond those specifically regulated by the eIDAS Regulation. Spain follows a tiered legal model for electronic signatures, in line with the eIDAS Regulation, which recognizes three types of electronic signatures: simple (SES), advanced (AES), and qualified (QES), but also Spanish law takes a flexible approach and does not limit valid electronic signatures only to these three types.

The Spanish Electronic Commerce Act 34/2002 establishes additional provisions regarding the enforceability of agreements executed through electronic means. According to Spanish law, generally any form of electronic signature and handwritten signatures can be used to create valid contracts that do not need additional warranties (Spanish courts have shown a pragmatic approach in accepting various forms of electronic signatures). The use of electronic signatures provided by suppliers such as DocuSign is a controversial point as its use can be validated by certain courts but rejected by others.

Article 1278 of Spanish Civil Code establishes the general principle of freedom of forms for contracts, meaning that no specific form is generally required for a contract to be valid, this principle extends to electronic signatures. Spanish jurisdiction recognizes and accepts a wide range of electronic signature types, including those not explicitly defined in the eIDAS Regulation, as long as they can demonstrate the identity and the integrity of the signed document. However, for certain specific transactions, especially those involving government entities or highly regulated industries, more stringent forms of electronic signatures (like QES) may be required.

5. Is it possible for a Notary Public (or another person/entity) to officially verify a signature that has been made by electronic means? If so, in which cases and under what conditions?

Notaries and other public entities can verify electronic signatures; however, we have to consider a few key points: - QES are automatically considered to be legally valid.

Advanced Electronic Signatures (AES) and Simple Electronic Signatures (SES) do not provide the same level of validity, however, they can still be verified. The verification of electronic signatures is precise in the following situations:

(i) high – value transactions;

(ii) legal procedures where this point has to be proven and

(iii) specific regulatory transactions.

Notaries can validate QES signatures:

(i) through presentation of a valid national identification document

(ii) validate the signature in person;

(iii) the validation of electronic signatures by a notary must meet certain conditions.

SES and AES signatures cannot be validated by a notary public. Article 261 of the Notary Act (Decreto de 2 de junio de 1944 por el que se aprueba con carácter definitivo el Reglamento dela organización y régimen del Notariado) only establishes the rules and conditions to be met for AES and QES, therefore SES are left out of this scope.

6. Which type of electronic signature is required when interacting with courts and public authorities? Is this practice uniform across all public bodies and authorities?

The type of electronic signature required when interacting with courts and public authorities is generally an advanced or qualified electronic signature. The requirements for interacting with courts and public authorities are as follows:

Courts:

(i) advanced electronic signatures are typically accepted and given substantial legal value;

(ii) signatures based on recognized certificates and created by secure signature creation devices are considered equivalent to handwritten signatures;

(iii) even if an electronic signature doesn't meet all specified requirements, it is not automatically denied legal effects or excluded as evidence in court. However, it may be subject to different treatment based on the tribunal's criteria.

Public Authorities:

They are required to accept qualified or advanced electronic signatures as defined in the eIDAS Regulation. Each administration may provide specific electronic signature systems to its personnel, identifying both the individual and the administration or body they serve. The Law on Common Administrative Procedure (LPAC) and the Ley 40/2015, de 1de octubre, de Régimen Jurídico del Sector Público outlines the use of electronic signatures in administrative acts.

7. In practice, do public authorities effectively recognise the use of signing tools *(e.g. Adobe Sign, DocuSign)* when interacting with them?

Spanish public authorities have a mixed approach to recognizing signing tools like Adobe Sign or DocuSign when interacting with them but Spanish public authorities generally prefer and promote the use of their own electronic signature systems or those specifically recognized by

Spanish law like (i) CERES (Spanish Certification) system offered by the Spanish Royal Mint (FNMT) is widely used and recognized and (ii) Cl@ve system, which is a centralized identification, authentication, and electronic signature service shared by the whole State Public Administration Sector.

Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas outlines specific systems for identification and signature permitted by Public Administrations. These often require advanced or qualified electronic signatures, certificates issued by recognized certification service providers and signatures created using secure signature creation devices. Some public sector entities require qualified electronic signatures created using digital certificates issued by specific trust service providers, such as the Fábrica Nacional de Moneda y Timbre (FNMT).

Spanish public authorities are increasingly adopting and recognizing electronic signatures, they tend to favour officially recognized systems and certificates. Commercial signing tools may not be widely accepted for official interactions with public authorities, especially for formal procedures or high-security transactions. For individuals or businesses interacting with Spanish public authorities, it's advisable to use the officially recognized systems (like Cl@ve or CERES) or to inquire with the specific authority about accepted signature methods, rather than assuming that widely used commercial tools will be recognized.

2. Electronic Identification

1. What means can be used to prove an individual´s identity electronically in your jurisdiction? Do electronic ID cards work *(e.g. in the form of mobile app)*?

There are a few ways for people to identify themselves through electronic means:

Electronic ID Cards which would be an equivalent to the traditional ID Card, however, this electronic validation is still in process of implementation (once it´s fully functional it would operate through a mobile app)

Cl@ve System: it is an electronic generated password that allows people to carry out administrative and/or legal proceedings. It offers permanent and temporary passwords sent via SMS and mobile app

Digital Certificates: (i) FNMT Certificate (issued by la Fábrica Nacional de Moneda y Timbre) and idCat which is a digital certificate issued by Catalonian authorities.

2. Are there any means of electronic identification of legal entities in your jurisdiction?

Under Spanish law, legal entities can use digital certificates that serve as electronic IDs to identify these entities in their interaction with administrative and public authorities. These certificates are the FNMT Certificate and the idCat Certificate.

Legal entities are required to use electronic means to communicate with Spanish public authorities through a QES for

(a) accessing certain areas of the Spanish Administration and

(b) signing and submitting documents that need to be filed with public authorities as well as interacting with public authorities.

Since Spain has adhered to the EU Regulation No. 910/2014 there is cross border identification for legal entities.

3. Are there any electronic identification means provided by private entities in your jurisdiction *(e.g. Bank ID)?* Do they provide sufficient proof of identity when interacting with all public authorities or are there any limitations?

There are some electronic identification means provided by private entities in Spain, but their use and acceptance by public authorities appears to be limited:

Bank ID systems: While some Spanish banks offer digital identification services to their customers, there is no widespread "Bank ID" system in Spain that is universally accepted by public authorities.

Private certification authorities: Some private companies are authorized to issue digital certificates in Spain

(i) Camerfirma: Issues digital certificates for individuals and businesses and

(ii) ANF Autoridad de Certificación: Provides various types of digital certificates.

Preference for official systems: Spanish public authorities generally prefer and promote the use of government-issued electronic identification systems, such as:

(i) DNI electrónico (electronic National Identity Card);

(ii) Cl@ve system (a centralized identification and signature platform for public administration) and

(iii) Certificates issued by the FNMT (Spanish Royal Mint).

There are some private electronic identifications available in Spain but they do not generally provide sufficient proof of identity for comprehensive interactions with all public authorities. The Spanish system heavily relies on government-issued and controlled electronic identification methods for official purposes. Private solutions may be used in specific contexts or for certain transactions, but they are not universally accepted alternatives to official electronic IDs when dealing with public authorities.

4. Is there only one/multiple electronic identification means offered directly by the state in your jurisdiction?

Electronic means that legal entities and natural persons can use to identify themselves are directly controlled by the State. These are:

(i) Electronic ID Card

(ii) Cl@ve System which offers three options (Clave Pin, Clave Permanente y Clave Firma)

(iii) Digital Certificates.

3. Electronic Communications

1. What means of electronic communication with public authorities are used in your jurisdiction?

The Spanish jurisdiction establishes several electronic means for interaction between citizens, legal professionals and public authorities, which are:

LexNet: this is a system used between judicial bodies and legal professionals used for presentation of legal documents and notification of judicial resolutions.

HERMES System: this system allows interactions between the national Health System, the Police and Local Authorities.

Electronic Administrative File Loader System: allows upload of administrative documents between Public Administration and the Justice Administration.

These electronic systems for interaction are based on several national laws: Law 39/2015 that regulates the framework of electronic means for the Public Administration and Law 11/2022(Ley 11/2022,de 28 de junio, General de Telecomunicaciones) which is a law that complements and completes the already established electronic systems.

2. Are there any state-guaranteed means of electronic communication that can be used to communicate with the public authorities? If so, can individuals and legal entities also communicate with each other through this/these means?

By state guaranteed means we mean electronic communications means that come from and are operated by the state/state institutions themselves.

Yes, the Spanish law has established state – guaranteed means for legal entities and citizens to interact with public authorities. Spanish legislation recognizes citizens right to interact with public authorities through electronic means and for this purpose the Spanish ministry has established the Electronic Judicial Office that regulates and facilitates these communications.

On the other hand, communications between legal entities and entities without legal personality is made through the Electronic Address – this means that these entities are required to communicate electronically, in any case. Law 11/2022 has established a few methods for communication between private parties - Robinson List, which is a registry where natural persons can designate their desire and/or lack hereof to receive commercial advertisement.

3. In your jurisdiction, is the use of data boxes in communication with courts and public authorities common? If so, are there any exceptions when a data box cannot be used?

**** Data box is an electronic documents delivery system that enables individuals and legal entities to send/receive electronic documents to/from public authorities free of charge. It works similarly to an email box, except that the identity of the owner of the data box is officially verified. Individuals and legal entities can also communicate electronically with each other using the data box, but for a fee.***

There is no specific mention of "data boxes" as they are used in some other European countries (Czech Republic). However, Spain does have electronic systems for communication with courts and public authorities.

Electronic communication systems:

(i) LexNET: This is the primary electronic system used for communication with courts in Spain and

(ii) Electronic Courthouses (Sedes Judiciales Electrónicas).

Mandatory use of electronic systems: According to Article 273 of the Code of Civil Procedure, all justice-sector professionals must use remote or electronic systems to submit documents to courts. The Law on Civil Procedure was amended in 2015 to make it mandatory, from January 1, 2016, for all professionals working in the justice sector to use secure electronic systems for serving documents related to proceedings.

Spain doesn't use the term "data boxes," it does have mandatory electronic communication systems for most interactions with courts and public authorities. However, there are some exceptions, particularly for initial summons to legal persons and for natural persons not required by law to use electronic means.

4. Are there any specific formalities that must be met when communicating with public authorities *(e.g. document format, signatures, attachments etc.)*?

There are indeed specific formalities that must be met when communicating with public authorities in Spain:

Electronic communication requirement: According to the Administrative Proceeding Act, certain entities and professionals are required to use electronic means and a Qualified Electronic Signature (QES) when conducting administrative procedures or formalities with Spanish public authorities or government entities.

Mandatory electronic communication for: Legal entities; Entities without legal personality; Those exercising a professional activity requiring mandatory membership in a professional association; Public sector employees for procedures and actions carried out with Public Administrations by reason of their status as public employees.

Electronic signatures. Qualified Electronic Signatures (QES) are often required for official communications with public authorities. and for certain administrative procedures, the use of QES is mandatory.

Specific platforms: LexNET platform is used for submitting documents related to legal proceedings and Electronic Courthouses (Sedes Judiciales Electrónicas) are used for notification procedures.

Document format: While not explicitly mentioned in the search results, it's common for public authorities to specify acceptable document formats (e.g., PDF) for electronic submissions.

Notifications: Public authorities are increasingly using electronic means for notifications. Entities required to communicate electronically are also obliged to receive notifications electronically.

5. Are there any legal fictions/presumptions associated with electronic service of documents in your jurisdiction *(e.g. service by fiction)*?

There are some legal fictions and presumptions associated with electronic service in Spain:

Presumption of receipt: When documents are served electronically, there is generally a presumption that the documents have been received by the addressee once they are made available in the designated electronic system or platform.

Date of service: According to the amended Rules 126(2) and 127(2) of the European Patent Convention, electronic service is deemed to have taken place on the date shown on the document. This new fiction of service replaces the previous "10day rule".

Lawful service: Documents are deemed lawfully served where the record of service contains adequate evidence that the documents were delivered to the person concerned at their authorized email address, via an electronic notifications' portal, or by any remote or electronic means chosen by the addressee.

Consent for electronic service: There is a presumption that certain entities and professionals' consent to receive notifications electronically, as they are obliged by law to interact electronically with public administrations.

Time of availability: For electronic notifications, there's often a presumption that the notification is available to the addressee from the moment it is deposited in the designated electronic mailbox or platform, regardless of when the addressee accesses it.

Rejection of notification: If an addressee does not access an electronic notification within a specified period (often 10 days), it may be presumed rejected, with legal consequences like those of an actual rejection of notification.

Integrity and authenticity: There's a presumption of integrity and authenticity for documents served electronically through official systems, unless proven otherwise.

Identification of sender: When public administrations use their designated electronic signature systems, there's a presumption that both the individual and the administration or body they serve are properly identified.

6. In your jurisdiction, is it possible to communicate electronically with all public authorities? If not, which ones cannot?

Under Spanish jurisdiction, the public authorities that allow electronic communications are the General Public Administration, Tax Agency, Social Security Administration, State and municipal Organizations and Comunidades Autonomas (Regional Authorities).

However, there are limitation in the communication with electronic means within certain public bodies such as small-town halls (that do not have advanced electronic means), Judicial System as there are some legal proceedings that require filing documents physically.

7. Is there an obligation to communicate with some public authorities/on certain matters only electronically?

Under Spanish jurisdiction, Law 39/2015 requires electronic communication with public authorities for the following persons:

- Legal entities;
- Entities with no legal personality;
- Legal professionals within their legal activity;
- Professional representatives of legal entities and/or natural persons that are bound to communicate electronically.
- Public employees within their communications with public authorities.

These persons must communicate electronically with the Spanish Tax Agency, Spanish Security Administration and Ministry of Justice.

SWEDEN

Wesslau Söderqvist

1. Electronic Legal Acts and Signatures

1. What are the requirements for a written legal act executed by electronic means to be valid? *(e.g. signature, identification of the person acting, capture of its content...)*

A written legal act executed by electronic means is valid if it is signed by electronic signature. The signature can be made by different standards, which is considered to have different strength if, for example, a court is to evaluate the evidence of the signed deed. For example, if the electronic signature can be uniquely linked to the person signing, it holds a higher evidential value.

2. How does judicial practice view electronic legal acts? In practice, what evidence is required and/or accepted by the courts?

The courts do accept electronic legal acts, and they have their own system for electornic signing of court documents. In many cases it is required to show that the document has been signed by an advanced signature or a qualified signature.

3. Does the national legislation differ in any respect from the EU Regulation No. 910/2014 (eIDAS)? If so, in which areas?

The national legislation is in line with eIDAS.

4. Does your jurisdiction recognise other types of electronic signatures than those regulated by the Regulation eIDAS?

No.

5. Is it possible for a Notary Public (or another person/entity) to officially verify a signature that has been made by electronic means? If so, in which cases and under what conditions?

N/A

6. Which type of electronic signature is required when interacting with courts and public authorities? Is this practice uniform across all public bodies and authorities?

It is different practice between different public bodies, the courts often require qualified signatures.

7. In practice, do public authorities effectively recognise the use of signing tools *(e.g. Adobe Sign, DocuSign)* when interacting with them?

In some cases yes, but not always

2. Electronic Identification

1. What means can be used to prove an individual´s identity electronically in your jurisdiction? Do electronic ID cards work *(e.g. in the form of mobile app)*?

Bank ID, Freya ID, mobile apps to prove identity.

2. Are there any means of electronic identification of legal entities in your jurisdiction?

No, legal entities cannot be identified electronically, but the companies' representatives can identify themselves electronically.

3. Are there any electronic identification means provided by private entities in your jurisdiction *(e.g. Bank ID)?* Do they provide sufficient proof of identity when interacting with all public authorities or are there any limitations?

Yes, Bank ID.

4. Is there only one/multiple electronic identification means offered directly by the state in your jurisdiction?

Both Bank ID and Freya are approved by the state, but they are not offered by the state.

3. Electronic Communications

1. What means of electronic communication with public authorities are used in your jurisdiction?

More or less all communication is electronic.

2. Are there any state-guaranteed means of electronic communication that can be used to communicate with the public authorities? If so, can individuals and legal entities also communicate with each other through this/these means?

By state guaranteed means we mean electronic communications means that come from and are operated by the state/state institutions themselves.

Many public bodies have online services that can be used in the communication with the public bodies. Individuals cannot communicate with each other.

3. In your jurisdiction, is the use of data boxes in communication with courts and public authorities common? If so, are there any exceptions when a data box cannot be used?

**** Data box is an electronic documents delivery system that enables individuals and legal entities to send/receive electronic documents to/from public authorities free of charge. It works similarly to an email box, except that the identity of the owner of the data box is officially verified. Individuals and legal entities can also communicate electronically with each other using the data box, but for a fee.***

Data boxes are used in some cases, but not for communications between individuals/legal entities.

4. Are there any specific formalities that must be met when communicating with public authorities *(e.g. document format, signatures, attachments etc.)*?

No.

5. Are there any legal fictions/presumptions associated with electronic service of documents in your jurisdiction *(e.g. service by fiction)*?

N/A

6. In your jurisdiction, is it possible to communicate electronically with <u>all</u> public authorities? If not, which ones cannot?

Yes.

7. Is there an obligation to communicate with some public authorities/on certain matters only electronically?

No.

SWITZERLAND

Meyerlustenberger Lachenal Ltd. (MLL)

1. Electronic Legal Acts and Signatures

1. What are the requirements for a written legal act executed by electronic means to be valid? *(e.g. signature, identification of the person acting, capture of its content...)*

Valid qualified electronic signature, be registered on one of the messaging platforms recognised by the authorities, be equipped with the software needed to draw up and sign documents in PDF format.

2. How does judicial practice view electronic legal acts? In practice, what evidence is required and/or accepted by the courts?

Receipt of deposit serving as proof of compliance with the time limit.

3. Does the national legislation differ in any respect from the EU Regulation No. 910/2014 (eIDAS)? If so, in which areas?

No application of European law in Switzerland.

4. Does your jurisdiction recognise other types of electronic signatures than those regulated by the Regulation eIDAS?

To date, no agreement on the mutual recognition of electronic signatures has been concluded between Switzerland and a third country (or the European Union).

In the absence of such an agreement, a qualified electronic signature based on a certificate qualified under foreign law is not recognised as equivalent to a qualified electronic signature under Swiss law. A qualified electronic signature in Switzerland is not recognised as equivalent to a qualified electronic signature abroad.

5. Is it possible for a Notary Public (or another person/entity) to officially verify a signature that has been made by electronic means? If so, in which cases and under what conditions?

As far as we know, no.

6. Which type of electronic signature is required when interacting with courts and public authorities? Is this practice uniform across all public bodies and authorities?

A signature from the list of certification service providers recognised by the Confederation.

7. In practice, do public authorities effectively recognise the use of signing tools *(e.g. Adobe Sign, DocuSign)* when interacting with them?

We do not know.

2. Electronic Identification

1. What means can be used to prove an individual´s identity electronically in your jurisdiction? Do electronic ID cards work *(e.g. in the form of mobile app)*?

An e-ID project is currently being developed in Switzerland.

2. Are there any means of electronic identification of legal entities in your jurisdiction?

We do not know.

3. Are there any electronic identification means provided by private entities in your jurisdiction *(e.g. Bank ID)?* Do they provide sufficient proof of identity when interacting with all public authorities or are there any limitations?

We do not know.

4. Is there only one/multiple electronic identification means offered directly by the state in your jurisdiction?

The Confederation provides a list of recognition bodies accredited by the Swiss Accreditation Service.

3. Electronic Communications

1. What means of electronic communication with public authorities are used in your jurisdiction?

E-mailing of brief and statement.

2. Are there any state-guaranteed means of electronic communication that can be used to communicate with the public authorities? If so, can individuals and legal entities also communicate with each other through this/these means?

By state guaranteed means we mean electronic communications means that come from and are operated by the state/state institutions themselves.

The Swiss Accreditation Service (SAS) publishes and maintains a list of recognised certification service providers.

3. In your jurisdiction, is the use of data boxes in communication with courts and public authorities common? If so, are there any exceptions when a data box cannot be used?

**** Data box is an electronic documents delivery system that enables individuals and legal entities to send/receive electronic documents to/from public authorities free of charge. It works similarly to an email box, except that the identity of the owner of the data box is officially verified. Individuals and legal entities can also communicate electronically with each other using the data box, but for a fee.***

No.

4. Are there any specific formalities that must be met when communicating with public authorities *(e.g. document format, signatures, attachments etc.)*?

C.f. Answer question 1.

5. Are there any legal fictions/presumptions associated with electronic service of documents in your jurisdiction *(e.g. service by fiction)*?

No.

6. In your jurisdiction, is it possible to communicate electronically with <u>all</u> public authorities? If not, which ones cannot?

No, some cantonal courts, such as those in Geneva, do not yet accept electronic communications, particularly for filing briefs.

7. Is there an obligation to communicate with some public authorities/on certain matters only electronically?

THE UNITED KINGDOM

Wedlake Bell

1. Electronic Legal Acts and Signatures

1. What are the requirements for a written legal act executed by electronic means to be valid? *(e.g. signature, identification of the person acting, capture of its content...)*

No difference with underlying law. Important to remember need for physical presence for deeds (English law has a particular regime for deeds).

2. How does judicial practice view electronic legal acts? In practice, what evidence is required and/or accepted by the courts?

No different to wet ink.

3. Does the national legislation differ in any respect from the EU Regulation No. 910/2014 (eIDAS)? If so, in which areas?

English law predates eIDAS. However, standard market practice is not to use qualified electronic signatures.

4. Does your jurisdiction recognise other types of electronic signatures than those regulated by the Regulation eIDAS?

Yes.

5. Is it possible for a Notary Public (or another person/entity) to officially verify a signature that has been made by electronic means? If so, in which cases and under what conditions?

This is not a legal requirement and would not be normal.

6. Which type of electronic signature is required when interacting with courts and public authorities? Is this practice uniform across all public bodies and authorities?

No difference to contracts between commercial parties.

7. In practice, do public authorities effectively recognise the use of signing tools *(e.g. Adobe Sign, DocuSign)* when interacting with them?

Yes.

2. Electronic Identification

1. What means can be used to prove an individual´s identity electronically in your jurisdiction? Do electronic ID cards work *(e.g. in the form of mobile app)*?

There is no formal, government-approved ID-V route, but a number of electronic tools, plus new obligations for ID-V of directors and certain beneficial owners of companies are coming into force in the coming years.

2. Are there any means of electronic identification of legal entities in your jurisdiction?

https://www.gov.uk/get-information-about-a-company . We have a free to access electronic company register in the UK.

3. Are there any electronic identification means provided by private entities in your jurisdiction *(e.g. Bank ID)?* Do they provide sufficient proof of identity when interacting with all public authorities or are there any limitations?

Not really relevant.

4. Is there only one/multiple electronic identification means offered directly by the state in your jurisdiction?

Different methods for different things (company registration/VAT number verification/ID through driving licence or passport). There is no national ID card in the UK.

3. Electronic Communications

1. What means of electronic communication with public authorities are used in your jurisdiction?

E-mail.

2. Are there any state-guaranteed means of electronic communication that can be used to communicate with the public authorities? If so, can individuals and legal entities also communicate with each other through this/these means?

By state guaranteed means we mean electronic communications means that come from and are operated by the state/state institutions themselves.

NHS (heathcare) uses secure email.

3. In your jurisdiction, is the use of data boxes in communication with courts and public authorities common? If so, are there any exceptions when a data box cannot be used?

**** Data box is an electronic documents delivery system that enables individuals and legal entities to send/receive electronic documents to/from public authorities free of charge. It works similarly to an email box, except that the identity of the owner of the data box is officially verified. Individuals and legal entities can also communicate electronically with each other using the data box, but for a fee.***

No.

4. Are there any specific formalities that must be met when communicating with public authorities *(e.g. document format, signatures, attachments etc.)*?

No.

5. Are there any legal fictions/presumptions associated with electronic service of documents in your jurisdiction *(e.g. service by fiction)*?

No.

6. In your jurisdiction, is it possible to communicate electronically with <u>all</u> public authorities? If not, which ones cannot?

Particular requirements where national security issues arise and in relation to healthcare data.

7. Is there an obligation to communicate with some public authorities/on certain matters only electronically?

No.