CEE LEGAL MATTERS COMPARATIVE LEGAL GUIDE: TMT 2022

CEE
LEGAL MATTERS

www.ceelegalmatters.com

FOREWORD

By Tamas Bereczki, Partner, Provaris

Technology has been shaping the lives of humans since the dawn of humanity. Between inventing the wheel to building steam engines centuries passed, and then the discovery of electricity took a few centuries still. It's a cliche that technological advancement has rapidly increased in the past decades and with the digital era. Our lives slowly started to expand into somewhat of a virtual extension of our physical world and in the past 10-15 years customs like sending regular mail or buying music that the older generations were used to barely exist nowadays. The way we communicate with each other also moved into the digital space. We send tweets, SMS, and instant messages rather than emails.

Digitalization brought and will bring many more benefits to human welfare and the way we deal with each other in our everyday lives. The great lockdowns from 2020 also gave a strong boost to digitalization and even "old school" brick-and-mortar shops started to move online, develop digital services and solutions, and change their business models. We used to buy things in the physical world but we now shifted to online marketplaces and shops (we can even buy cars and clothing online, no need to take long drives to crowded plazas anymore).

These changes also affect the laws that regulate how we can identify ourselves in the digital world and how can we conclude contracts that require formal attributes, like the verifiable, authentic signature of the contracting parties and securing non-repudiation of contractual statements. The way countries and jurisdictions regulate digital signatures and digital contracting can be a game changer for the digital economy, the supply chain, and international economic cooperation. Bad or lacking regulation can lead to actual economic detriments by keeping the costs of conducting business higher than in jurisdictions with more well-formulated, well-thought regulations.

As we leave paper documents behind, archiving digital assets becomes more and more important. Digital archiving is not just about archiving digital information, but also the means to (even decades) later be able to retrieve such information. This also requires the archiving of software, sometimes even – now deprecated – dedicated hardware.

This CEE Legal Matters comparative guide collects and showcases the most important regulations relative to online contracting, digital signatures, and digital archiving for the reader to get a high-level, comprehensive picture of the legal landscape of these critical aspects in the region. ■

The Editors:

■ Radu Cotarcea
radu.cotarcea@ceelm.com
■ Radu Neag
radu.neag@ceelm.com

Letters to the Editors:

If you like what you read in these pages (or even if you don't) we really do want to hear from you. Please send any comments, criticisms, questions, or ideas to us at: press@ceelm.com

TABLE OF CONTENTS

CHAPTER CONTENTS

GUIDE CO-EDITORS

CEE LEGAL MATTERS COMPARATIVE LEGAL GUIDE: TMT 2022

CROATIA

Mojmir Ostermann
Managing Partner
mojmir.ostermann@ostermann.hr
+385 1 5599800

Marta Jelakovic
Senior Associate
marta.jelakovic@ostermann.hr
+385 1 5599800

Janica Rakoci
Associate
janica.rakoci@ostermann.hr
+385 1 5599800

1. Legal framework for writing and electronic contracts

a. What are the requirements in your jurisdiction to consider a document to be in writing? Are there any formal/technical requirements?

For a document to be considered in writing under Croatian law, the parties must exchange letters or come to an agreement via other means that allow determining the content of their statements and the parties' identities. Available "other means" depend on the development of technology which continuously provides further possibilities. Therefore, nowadays a written document is not only one where statements are written on paper. For instance, the Croatian Financial Services Supervisory Agency issued an official opinion that a leasing agreement concluded electronically meets the criteria of a mandatory written form if its content and the identity of the parties can be determined with certainty.

Despite the long-established principle for determining a party's identity based on a full signature (first and last name), Croatian laws do not require an agreement to be signed (by hand or electronically) to be considered to be in writing. Along with a full signature, additional pieces of data specified in other parts of the document can also help identify parties, such as personal identification number and address.

b. Are electronic documents [e.g., an email] per se considered to be in writing under your law?

Due to technological developments and the introduction of electronic forms, Croatian law (and case law) adapted and now considers electronic documents, such as e-mails, as documents in writing. However, this specific approach requires caution due to the fact that an e-mail account can be registered without any identity check, so a manifestation of will via e-mail without a digital signature often might not be sufficient.

As a general rule, an electronic document can be considered to be in writing whenever its content is relatively permanently recorded, whereas the means by which such record has been created and the medium on which it is recorded are irrelevant, as long as they ensure that the record is relatively permanent. The content of an electronic document can therefore include all forms of written text, data, photos and graphics, maps, sound, music, and speech.

c. What probative power paper and/or electronic documents have that are to be considered in writing?

The advantage of any document in writing is that it makes proving its content much simpler, as opposed to proving orally concluded agreements. When it comes to paper documents, the burden of proof is on the party which disputes its authenticity or content. Specifically, probative power in such cases might depend on several factors (e.g., the existence and type of signatures, certification of a document by a notary public, and type of document [private or public]). For instance, if an official document was issued by a state authority, whatever is confirmed or established in that public document is presumed to be true, until proven otherwise.

The probative power of electronic documents depends on whether they contain a documentation feature. Documentation feature (as defined in the *Electronic Document Act*) is a set of data such as electronic signature, time of creation, name of the creator, and other data which are incorporated in a document in order to maintain its authenticity, integrity, and validity through time. This data enables verification of the creator's identity, the authenticity of the message, and the time of creating, sending, and modifying the content. This is achieved by using an advanced electronic signature, a qualified electronic signature, and a qualified electronic time stamp. For the purposes of this article, we will refer to electronic documents with a documentation feature as "e-documents."

Therefore, electronic documents in general have the same probative power as paper documents, but not all electronic documents have the same probative power. E-documents have greater probative power than electronic documents which do not contain documentation features. What is more, a printed copy of an e-document has the same probative power as certification of the content of the e-document by a notary public.

However, the submission of regular electronic documents and verifiable e-documents as court evidence is primarily limited by the ability of the court to accept and examine such evidence. On the other hand, in the case of regular electronic documents, the court can most likely examine their content, but it will be more difficult to prove the authenticity and origin of such documents.

d. What are the general rules and requirements to conclude a contract electronically?

Regarding the conclusion of contracts by electronic means, an electronic contract is concluded when the parties agree on the essential elements of the contract, i.e., at the moment when the offeror receives an electronic message containing the offeree's acceptance (the same principle appropriately applies to the conclusion of contracts in general). One of the general requirements to conclude a contract electronically is that the contract is electronically signed, for the purpose of verification of the contracting parties' identities.

The validity of a contract concluded in an electronic form, such as an e-mail, cannot be disputed solely on the ground that

it was drawn up in an e-mail. Nevertheless, certain requirements still need to be met when concluding a contract electronically, such as the possibility to identify the parties, verify the authenticity of the content, and stability of the content over time, which all contribute to legal certainty, as it brings assurance and clarity regarding rights and obligations in a legal relationship.

To elaborate on the example of e-mails, as already mentioned, anyone can open an e-mail account without an identity check, which can raise the issue of proving the e-mail holder's identity. However, if the contracting parties have regularly used certain e-mail addresses in their business, and especially if they have already used them in previous contracts or undertakings, then the requirement of identification will be considered met.

In compliance with the *EU e-Commerce Directive*, Croatia has restricted the right to conclude contracts electronically with regard to some types of contracts. Contracts that cannot be concluded electronically include real estate contracts (except lease), family law, and succession law contracts, as well as various contracts which require the participation of public authorities (notary public, court, etc.). Interestingly though, according to Croatian courts, guarantee contracts, which have also been excluded from the *e-Commerce Directive*, can be concluded electronically if the parties used a digital signature that confirms the authenticity and content of the document.

The possibility to conclude contracts electronically is also available in many everyday business situations, like employment contracts. The Ministry of Economy, Employment and Entrepreneurship of Croatia issued an official opinion that an employment contract that is concluded electronically and signed with a qualified electronic signature, is considered to be in writing in compliance with the *Employment Act*.

e. Are there any sector-specific rules that define further requirements to conclude contracts electronically [e.g., contracting via an authenticated electronic channel, contracting via video chat, etc.]?

Technology provides another means of communication that can be used for the conclusion of contracts – video calls. In essence, an agreement reached on a video call is an oral contract. However, if the video call is recorded, it can have the same effect as a written contract. This recording could be used as evidence of the contract itself, as well as of its terms and conditions.

While oral contracts are in general difficult to prove and enforce, recorded oral contracts, i.e., video call contracts can mitigate this problem. The recording of a video call contract could provide sufficient evidence for a court to determine whether the contract is enforceable. However, other call participants need to be previously notified that the call would be recorded, otherwise, such evidence might be dismissed by the court as illegal.

A more specific set of rules for the conclusion of contracts electronically can be found within the framework of consumer protection. For example, when selling products online, the seller has to provide a pre-contractual notification which contains a summary of the most important information regarding the seller, the product and/or service, the customers' right to file a written complaint, and the customers' right of unilateral termination of the contract. It is also obligatory to have a form for unilateral termination easily accessible to customers, and terms and conditions of sale which have to be available and transparent.

When concluding a distance contract in general (without the simultaneous physical presence of the trader and consumer in one place), the offer and its acceptance are considered to be received when the person to whom they are addressed can access them (through e-mail, applications, etc.).

2. Digital signatures

a. Are there any laws regulating the use of digital signatures in your jurisdiction?

The use of digital (electronic) signatures in Croatia is regulated directly by the *EU Regulation No 910/2014 on electronic identification and trust services for electronic transactions in the internal market* (the eIDAS Regulation), which harmonized the legal framework for digital signatures on the level of the European Union.

However, the eIDAS Regulation has been further supplemented on the national level by the Act on Implementation of the eIDAS Regulation which imposes some additional obligations for the signatory, trust services provider, and the holders of means of electronic identification.

Firstly, every signatory is obligated to take all necessary measures of protection from loss and damage which might be caused to other signatories, trust services providers, or third parties. Above all, this includes applying due diligence in the use of the means and data for creating digital signatures, as well as protection from unauthorized access or use. Specifically, the signatory should do everything in its power to ensure that the means and data are under its exclusive supervision in order to prevent theft, loss, or unauthorized use. In case of loss of or damage to the means and data, the signatory has to notify the trust services provider and request revocation of the certificate.

Additionally, each signatory should notify the trust services

provider of any and all changes which might affect the accuracy of the digital signature and deliver all relevant information within seven days of any such change.

Signatories will be liable for damage if they fail to comply with these obligations. Exceptionally, if the injured party did not take the necessary measures to validate the digital signature, then the signatory's liability can be excluded.

The national legislator additionally regulated the revocation of certificates. The trust services provider must revoke a certificate in the following cases: if the signatory requested this, if certificate data is incomplete or inaccurate, if the signatory has passed away or has been deprived of legal capacity, or if digital signature data is being used contrary to the laws of Croatia.

For the purpose of preserving evidence to be used in judicial, administrative, and other proceedings, trust services providers are obligated to keep all documentation on issued and revoked certificates for ten years from the expiration of the certificate.

Penalties for non-compliance with the national acts and the eIDAS Regulation range approximately from EUR 260 to EUR 1,300 for natural persons, signatories, and representatives of legal entities, whereas trust services providers can be fined up to approximately EUR 13,000.

A number of other national laws also regulate digital signatures in certain sector-specific aspects, such as the *E-commerce Act* (legal framework for concluding contracts electronically, which is also partially regulated by the *Civil Obligations Act*), *Accounting Act* (regulates the use of digital signature in accounting documents), and the *Electronic Communication Regulation* (contains rules for electronically signing and submitting submissions to courts).

Digital signatures for a large number of contracts, however, are not clearly regulated. Therefore, before deciding on the type of signature being used, the nature of each contract and possible additional requirements for the perfection of the contract should be taken into account. For instance, the use of digital signatures is generally not possible for testamentary affairs, disposal of assets which requires consent from the Centre for Social Welfare, lifelong support agreements, and other contracts which have to be executed in the form of a notarial deed or if the certification of parties' signatures by a notary public is mandatory. Since there is no conclusive list of such contracts, each case needs to be assessed individually to confirm whether it is indeed possible to digitally sign a given contract.

b. Is there any difference between the different types of digital signatures in your jurisdiction?

Pursuant to the eIDAS Regulation, only advanced digital signatures and qualified digital signatures enable the recognition of the legal effects of a digital signature. Specific requirements for advanced and qualified digital signatures are prescribed by the eIDAS Regulation (it is uniquely linked to the signatory, it enables identification of the signatory, it is created using data under the sole control of the signatory, and enables detection of any changes to the signed content).

A qualified digital signature is basically an advanced digital signature created by using advanced technology which enables a higher level of security. A qualified digital signature is considered to be equal to a handwritten signature and has the exact same legal effects (whereas the advanced digital signature is only verifiable and in general does not have the same legal effect as a handwritten signature).

Other digital signatures, such as a plain e-mail signature (name at the end of an e-mail) would be considered a "simple" digital signature, which does not have the legal effect of advanced and qualified digital signatures.

c. What probative power each type of digital signature has in your country?

According to the eIDAS Regulation, the legal effects of a digital signature as evidence in court proceedings cannot be denied solely because of its electronic form or because the signature does not meet all requirements for a qualified digital signature. E-documents should indeed have the same legal treatment as paper documents with handwritten signatures. From a practical point of view, this means that whoever disputes the authenticity of a digital signature, will have to propose evidence to prove their argument, in the same way as if it were a handwritten signature – e.g., by expert document examination.

Exceptionally, if there have been oversights by the signatory with regard to the protection of the means and data for creating a digital signature from unauthorized access and use, then the burden of proof could be transferred to the signatory. Otherwise, it is found that a qualified digital signature is authentic, and any contrary statements should be proven.

A specific difficulty arises in the case of signatures for which the certificate has expired. It is considered that these signatures are still valid if the certificate was valid at the time of signing, even though it might have expired in the meantime. However, this complicates the process of validation, which is then possible only by submitting a request to the trust services provider, which is obligated to keep all data for 10 years after the expiration of the certificate. Nevertheless, more problems may occur in the case of certain documents which have to be kept for more than 10 years, such as accounting documents, leaving open the question regarding the possibility of verification of such e-documents and digital signatures after the expiration of the 10-year period.

d. Are there any specific groups of people that are required to have digital signatures [e.g., attorneys, notaries, government officials, etc.]?

In accordance with the *Civil Procedure Act*, all state authorities, the state attorney's office, attorneys-at-law, notaries public, court experts, court interpreters, bankruptcy administrators, liquidators, and all legal entities and natural persons who perform registered activities, are required to file their submissions to the court electronically. For this purpose, they must have previously obtained digital signatures. Submissions by these persons filed without a qualified digital signature will be disregarded by the court.

In performing their official duties, government officials (such as authorized persons in tax authorities, administrative bodies, judges, etc.) are also required to use digital signatures (unless the use of digital stamps is permitted instead).

e. Are non-personalized digital stamps recognized in your country with probative power [e.g., digital stamps used by companies, government, or administrative bodies]?

Non-personalized digital stamps can be used when an individual person is not required to sign a document, but it is sufficient to confirm that the document was issued by a certain legal entity. For instance, decisions in administrative proceedings can be signed either by a digital signature of the authorized official or by a digital stamp of the competent authority. Other examples of the use of digital stamps can be found in laws regulating the activities of notaries public and tax authorities, and digital stamps can also be used as a means of identification for anti-money laundering purposes.

The regulation of digital stamps is also based on the eIDAS Regulation (which uses the term electronic seal). The rules for digital signatures mostly apply to the digital stamp as well. The digital stamp can also be used as evidence in legal proceedings, whereas only a qualified digital stamp shall enjoy the presumption of integrity of the data and of the correctness of the origin of that data to which the digital stamp is linked. The requirements for advanced and qualified digital stamps are the same as the requirements for advanced and qualified digital signatures.

3. Digital archiving

a. Are there any laws regulating digital archives and digital archiving in your jurisdiction?

The *Croatian Electronic Document Act* only scarcely regulates digital archives and digital archiving. A digital archive is defined as a set of electronic documents organized into documentary units in accordance with the law and other regulations governing the procedures for the storage and archiving of documents. Digital archives can consist of any documents created with the application of information technologies written in the form of a binary code (images, sounds, PDF documents, etc.) in the form of a database.

Holders of public archives and archives of special significance for national history, science, and culture are additionally subject to provisions of the *Act on Archival Materials and Archives*, which also regulate the creation, storage, and conversion of archive materials to digital form.

Accounting documents can also be stored in digital form instead of paper, under conditions set out in the *Accounting Act*.

b. What are the main legal and technical requirements to digitally archive documents?

It is important to have proper storage and protection for the preservation of electronic documents since they need to be preserved in their original form. Even when stored, electronic documents need to be accessible, whereas in the case of e-documents, their content, sender, recipient, time, means, and form of creation and receipt need to be readily determined in a reliable manner at all times.

The digital archive needs to ensure that e-documents are kept in the original form in which they were created, sent, received, and stored and which does not allow changes or deletion of information and content of the document. The form of e-documents has to be readable to the persons who have the right to access them the entire time the documents are being preserved.

For the purpose of verification, the digital archive should also contain data on digital signatures on e-documents, as well as data necessary to determine the source, creator, time, and form in which the e-document has been received. Electronic documents are to be saved originally in the information system or on media which enables permanent electronic records for the established storage time.

Whenever a natural or legal person is obligated by law to keep documents in their original form, that person must keep the documents in accordance with the aforementioned conditions.

c. Is there any difference in your country's regulations between the digital archiving of paper and electronic documents?

Paper documents can also be archived in a digital form in a manner that preserves the authenticity, integrity, origin, legibility, and confidentiality of documents. Documents that have been digitally archived without meeting these requirements, are to be kept in their original form as well until the expiration of the storage period.

A set of more specific requirements applies for archives of

national interest subject to the *Act on Archival Materials and Archives*. In the case of cloud storage, archives have to be preserved in a separate cloud, protected by encryption and password, and the server must be located in Croatia.

These digital archives should be protected from loss by creating backup copies or using other methods, in accordance with the risk assessment, and the information system should enable the users to export archive units. Furthermore, the conversion of archives must be performed in a way that ensures the preservation of integrity, a guarantee of no unauthorized or undocumented modifications, and compliance with copyright regulations (where applicable).

Only documents converted to digital archives under the prescribed conditions are considered to be equal to the original documents.

d. Is any third party required to participate in the process of digital archiving in your country [e.g., a trusted service provider, government / administrative bodies, etc.]?

When it comes to private records, there is no legal requirement to engage a third party in the process of digital archiving. However, keeping a digital archive often requires special knowledge of information and communication technology, so it is logical to assume that many entities will use the services of persons who have that kind of know-how. This possibility has been foreseen in the *Electronic Document Act*, and the persons providing such services are known as information brokers.

Information brokers are obligated to ensure the security of procedures and electronic documents, but they are not responsible for the material content of electronic documents regarding which they provide their services in connection with the transfer, storage, and preservation of electronic documents.

e. Are there any sector-specific requirements and rules for digital archiving [e.g., archiving both the software and the related data to retrieve information in the financial sector]?

Most sector-specific requirements and rules for digital archiving can be found in the *Accounting Act*. Companies and entrepreneurs can convert their accounting documents preserved in the original paper form into electronic form if such conversion would not diminish their authenticity and probative power. The information system used for conversion should store information on who performed the conversion and when, for the purpose of verifying the source of the electronic form of a document.

Electronic records of accounting documents have to be stored in an information system that provides an appropriate level of protection from malware, unauthorized access, and loss of data and which ensures the integrity and legibility of the content until the expiration of the obligatory storage period.

Accounting documents converted in accordance with all legal requirements are considered to be identical to the original and have the same legal effects. Nevertheless, it is up to the entrepreneur to prove that the converted document is identical to the original, which seems an unjustified burden for a responsible business that complied with all legal requirements for such conversion. Moreover, this provision practically derogates the principle of equivalence of paper and electronic accounting documents, which might result in discouraging businesses from the use of digital archives altogether.

Mojmir Ostermann
Managing Partner
mojmir.ostermann@ostermann.hr
+385 1 5599800

Marta Jelakovic
Senior Associate
marta.jelakovic@ostermann.hr
+385 1 5599800

Janica Rakoci
Associate
janica.rakoci@ostermann.hr
+385 1 5599800

CEE LEGAL MATTERS COMPARATIVE LEGAL GUIDE: TMT 2022

CZECH REPUBLIC

Josef Donat
Partner
donat@rowan.legal
+420 224 216 212

Jan Tomisek
Partner
tomisek@rowan.legal
+420 224 216 212

Pavel Hejl
Counsel
hejl@rowan.legal
+420 224 216 212

CEE
Legal Matters

1. Legal framework for writing and electronic contracts

a. What are the requirements in your jurisdiction to consider a document to be in writing? Are there any formal/technical requirements?

According to Article 562(1) of *Act no. 89/2012 Coll.*, the *Civil Code*, as amended, the written form of a legal act is preserved when the legal act is made by electronic or other technical means that enable the recording of its content and the identification of the person acting. Therefore, a document is in writing if its content is recorded, either physically, or electronically.

Should an electronic document present a legal act, it must also be properly signed by the person acting, using a digital signature (see Article 2a).

In some cases, the law may require a paper form of a document, which means a physical form only. In these cases (e.g., a contract that transfers the ownership of real estate) such legal acts cannot be made electronically.

b. Are electronic documents [e.g., an email] per se considered to be in writing under your law?

Yes, as an email fulfills the requirement of its content being recorded pursuant to Article 562(1) of the *Civil Code* (see Section 1.a.).

c. What probative power paper and/or electronic documents have that are to be considered in writing?

In theory, the probative power of paper and electronic documents is equal. E.g., pursuant to Article 79(2) of *Act No. 99/1963 Coll.*, the *Code of Civil Procedure*, as amended, the applicant in civil proceedings may attach evidence to an application in either paper or electronic form. In practice, the probative power of documents relies on the individual nature of the document and its signature, as in particular cases it may be easier or more difficult to challenge the validity of the document.

d. What are the general rules and requirements to conclude a contract electronically?

Czech law allows contracts to be concluded in various forms, namely in writing, orally, or implicitly. In some cases, contracts must be made in writing, but that does not exclude electronic documents (see Section 1.a.). A contract is concluded when its parties agree on its content (Article 1725 of the *Civil Code*). Since concluding a contract is a legal act, the signatures of the parties are required (Article 561(1) of the *Civil Code*).

Rarely, the law may require a legal act **(i)** to be made in the form of a public deed (pursuant to Article 3026(2) of the *Civil Code* this is usually a notarial record) or **(ii)** to have the signatures of all the parties on the same page of paper (e.g., contracts that transfer the ownership of real estate) – in which case such legal acts cannot be made electronically.

e. Are there any sector-specific rules that define further requirements to conclude contracts electronically [e.g., contracting via an authenticated electronic channel, contracting via video chat, etc.]?

There are some relevant sector-specific rules relating to anti-money laundering regulations. If identification of a party is required in the process of concluding a contract, such identification must be done physically, not online, which may limit the options for the electronic conclusion of a contract.

2. Digital signatures

a. Are there any laws regulating the use of digital signatures in your jurisdiction?

The main regulation applicable in the Czech Republic is *Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC* (eIDAS Regulation). In terms of national law, the relevant act is *Act No. 297/2016 Coll.*, on trust services for electronic transactions, as amended (Act on Services).

b. Is there any difference between the different types of digital signatures in your jurisdiction?

Yes, the difference between the different types of digital signatures depends on their use, as for certain purposes, only certain types may be used. The Act on Services also establishes a specific local type of digital signature called a recognized electronic signature, which is an advanced electronic signature based on a qualified certificate for electronic signatures or a qualified electronic signature (Article 6(2) of the Act on Services).

c. What probative power each type of digital signature has in your country?

Contrary to the eIDAS Regulation and pursuant to the Act on Services, any type of digital signature is considered to be a handwritten signature, so any type of digital signature may be used freely unless stipulated otherwise by law (Article 7 of the Act on Services). Please note, however, that the aforementioned interpretation has been subject to some degree of professional debate, despite the fact that it was clearly the lawgiver's intent to create a different regulation from the eIDAS Regulation. Therefore, in theory, the probative power of various types of digital signatures is the same. In practice, however, the probative power of digital signatures differs, as in particular cases it may be easier or more difficult to challenge the validity of the signature.

d. Are there any specific groups of people that are required to have digital signatures [e.g., attorneys, notaries, government officials, etc.]?

According to the law, when exercising their powers public authorities and persons are obliged to use a qualified electronic signature to sign electronic documents (Article 5 of the Act on Services). When signing an electronic document by which an act is performed in relation to a public signatory or another person in connection with the exercise of their powers, only a recognized electronic signature may be used for signing with an electronic signature (Article 6(1) of the Act on Services).

e. Are non-personalized digital stamps recognized in your country with probative power [e.g., digital stamps used by companies, government, or administrative bodies]?

In the Czech Republic, electronic seals pursuant to Section 5 of the eIDAS Regulation and Articles 8–10 of the Act on Services are recognized.

3. Digital archiving

a. Are there any laws regulating digital archives and digital archiving in your jurisdiction?

Yes, *Act No. 499/2004 Coll.*, on archives and record management and on amendments to certain acts, as amended (Act on Archives), mostly in its Title II, where the performance of filing services is covered. The performance of filing services means ensuring the professional management of documents arising from the activities of the originator, or from the activities of its legal predecessors, including their proper receipt, registration, distribution, circulation, handling, execution, signing, dispatch, storage, and disposal by shredding, including the checking of these activities (Article 2(l) of the Act on Archives).

b. What are the main legal and technical requirements to digitally archive documents?

Public originators carry out, by default, filing services in electronic form in electronic filing systems. Where public originators perform filing services in an electronic filing system that is part of an information system for the handling of classified information, such a system must meet the requirements set out in the national standards. Originators maintain a register of names for the automatic processing of data on the senders and addressees of registered documents. When documents are processed, all documents relating to the same matter are combined in a file. Documents in digital form are linked to each other by means of metadata. Public originators may use special technological means which may substitute an electronic signature, electronic seal, electronic time stamp, or other electronic means for a similar purpose, exclusively for the needs of the originator concerned; these special technological means must make it possible to detect any subsequent modification of the data in the document and to unambiguously verify the identity of the person who attached it. (Article 63–65 of the Act on Archives)

c. Is there any difference in your country's regulations between the digital archiving of paper and electronic documents?

No, aside from the differences originating from the form of the document. E.g., paper documents relating to the same matter are combined in a file physically, whereas digital documents are combined by metadata.

d. Is any third party required to participate in the process of digital archiving in your country [e.g., a trusted service provider, government / administrative bodies, etc.]?

All electronic filing systems used for archiving must meet the requirements of the Act on Archives, *Decree No. 259/2012 Coll.*, on the details of the filing service, and the national standards. Compliance with these requirements must be confirmed by an attestation (Article 69e of the Act on Archives). Attestation is performed by attestation centers – various subjects pursuant to Article 69b of the Act on Archives.

e. Are there any sector-specific requirements and rules for digital archiving [e.g., archiving both the software and the related data to retrieve information in the financial sector]?

No. The requirements for archiving generally do not distinguish between physical and digital documents. Some related issues concern the validity of electronic signatures on digital documents, for which reason electronic time stamps are usually employed. On the other hand, where electronic legal transactions are carried out and stored in an electronic system in a systematic and sequential manner and are protected against alteration, such records are by law presumed to be reliable (Article 562(2) of the *Civil Code*), thus repeated application of electronic time stamps may be unnecessary in such cases.

Josef Donat
Partner
donat@rowan.legal
+420 224 216 212

Jan Tomisek
Partner
tomisek@rowan.legal
+420 224 216 212

Pavel Hejl
Counsel
hejl@rowan.legal
+420 224 216 212

ROWAN LEGAL

DRAKOPOULOS

CEE LEGAL MATTERS COMPARATIVE LEGAL GUIDE: TMT 2022

GREECE

Michalis Kosmopoulos
Partner
mkosmopoulos@drakopoulos-law.com
+30 2106836561

Panagiotis Tampoureas
Senior Associate
ptampoureas@drakopoulos-law.com
+30 2106836561

CEE
LEGAL MATTERS

www.ceelegalmatters.com

1. Legal framework for writing and electronic contracts

a. What are the requirements in your jurisdiction to consider a document to be in writing? Are there any formal/technical requirements?

Under Greek law, it is required that a document bear the handwritten signature of its issuer (Article 443 of the *Greek Code of Civil Procedure* (GCCP) and Article 160 of the *Greek Civil Code* (GCC)). Also, the *Greek Criminal Code* seems to enrich and clarify the aforementioned definition of a written document, stating that any writing intended or likely to prove a fact having legal effect may be qualified as a document.

Furthermore, as per Article 444 of the GCCP, the following are also considered to be private documents: **i)** the books kept by traders and professionals under commercial law or other provisions, **ii)** the books kept by lawyers, notaries, bailiffs, doctors, pharmacists, and midwives under the applicable provisions, **iii)** photographic or cinematographic representations, voice recordings, and any other mechanical representation, which is deemed to include also electronic documents. Therefore, Greek law recognizes the fact that technology affects all kinds of transactions and does not remain impassive by these developments.

b. Are electronic documents [e.g., an email] per se considered to be in writing under your law?

In general, according to the Greek legal framework, an electronic document is defined as a set of data records on the magnetic disk of a computer, which is printed on the basis of program instructions in a human-readable manner, either on the screen of the machine or on its attached printer. Article 15 of *Law 4727/2020* states that electronic documents are mandatorily accepted by public sector bodies as well as by the courts of all instances, provided that they have been signed by means of a qualified electronic signature or qualified electronic stamp. Such a signature is necessary to qualify the document as signed via a handwritten signature. However, under Article 16 of the same law, an electronic document bearing any kind of electronic signature is considered to be a mechanical representation and, thus, a private document.

More specifically and with respect to e-mails, the e-mail address specified by each user in a unique way and its declaration in each transmitted message constitutes proof of the identity of the sender. Prior to *Law 4727/2020*, Greek case law had accepted that the unique e-mail address has the same nature as a handwritten signature, even if it does not have the traditional form of the latter. Therefore, the most important condition of the term "document" (the handwritten signature of the issuer) is fulfilled through the unique e-mail address, leaving no doubts that electronic documents are considered to be equal to traditional (i.e., handwritten) documents in Greece. The fact that the Greek legal system has fully recognized the existence of electronic documents is also confirmed by the acceptance of the electronic service of documents both for court and mediation procedures (Article 112A of the GCCP & Article 7 Paragraph 2 of *Law 4640/2019*).

c. What probative power paper and/or electronic documents have that are to be considered in writing?

The probative power of the paper and/or electronic documents is the same, provided that paper documents bear the handwritten signature of a physical person and the electronic documents are signed by a qualified electronic signature or qualified electronic stamp. The same probative value is recognized in case the documents are mechanical representations (e.g., e-mail), but under Article 16 Paragraph 2 of *Law 4727/2020*, the probative value of the electronic documents bearing a simple or advanced signature remains at the discretion of the court. As mentioned above, Greek courts have ruled that the legally certified copy of the e-mail sent, which is contained in the recipient's hard disc, constitutes full proof that the statement included therein originates from the sender.

d. What are the general rules and requirements to conclude a contract electronically?

In general, the conclusion of an electronic contract requires all the necessary elements of a traditional contract under Articles 127 subs. of the GCC. In particular, the necessary elements are **(i)** a declaration of will of one party to enter into a contract and **(ii)** a declaration of acceptance of the proposal to enter into a contract by the other party.

What differentiates the legal dogma from the electronic environment is that the coincidence of these declarations of will is made electronically, through the unique e-mail address that proves the identity of each contracting party or an application having the same effect. Following the sending of an electronic message by one contracting party, the receipt of the declaration of will is deemed to have taken place when the message reaches the electronic mailbox of the other contracting party.

When it comes to e-commerce contracts, electronic contracts in Greece are regulated by *EU Directive No. 2000/31* along with the respective *Presidential Decree No. 131/2003* implementing the directive. By virtue of this legislation, it is fully accepted that in every EU member state, electronic contracts should be awarded the same legal status as paper contracts. The provisions of the aforementioned presidential decree permit the conclusion of contracts with electronic means, providing for three exceptions. More specifically, electronic contracts are not permitted when **(i)** the contract creates or transfers property rights to real estate assets, **(ii)** the contract by law requires

recourse to the courts, public authorities, or professions exercising public authority, and **(iii)** the contract falls within the scope of family law or the law of succession.

e. Are there any sector-specific rules that define further requirements to conclude contracts electronically [e.g., contracting via an authenticated electronic channel, contracting via video chat, etc.]?

It is indisputable that the COVID-19 outburst that forced many more people to work from home has significantly reduced face-to-face business, and has triggered a growth in video conferencing. In particular, in the banking and finance sectors, the number of video (i.e., distance) interactions has sharply increased.

However, in Greece, there are no rules in force regulating further requirements, such as the use of video chat, in order to conclude a contract electronically. This may be explained by the preference of the Greek legal system for the written form of contracts for evidence purposes. The aforementioned facts do not necessarily suggest that, in Greece, means such as video chat or electronic channels are something completely unknown. The truth is that many administrative authorities are now serving citizens through video calls. For example, a Greek citizen may communicate through a video chat with an employee of the competent Tax Office in order to obtain a tax registration number. However, it must be clarified that under no circumstances does the aforementioned service equal to the conclusion of a contract.

It is strongly believed that in a few years, the Greek legal system will be mature enough to accept and regulate the conclusion of contracts via such means.

2. Digital signatures

a. Are there any laws regulating the use of digital signatures in your jurisdiction?

The use of digital signatures in Greece is regulated by *Regulation 910/2014 of the European Parliament and of the Council of July 23, 2014, on electronic identification and trust services for electronic transactions in the internal market* (Regulation 910/2014 or eIDAS), along with *Law 4727/2020 on Digital Governance* (transposition of *Directives (EU) 2016/2102* and *2019/1024*) and *Electronic Communications* (transposition of *Directive (EU) 2018/1972*), the latter applying to the public sector.

b. Is there any difference between the different types of digital signatures in your jurisdiction?

Under the eIDAS Regulation the following types of signatures are provided:

- "electronic signature" – data in electronic form which are attached to other electronic data or logically associated with other data in electronic form, and which are used by the signatory to sign;
- "advanced electronic signature" – a signature which must be uniquely linked to the signatory, be capable of identifying the signatory, and be created using electronic signature creation data that the signatory can, with a high level of confidence, use under their sole control and be linked to the data signed therewith in such a way that any subsequent change in the data is detectable;
- "qualified electronic signature" – a signature created by a qualified electronic signature creation device and based on a qualified certificate for electronic signatures.

As already mentioned, electronic documents which have a qualified electronic signature or qualified electronic stamp are mandatorily accepted by public sector bodies as well as by the courts of all instances, since the qualified electronic signature is equivalent to a handwritten signature. This does not necessarily mean that the other types of signatures are less important, because electronic documents bearing a simple or advanced electronic signature are freely admissible as legal evidence, while their probative value lies at the discretion of the court.

c. What probative power each type of digital signature has in your country?

As per Article 25 of the eIDAS Regulation, in conjunction with *Law 4727/2020*, an electronic signature has the same legal and probative power as a handwritten signature.

Before the implementation of the eIDAS Regulation, *Presidential Decree no. 150/2001*, through which the *Directive (EU) 1999/93* was transferred into Greek law, had equalized the advanced electronic signature with the handwritten one, in the sense of giving it the same probative power. However, as provided under the eIDAS Regulation, the electronic signature shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic signatures.

As already mentioned hereinabove, by taking into consideration that only electronic documents which have a qualified electronic signature or qualified electronic stamp are compulsorily accepted by public sector bodies as well as by courts of all instances, the qualified electronic signature is of higher probative value. This does not necessarily mean that other types of signatures are less important because as already mentioned electronic documents with a simple or advanced electronic signature are also admissible as legal evidence.

d. Are there any specific groups of people that are required to have digital signatures [e.g., attorneys, notaries, government officials, etc.]?

Although there is no explicit provision in *Law 4727/2020* requiring a specific group of people to have an electronic signature, Article 17 of the same law provides that the electronic circulation of documents within public bodies cannot take place without an advanced or qualified digital signature or stamp of the competent body. This provision may imply a requirement for digital signature when it comes to government/administrative bodies. Moreover, lawyers also need a qualified digital signature in order to file writs electronically.

e. Are non-personalized digital stamps recognized in your country with probative power [e.g., digital stamps used by companies, government, or administrative bodies]?

Non-personalized digital stamps are not recognized under Greek law and therefore their probative value remains to be examined at the discretion of the courts.

3. Digital archiving

a. Are there any laws regulating digital archives and digital archiving in your jurisdiction?

Article 20 of *Law 4727/2020* as well as *Presidential Decree no. 25/2014*, which applies only to the public sector, regulate digital archiving by public sector bodies. There is no relevant legislation with respect to the private sector.

b. What are the main legal and technical requirements to digitally archive documents?

The basic principles of digitally archiving documents are security, integrity, authenticity, confidentiality, accessibility, legibility, and quality.

In particular, according to *Presidential Decree no. 25/2014*:

- Electronic documents shall be organized and classified into relevant groups by the institutions obtaining them on the basis of the functions or activities of each institution in order to ensure their optimal access, retrieval, management, and final disposal;
- any electronic document filed in an electronic folder automatically acquires the properties and characteristics of the folder to which it belongs;
- the content, structure, and metadata of electronic documents from the moment they are archived until the completion of the process of their clearance shall remain the same for the entire retention period, as defined for paper documents.

c. Is there any difference in your country's regulations between the digital archiving of paper and electronic documents?

Under *Presidential Decree no. 25/2014*, which is also applicable to paper documents, an additional requirement for the archiving of paper documents shall be their prior digitalization.

Other than that, no other differences arise from the legislation in force.

d. Is any third party required to participate in the process of digital archiving in your country [e.g., a trusted service provider, government / administrative bodies, etc.]?

The process of digital archiving within the public sector, as expressly provided for by Article 20 of *Law 4727/2020*, is carried out by an authorized (for this purpose) body of the public sector.

e. Are there any sector-specific requirements and rules for digital archiving [e.g., archiving both the software and the related data to retrieve information in the financial sector]?

The archiving of Armed Forces' documents constitutes an exception to the general rule that paper documents must be destroyed five years following their digitalization.

Michalis Kosmopoulos
Partner
mkosmopoulos@drakopoulos-law.com
+30 2106836561

Panagiotis Tampoureas
Senior Associate
ptampoureas@drakopoulos-law.com
+30 2106836561

provaris
VARGA & PARTNERS

CEE LEGAL MATTERS COMPARATIVE LEGAL GUIDE: TMT 2022

HUNGARY

Adam Liber
Partner
liber.adam@provaris.hu
+36 20 524 4959

Tamas Bereczki
Partner
bereczki.tamas@provaris.hu
+36 30 220 2428

CEE
Legal Matters

1. Legal framework for writing and electronic contracts

a. What are the requirements in your jurisdiction to consider a document to be in writing? Are there any formal/technical requirements?

The Hungarian legal framework considers the formal requirements of documents crucial and as a validity requirement in certain cases, especially in civil law and in certain industries, business sectors (e.g., finance), for instance with documents concerning suretyships, contractual penalties, or with contracts such as the sale of real estate or pre-emption. The requirement for a document to be made in writing is a precaution to ensure that the content and party(ies) producing the document can be subsequently proven.

The requirements for a document to be in writing are established by Section 6:7 of the *Hungarian Civil Code*, which states that a document qualifies as written if at least its material content is put down in (hand)writing, and the party(ies) sign it. The material content of a document cannot be determined generally, considering that different types of documents (e.g., contracts of sale, wills, authorizations, etc.) require different essential elements to be valid. Under applicable Hungarian law practice, a document is signed when the party executes the document with a wet signature, which is capable to prove the identity of the party, and which also indicates that the party acknowledges the document as their own. Either the *Civil Code* or different legal acts may contain further requirements regarding special situations (e.g., public deeds or private deeds of full probative power), but these two conditions are considered by the *Civil Code* to be the most fundamental.

However, electronic documents must correspond to further requirements so that the law would consider them to have been made in writing. The *Civil Code* intends to secure that an electronic document is authentic and unadulterated, with regard to the content, time, and the party(ies), hence it requires that it is presented in a form that allows for the proper recall of the content of the document, and for the identification of the person who made the statement and the time the statement was made.

In line with European Union policy, the regulation of the validity of electronic documents is technology-neutral, thus it allows for the possibility that many solutions could provide valid electronic documents. Unfortunately, the requirements set by the aforementioned provisions of the *Civil Code* can only be satisfied by the use of digital signatures. Simple electronic documents cannot adequately prove the authenticity of either condition or they are generally not regarded to be in writing.

b. Are electronic documents [e.g., an email] per se considered to be in writing under your law?

Under applicable Hungarian court practice, decisions of the Budapest Regional Court of Appeal and the Szeged Regional Court of Appeal both categorically declined the notion to accept the "written" nature of simple emails. The former case is of particular interest: the plaintiff sent a properly written, signed, and stamped claim for press correction to the defendant in scanned format via email. The court held that this way the claim cannot be considered to have been made in writing – which is a pre-requirement for the procedure to initiate – because it was attached to an email that was not signed with an advanced electronic signature, and as such the scanned document cannot sufficiently satisfy the requirements to be authentic and unadulterated.

However, Hungarian labor courts hold a different opinion. While the *Labor Code* also states that a document must allow for the recall of the proper content, the identification of the person who made the statement, and the time of the statement, it does not require the document to be signed by the party. In an opinion, the Curia (the Hungarian supreme court) held that the validity of an electronic document not properly signed by the employer cannot be disputed by the employee if it is undoubtedly made by the employer and the authenticity of the document is not contested by the employee.

c. What probative power paper and/or electronic documents have that are to be considered in writing?

The *Hungarian Code of Civil Procedure* is based on the principle of free appraisal of evidence and the validity of a document made in writing does not automatically imply probative power to it. In this matter, Hungarian law does not differentiate between paper and electronic documents: if they do not qualify as a public deed or a private deed with full probative power, they are not given a statutory presumption, and the court will determine their probative value in accordance with the standard procedure.

On the other hand, electronic documents can qualify as both public deeds and private deeds with full probative power. Public deeds, issued by a court, a notary, or another authority or administrative organ, prove with full probative power that the issuing entity carried out a measure or adopted a decision and that the data and the facts included in the document are true, and the statement was made as that specific place and manner. The *Hungarian Code of Civil Procedure* also requires public deeds made in an electronic form to contain a qualified electronic signature or stamp, an advanced electronic signature or stamp based on a qualified certificate, and – if required by law – a timestamp. The advantage of making such documents (and private deeds with full probative power) is that, unlike a

regular, unauthenticated private deed, the document, and its content shall be deemed original unless proven to the contrary.

The *Code of Civil Procedure* also offers a number of ways to perform an electronic private deed with full probative power: the document must be attached with a qualified electronic signature or an advanced electronic signature based on a qualified certificate, and it must be authorized using a Document Authentication Based on Identification service, or the document is attributed to the issuing person by a service provider via a specific authentication service specified by law.

d. What are the general rules and requirements to conclude a contract electronically?

With regard to the conclusion of contracts electronically, it must be noted that the *EU E-Commerce Directive* specifically obliges EU Member States to allow for and create the legal framework of electronic contracts.

The requirements for concluding a contract electronically do not substantially differ from those of a valid electronic document. To conclude a contract electronically, the parties need to have at least an advanced electronic signature, the use of which will enable them to create a valid electronic contract. The law does not stipulate that both parties must sign the contract electronically: it is perfectly acceptable that one party attaches their electronic signature with the contract while the other signs it traditionally. In fact, it is not necessary for the parties to sign the same copy of the contract if both the traditionally and electronically signed copies are available to both of them.

Furthermore, the use of electronic signatures to conclude the contract may prove beneficial to enterprises if they have qualified electronic signatures or advanced electronic signatures based on a qualified certificate. Concluding contracts with these two types of electronic signatures will render the contract into a private deed with full probative power which offers more security for the parties than signing a contract by hand.

By incorporating the provisions of the EU's *E-Commerce Directive*, Sections 6:82-85 of the *Civil Code* also provide regulation for the conclusion of electronic contracts. These sections do not regulate the conclusion of contracts via email or any equivalent individual communication device, hence they only apply to contracts concluded via "clicks."

The *Civil Code* provisions oblige the party to the contract who provides the electronic way of contract conclusion to offer adequate information on the process of the conclusion of the contract (e.g., technical steps, the language of the contract, consequences of technical failures), to ensure the continuous availability of its general terms and conditions, and to ensure that the other party is able to correct any mistakes it might have done while filling out the contract with the required information. Any juridical act done electronically becomes applicable only when it is available to the other party. The party who provides the electronic way must also confirm the arrival of the other party's statements without delay.

It can be seen that these provisions of the *Civil Code* are mostly of a consumer protection nature, as they provide obligations for the party that provides the electronic way of contract conclusion which is usually the business offering its products or services. They also apply in B2B contracts, however, parties to B2B contracts may deviate from these provisions, while parties to B2C contracts are not allowed to do so.

e. Are there any sector-specific rules that define further requirements to conclude contracts electronically [e.g., contracting via an authenticated electronic channel, contracting via video chat, etc.]?

Besides the general provisions, there are some specific rules in Hungarian legislation for different sectors, such as e-commerce or consumer protection. Following EU legislation, Hungary has enacted *Act no CVIII of 2001 on Electronic Commerce and on Information Society Services* (E-Commerce Act), which in Sections 5 and 6 regulates the conclusion of electronic contracts in the case of information society services. The provisions of the E-Commerce Act do not apply solely to B2C contracts, but it does not apply to the conclusion of contracts via emails or equivalent individual communications. The act outlines the procedure of how to conclude contracts electronically, it establishes what information the service providers must supply to the recipients of the service, and it also requires the service provider to make available its terms and conditions of service in order to try and level the playing field. As the content of these sections is also incorporated into the provisions of the *Civil Code* specified in Section 1(d), we do not deem it necessary to reiterate them.

Specific rules on the conclusion of contracts, including electronic contracts between businesses and consumers are found in *Gov. Decree no 45/2014 (II. 26.)*. The provisions of the government decree mainly focus on the information the business must provide the consumer with, while also stipulating the procedure of cancellation and unilateral termination of the contract.

In 2021 the aforementioned Section 6:7 of the *Civil Code* was amended with paragraph (3a) which regulates the electronic conclusion of contracts regarding real estate, matters of succession, family, companies, and financial services. According to this paragraph, contracts concerning these fields of law that are concluded electronically shall only be considered valid if their content is recorded using characters and they comply with the legal provisions that regulate the creation of electron-

ic documents. The purpose of the amendment was to guarantee the security of such contracts, by establishing the specific requirements they must adhere to in order to exclude the possibility of disputes in these matters that could arise from the insufficient formal requirements of the contracts.

Specific regulations for the electronic conclusion of contracts can also be found in *Act no CCXXXVII of 2013 on Credit Institutions and Financial Undertakings* (Hpt.), which regulates the activities of actors in the financial sector. Section 279 of the Hpt. expressly requires any contract concerning financial services offered by financial undertakings to be concluded in writing, for which there are some options on how to achieve this. Firstly, the application of advanced or qualified electronic signatures is the most generic solution, that fulfills the requirements, however, it is possible to conclude contracts via closed systems, the application of central administrative electronic identification service, or to make statements using biometric identification.

In order for any of these services to operate lawfully and to consider juridical acts and contracts made and concluded via using them valid, the Hungarian National Bank issued a circular that defines strict requirements that these services must adhere to, and financial undertakings must notify the Hungarian National Bank about their use of such systems and services.

Regarding the conclusion of contracts of financial nature, *Act no XXV of 2005 on the Remote Sale of Financial Services* prescribes a list of information that financial institutions must provide the consumer with when concluding contracts – among else – electronically.

When concluding a contract, financial institutions must ensure that the other party is not someone with whom they are forbidden to be contracted with under the rules of *Act LIII of 2017 on the prevention and combating of money laundering and terrorism financing* (Pmt). The Hungarian National Bank in its *Decree no 26/2020 (VIII. 25.*) allowed for the client screening procedure to be conducted via an audited electronic communications network, which must adhere to very strict requirements set by the National Bank.

A specific provision can be found in *Act no XLVIII of 2008 on Advertisements*, which in Section 5/B stipulates that contracts on the provision of advertisements must be concluded in writing, however, it also states that contracts concluded electronically are considered to be in writing even if they are not applied with electronic signatures.

2. Digital signatures

a. Are there any laws regulating the use of digital signatures in your jurisdiction?

As Hungary is an EU Member State, the *EU Regulation 910/2014 on electronic identification and trust services for electronic transactions in the internal market* (eIDAS Regulation) is applicable, which regulates the use of – among others – digital signatures in the entire European Union. The eIDAS Regulation is also incorporated in *Act no CCXXII of 2015 on Electronic Administration and Trust Services* (EATS Act), and the detailed provisions are provided in lower-level legislation, in government [*Gov. Decrees nos 451/2016 (XII. 19.) and 137/2016 (VI. 13.*)] and ministerial decrees [*Interior Ministerial Decrees nos 24/2016 (VI. 30.) and 41/2016 (X. 13.)*].

b. Is there any difference between the different types of digital signatures in your jurisdiction?

Based on the provisions of the eIDAS Regulation, there are three types of digital signatures currently acknowledged in Hungary:

(i) *Simple electronic signatures*, that are not subject to any specific requirements and as such do not hold any probative value either. The eIDAS Regulation defines it as data in electronic form which is attached to or logically associated with other data in electronic form, and which is used by the signatory to sign. Effectively, they are signatures drawn on the document using electronic means or scanned from handwritten signatures. These types of signatures are unable to adequately prove the identity of the signatory person and shall not be used when performing a contract to be in writing.

(ii) *Advanced electronic signatures* are the next level in terms of probative value and protection. According to the eIDAS Regulation, an advanced electronic signature shall be uniquely linked to the signatory, capable of identifying the signatory, created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control, and linked to the data signed therewith in such a way that any subsequent change in the data is detectable. This effectively means that the document that has been signed using advanced electronic signatures cannot be altered without the parties noticing it, and the document leaves no doubt about the identity of the signatory. Advanced electronic signatures are provided by so-called trust service providers who take responsibility for the identification of the signatories.

(iii) *Qualified electronic signatures* offer the highest level of authenticity when it comes to digital signatures and are defined by the eIDAS Regulation as advanced electronic signatures that are created by a qualified electronic signature creation device, and which are based on a qualified certificate for electronic signatures. They are issued by qualified trust service providers

that must adhere to rigorous security requirements in order to ensure a high level of protection and trust in these services. Qualified electronic signatures are created using a special card or token, and/or software, which will allow the qualified trust service provider to issue a certificate that will become a part of the document and will ensure the identity of the signatory and the authenticity of the signature.

c. What probative power each type of digital signature has in your country?

The different types of digital signatures offer different levels of probative powers to the documents they are attached to. Simple and advanced electronic signatures do not provide any probative value to the documents they are attached to, they only differ in that documents applied with advanced electronic signatures are considered to be in writing, while simple electronic signatures do not have this result. Qualified electronic signatures, on the other hand, will result in the document it is attached to being a private deed with full probative power or – in case the document is issued or signed by the appropriate entities – a public deed.

d. Are there any specific groups of people that are required to have digital signatures [e.g., attorneys, notaries, government officials, etc.]?

With the spread of electronic administration in Hungary from the 2000s onwards, the use of digital signatures became mandatory or at least unavoidable in certain areas. The authenticity of documents and public trust in their services are especially important with notaries, which is why notaries are required to have digital signatures from 2007 onwards. Digital signatures are used to sign electronic public deeds and in certain other cases, such as data requests to ascertain the identity of the party.

Attorneys are not required to obtain a digital signature, however, in most cases, it is unavoidable for them to have one. The EATS Act stipulates that economic operators (e.g. companies, cooperatives, associations, etc.) are obliged to electronic administration in any criminal, misdemeanor, civil, administrative, and authority procedure they are party to, and as such, attorneys that represent economic operators cannot avoid the use of digital signatures. Moreover, in registration procedures, undertakings must submit all documentation in an electronic form to the company registration court, and since legal representation is mandatory in these procedures, attorneys representing the undertaking in the procedure must sign the necessary documents using their digital signature.

Independent court bailiffs are also required to have digital signatures, considering the fact that in recent years, many procedures they participate in have gone digital. Both notaries and court bailiffs receive their digital signatures from their respective chamber or association.

Obviously, since the EATS Act offers the possibility to, and in some cases prescribes the use of electronic administration, it is unavoidable that government officials, court officials, etc. who work as case administrators in such procedures also have their own digital signatures. Within electronic administrative procedures, parties have the possibility to verify the validity of any digital signature on a document using the Governmental Electronic Signature Verification Service, and moreover, parties without a digital signature – in some cases – have the possibility to authenticate their electronic documents using the Document Authentication Based on Identification service provided by the government.

e. Are non-personalized digital stamps recognized in your country with probative power [e.g., digital stamps used by companies, government, or administrative bodies]?

Apart from electronic signatures, the eIDAS Regulation also provides for the use of electronic seals that legal persons can use for electronic documents and administration. These electronic seals are subject to the same provisions as electronic signatures and have the same three types that offer different levels of authentication. Where electronic signatures are used to identify the individual who signed the document, an electronic seal can identify the legal person who issued the document. Qualified electronic seals, just like qualified electronic signatures can also be used to create private deeds with full probative power, which can be of great use to organizations.

3. Digital archiving

a. Are there any laws regulating digital archives and digital archiving in your jurisdiction?

Unlike digital signatures, digital archiving is not regulated at an EU level, and Hungarian legislation is thus independent of that of other European countries. Hungarian law regulates the matter on two levels: the E-Commerce Act regulated the matter first, establishing that if any act prescribes to preserve a document, it can be done so via digital archiving; meanwhile, the EATS Act created a general regulation of archiving services. The more comprehensive, detailed provisions of digital archiving can be found in a lower-level piece of legislation: *Innovation and Technology Ministerial Decree no 1/2018 (VI. 29.)* (ITM Decree) completes the framework of the two acts established.

b. What are the main legal and technical requirements to digitally archive documents?

The ITM Decree declares itself applicable whenever archiving a document is performed electronically. The primary requirement of the decree is to ensure the preservation of the document in a way that ensures the protection of the electronic document against deletion, deliberate or unintended destruction, retrospective modification, damage, and unauthorized access. It also establishes the obligation of the person obligated to preserve the document to ensure that it remains legible and understandable throughout the period of archiving. The preservation must be done in a way that reflects the type and authenticity of the document.

The decree offers a variety of ways through which the archiving obligation can be performed. If the document is provided with at least an advanced electronic signature, the obligated person has two choices: it can entrust a trust service provider with the digital archiving of the document, or it can perform the obligation itself, by verifying and maintaining the validity of the electronic signature on the document, and it must also comply with the obligation to preserve the software and hardware that allows for the subsequent restoration of the document. The obligation may also be performed using an electronic data interchange system, or, in the case of electronic invoices, it can be done so by creating a hash code of the electronic invoice, which hash code is then transmitted to the tax authority and is preserved together with the electronic invoice document.

A new possibility that was not available before the aforementioned ITM Decree was issued is to perform digital archiving using closed systems without having to approve the use of it by an authority or to have it certified by an accredited certification body. It only requires the developer of the software or IT solution to issue a statement in writing that the software or IT solution is completely compliant with the applicable legal requirements. It also needs to have documentation that offers a detailed overview of the processes of the software or IT solution, applied technologies and standards, the solutions that guarantee the closed system archiving, and the built-in and subsequent control mechanisms. The developer and the person obliged to perform the archiving are jointly and severally liable to ensure that the closed system archiving solution is compliant with the requirements of the decree.

While a progressive approach, the ITM Decree failed to define what exactly is a closed system archiving solution. Different pieces of legislation also use this or similar terms, but only one, namely *Gov. Decree no 451/2016 (XII. 19.*) defines a closed system, which is an electronic information system separated due to its function that exclusively serves the purposes of satisfying specific demands and the operation of the organization and the technology created explicitly to satisfy said demands and its operation is based on law or an agreement between specific parties without affecting a third party.

International best practice defines a closed system as a state that is capable to ensure the confidentiality, integrity, and availability of the data processed, and the system provides overall and continuous protection to the data that is proportional to the risks. As a combination of the different definitions, a software or IT solution capable to provide closed system archiving should be interpreted as a solution that satisfies the special demands and the operation of the organization and the technology created explicitly to satisfy said demands by ensuring the confidentiality, integrity, and availability of the archived electronic document in a continuous, comprehensive manner that is proportionate to the possible risks.

c. Is there any difference in your country's regulations between the digital archiving of paper and electronic documents?

Digital archiving of paper documents is also allowed for by the *Gov. Decree no 451/2016 (XII. 19.*), both for administrative organizations and economic operators. When creating an electronic copy or a paper document, the operator must ensure that the content or the image of the electronic document is identical and authentic to that of the paper document. The operator must apply a clause to the document saying it is "identical to the original paper-based document," must attach their electronic signature or seal to the document, and must apply a timestamp, if the time of the creation of the copy is important. Economic operators must create a copy of the document in a way that the electronic copy is identical in image.

The governmental decree establishes a requirement that makes the creation of original electronic documents more feasible than creating electronic copies of paper documents. The electronic signature or seal that must be applied to the electronic copy has to be a qualified electronic signature or qualified electronic seal in order to exclude fraud. Many economic operators do not have much need for a qualified electronic signature or seal other than the conversion of paper documents to electronic copies, so this provision of the regulation makes it much harder for economic operators to take advantage of this opportunity. However, it is beneficial to all organizations, that having an authentic electronic copy of the original paper-based document makes the paper document obsolete, and it can be destroyed.

d. Is any third party required to participate in the process of digital archiving in your country [e.g., a trusted service provider, government / administrative bodies, etc.]?

Another great advantage of closed-system archiving solutions is that it excludes the obligation to involve a third party in the process, which could save time and cost to the person obligated to preserve the documents. The further digital archiving possibilities stipulated by the ITM Decree almost all necessitate the involvement of a third party: the hash code of electronic invoices must be transmitted to the tax authority, while the use of an electronic data interchange system fundamentally requires the participation of another party.

The use of trust service providers as provided for by the eIDAS Regulation means that the person obligated to preserve the documents entrusts a trust service provider to archive the electronic document attached with an advanced electronic signature for them. Trust service providers must register themselves with the Hungarian National Media and Infocommunication Authority, which keeps a list of the current trust service providers and performs their monitoring as well.

The provision of trust services is also subject to regulations set by the *Interior Ministerial Decree no 24/2016 (VI. 26.*). This decree provides detailed regulation within the framework of the eIDAS Regulation on how the digital archiving process is performed. When receiving the document, the trust service provider must first verify the advanced electronic signature on the document and place its timestamp on it. The service provider must not access the content of the document without prior authorization by the principal and must continuously provide access to the document for the principal. Specific and detailed provisions are established for qualified trust service providers and their services.

e. Are there any sector-specific requirements and rules for digital archiving [e.g., archiving both the software and the related data to retrieve information in the financial sector]?

The ITM Decree excludes its applicability from digital archiving of governmental or local governmental bodies, and organizations performing public duties. With the *Gov. Decree no 466/2017 (XII. 28.*) the government established the Governmental Data Vault which archives data and documents that have been issued in connection with the provision of electronic administration by organizations that are required to allow for electronic administration. The purpose of archiving is to enable data processors (i.e., the organizations that are obliged to archive their data) to rebuild their information systems in case of operational disturbances and to prevent the loss of data.

Regarding the operation of businesses and organizations outside the governmental sphere, there are a number of different requirements for archiving (e.g., invoices, accounting documents, employment documents, financial documentations, etc.), however, specific requirements for digital archiving are rare to be found. The laws and regulations prescribing the retention obligations usually only stipulate the obligation itself, and the means of how to achieve it are left to the obliged person to ensure, who can carry out the digital archiving by adhering to the provisions of the EATS Act and the ITM Decree.

As an example, Section 78 of *Act no CL of 2017 on the Rules of Taxation* prescribes that the tax subject must preserve invoices for five years, but it does not stipulate that it must be done in paper form or electronically. The only requirement regarding digital archiving is that if the tax authority asks for invoices archived digitally, the tax subject must provide them to the authority in electronic form.

A very specific retention obligation is set by *Act no CLV of 1997 on Consumer Protection*, which establishes that any complaints made via telephone or electronic communications network must be attached with an individual ID number and must be retained for three years, or – in some cases – five years for complaints made via telephone. Again, the act does not *define how exactly to archive the complaints, but it does require the business operating the* customer service to store the electronic copy of the documents in a way that it could give it out to the consumer or demonstrate compliance with the consumer protection authority. Another example is that of accommodation services (hotels, apartments, etc.) that previously had to keep a record of their guests' data, such as name, period of stay, and ID card number, on paper and provide it to the relevant authority by established periods. From 2021, all accommodation services in Hungary must record the necessary data on a digital platform provided by the touristic authority, to which access is available only to the accommodation service and the touristic authority. The accommodation service must use software to record the data provided and authorized by the touristic authority.

A more extensive data retention obligation is prescribed by Section 159/A of *Act no C of 2003 on Electronic Communications for electronic communication operators* (e.g., internet service providers), where such operators must preserve a large category of service data for one, or in some cases half a year for law enforcement, national security or national defense purposes, and must make such data available to the relevant authorities upon request. The use of data processors is subject to further regulations and the electronic communication operator must not use data processors or store the data outside the European Economic Area.

Adam Liber
Partner
liber.adam@provaris.hu
+36 20 524 4959

Tamas Bereczki
Partner
bereczki.tamas@provaris.hu
+36 30 220 2428

provaris
VARGA & PARTNERS

STRATULAT ALBULESCU
ATTORNEYS AT LAW

CEE LEGAL MATTERS COMPARATIVE LEGAL GUIDE: TMT 2022

MOLDOVA

Sabina Cerbu
Partner
scerbu@saa.ro
+373 78 888 876

CEE
Legal Matters

1. Legal framework for writing and electronic contracts

a. What are the requirements in your jurisdiction to consider a document to be in writing? Are there any formal/technical requirements?

According to Article 321 (Written form of a legal act) of the *Civil Code of the Republic of Moldova*, a written document is a document on which a signature is applied. If according to the law or by the parties' agreement a legal document must be concluded in writing, it may be concluded by drafting a single document on which the parties apply their signatures; this may be achieved via an exchange of letters, telegrams, electronic documents signed by the party who sends the same.

A written document may be validly concluded in an electronic form only if it is signed with an advanced qualified signature of the party(ies) who concludes (conclude) the document, and if the parties or the law do not require other types of an electronic signature to be applied, as per Article 318 (Electronic form of a legal act) of the *Civil Code of the Republic of Moldova*. At the same time, *Law no. 124/2022 on electronic identification and trusted services* (which shall enter into force on December 10, 2022) gives a definition of an electronic document, which represents content in electronic form, in particular text form or sound, visual or audio-visual recording on which was applied an electronic signature or an electronic seal. The *Civil code* uses the phrase "qualified advanced signature" which was used in the former electronic documents *Law no. 91/2014*, currently repealed. We expect that in near future the *Civil Code* will be revised to reflect the terms used in *Law no. 124/2022*, i.e., "qualified signature".

b. Are electronic documents [e.g., an email] per se considered to be in writing under your law?

A document in electronic form, generally, would be considered as being provided in writing only if it meets all requirements prescribed by the law. As mentioned above in p.1 (a) the electronic documents must be signed with an advanced qualified signature of the party(ies) who concludes (conclude) the document, and if the parties or the law do not require other types of an electronic signature to be applied, as per Article 318 (Electronic form of a legal act) of the *Civil Code of the Republic of Moldova*. Thus, an email would not be considered per se a document in writing under Moldovan legislation unless it is signed using an advanced qualified signature (see our notes under p. 1 (a) above).

c. What probative power paper and/or electronic documents have that are to be considered in writing?

A paper document must be signed using a holographic signature (hand signature) to produce legal effects.

An electronic document is equaled according to its probative value with written evidence or material means of evidence and cannot be rejected as evidence only for the reason that it is concluded in an electronic form.

As mentioned, an electronic document signed with a qualified electronic signature is assimilated, as to its effects, with a similar document on paper, signed with a holographic signature.

An electronic document signed with a different type of electronic signature than the qualified signature is assimilated, according to its effects, with a similar document on paper, signed with a holographic signature, only in specifically regulated situations by the law, or based on an agreement of the parties related to the application of electronic signatures and seals, provided they include provisions on the verification of the electronic signature and confidentiality and liability obligations for the parties.

d. What are the general rules and requirements to conclude a contract electronically?

According to Moldovan legislation, an electronic contract is not a particular type of contract; the use of an electronic form may concern the form of the contract or the modality in which the contract is concluded (i.e., by electronic means).

A contract in electronic form must comply with all the above-mentioned requirements prescribed for an electronic document.

As to contracts concluded via electronic means, Article 319 of the *Civil Code of the Republic of Moldova* sets out that legal acts may be concluded via any electronic means. However, if a party to the contract does not use an advanced qualified electronic signature (i.e., a qualified electronic signature under *Law no. 124/2022*) to sign a contract, the party's consent is presumed to be valid until that party challenges her consent. This rule will benefit e-commerce, where legal acts concluded through electronic means, where the party is not applying an electronic signature, are commonly used.

Additionally, to boost e-commerce, *Civil Code* has also regulated the concept of distance contracts (Article 1013), which are any contract negotiated and concluded between a professional and a consumer within a remote sales or service provision system, without a simultaneous presence of the professional and the consumer, using exclusively one or more remote communication means before and at the time of contract conclu-

sion, including any order made by the consumer which would produce binding effects on them.

Law no. 284/2004 on electronic commerce adds that contracts concluded by electronic means complying with the requirements of the Moldovan *Civil Code* are equivalent to the written contracts signed by the parties by hand (Article 24).

e. Are there any sector-specific rules that define further requirements to conclude contracts electronically [e.g., contracting via an authenticated electronic channel, contracting via video chat, etc.]?

Generally, there are no specific requirements in addition to those mentioned above. The law contemplates the entry into contracts in electronic form using various communication means such as e-mails, text messages, or other authenticated electronic channels. These types of contracts include those usually concluded with consumers by micro-finance companies offering small loans, or in e-commerce.

Specific requirements are mostly related to the extent and content of the information related to these contracts, where the professional shall make the information available to the consumer in a form appropriate to the communication means used for entry into the contract, using clear and intelligible language.

Under Moldovan legislation, distance contracts may be also concluded via phone call, e.g., a professional may call the consumer in order to conclude a contract. In this case, the professional's representative must introduce the professional at the beginning of the conversation and specify the commercial scope of the call. During the call, the representative of the professional shall confirm the offer presented to the consumer, whose commitment begins only after he has signed the offer or sent his consent in writing. These confirmations must meet the requirements of durable media.

Article 1020 of the *Civil Code* prescribes that if the agreement is to be concluded through electronic means, the professional is required, before the other party makes a bid or accepts an offer, to provide information on the following: **(i)** the technical steps to be taken to enter into the agreement; **(ii)** if the professional will generate a document representing the agreement and if the document would be accessible (i.e., to the parties); **(iii)** the technical means for identifying and reviewing errors in entering the data before the other party makes a bid or accepts an offer; **(iv)** the language in which the agreement may be concluded; and **(v)** all contractual clauses. Concerning the last obligation, the professional shall ensure that the contractual clauses are available in textual form.

2. Digital signatures

a. Are there any laws regulating the use of digital signatures in your jurisdiction?

Particular regulations related to electronic signatures have been since 2014 with the adoption of *Law no. 91/2014* on electronic signature and electronic documents. This law has been recently abrogated with the adoption of a new *Law no. 124/2022 on electronic identification and trusted services* (already mentioned above). This law shall enter into force on December 10, 2022.

b. Is there any difference between the different types of digital signatures in your jurisdiction?

Law no. 124/2022 on electronic identification and trusted services regulates two types of electronic signatures, i.e., advanced and qualified electronic signatures. *Law no. 124/2022* sets out different requirements for each type of signature and restrictions when a certain or another type of signature might be applied.

An electronic signature is considered advanced subject to meeting the requirements set out by the law, i.e., **(i)** the signature refers exclusively to the holder; **(ii)** the signature allows the identification of the holder; **(iii)** the signature is created using electronic signature creation data, which the signatory is able to use with an enhanced level of confidence, under their sole control; and **(iv)** the signature is linked to the data to which they relate in such a way that any subsequent changes to such data may be detected.

In respect to qualified electronic signatures, they also shall meet a few requirements mandatory under the law as follows: **(i)** rely on a qualified public key certificate issued by a qualified trust service provider; and **(ii)** are created by an electronic signature device and are verified by means of the electronic signature verification device and/or product, which comply with the requirements of the law. Specific requirements are laid down in relation to qualified certificates as well, which must include **(i)** a machine-readable mention that the certificate is issued as a qualified certificate for electronic signatures; **(ii)** the issuing trust services provider identification data; **(iii)** signatory identification data; **(iv)** validation data for the electronic signatures matching the signatures creation data; **(v)** date and hour when the certificate becomes valid and ceases to be valid, respectively; **(vi)** sole registration number of the certificate; **(vii)** verification data for the certificate matching the certificate creation data; and **(viii)** the qualified electronic signature of the issuing trust services provider.

As mentioned, there are certain limitations in using advanced electronic signatures, and the law prescribes it exhaustively. Thus, advanced electronic signatures may not be applied on **(i)** electronic documents comprising information classified as a state secret, except that it may be allowed to sign electronic documents comprising information classified as state secret

only with an advanced electronic signature by the person whose identity and quality constitutes a state secret, under *Law no. 245/2008 on state secret*, where such a person works for the Intelligence and Security Service, the National Anticorruption Center, and the Ministry of Internal Affairs within their system of electronic documents circulation; **(ii)** on electronic documents issued in legal relationships between public institutions and natural persons and non-public legal entities.

c. What probative power each type of digital signature has in your country?

Electronic signatures, regardless of their degree of protection (i.e., advanced or qualified), produce legal effects and are accepted as evidence including in judicial proceedings, even if: **(i)** they are presented in electronic form; or **(ii)** they do not rely on a certificate issued by a trust services provider; or **(iii)** do not rely on a qualified public key certificate; or **(iv)** are not created by means of a creating electronic signatures device.

A qualified signature has a stronger probative power, as it is stated expressly by *Law no. 124/2022* where it has the same legal value as a holographic signature. Qualified electronic signatures enjoy the legal presumption of integrity and correctness of the origin of the data to which they refer.

d. Are there any specific groups of people that are required to have digital signatures [e.g., attorneys, notaries, government officials, etc.]?

There are no specific groups of people that are mandated to have or use digital signatures. The use of electronic signatures is not yet mandated in Moldova, generally.

Attorneys, notaries, or bailiffs may rely on electronic signatures to ease certain processes (to fill a request in court, to request official information from public authorities, or for reporting purposes, etc.), or to have access to public electronic services. Some governmental officials use electronic signatures to sign annual declarations on wealth and personal interests; electronic documents within the internal and intra-institutional circulation of documents (within their respective public entities); or administrative procedures in response to electronic petitions, etc.

e. Are non-personalized digital stamps recognized in your country with probative power [e.g., digital stamps used by companies, government, or administrative bodies]?

Law no. 124/2022 on electronic identification and trusted services regulates electronic time stamps for the first time in Moldova. Qualified electronic time stamps are issued by trust services providers and meet the following requirements: **(i)** provides a connection between the date and hour and other dates excluding in a reasonable manner the risk to alter the data without detection; **(ii)** rely on a time source that is accurate and is connected to the universal time; **(iii)** rely on the qualified electronic signature or seal of the trust services provider or on the advanced electronic signature or seal of the trust services provider headquartered in another country, which benefits from the recognition procedure set out in *Law no. 124/2022*. Requirements for advanced electronic time stamps are set out by trust services providers.

Electronic time stamps shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements of the qualified electronic time stamp. At the same time, a qualified electronic time stamp shall enjoy the presumption of the accuracy of the date and the time it indicates and the integrity of the data to which the date and time are bound.

Moldovan law also regulates the use of electronic seals in a similar manner to electronic signatures; our notes in Sections 2.b. and 2.c. in relation to the requirements and probative power of advanced and qualified electronic signatures apply mutatis mutandis to advanced and qualified electronic seals.

3. Digital archiving

a. Are there any laws regulating digital archives and digital archiving in your jurisdiction?

Moldova is in the yearly stages of digitalizing its national archives. So far, there are very few regulations on digital archives.

Law no. 124/2022 defines secured electronic archiving as a structured repository of electronic documents ensuring the confidentiality, non-repudiation, and integrity of the documents and guarantees the probatory value of the electronic documents over time. *Law no. 124/2022* includes further provisions on the evidence of electronic documents (Article 49) and on the storage of electronic documents (Article 50), where entities that rely on the electronic circulation of documents are obliged to keep the originals of electronic documents in a way that allows verification of their authenticity. Please see the definition of electronic documents in Section 1.

The retention terms for electronic documents are identical to the retention terms for paper documents. Electronic documents are archived in digital archives. The Government shall establish the categories of electronic documents for storage in secured digital archives. As mentioned above, *Law no. 124/2022 on electronic identification and trusted services* shall enter into force by December 2022, the secondary regulation is yet to be drafted and approved by the Government, inclusively those related to digital archives, and categories of electron-

ic documents mandatory to be archived in secured digital archives.

b. What are the main legal and technical requirements to digitally archive documents?

Not yet available.

c. Is there any difference in your country's regulations between the digital archiving of paper and electronic documents?

Apart from retention periods for documents, which are the same irrespective of whether the documents are in paper or in electronic form, we expect that there would be different regulations for the digital archiving of paper and electronic documents, respectively. As for paper documents, there are special regulations (albeit old) such as *Law no. 880/1992 on Archival Fund of the Republic of Moldova*, and *Order no. 57/2016 of the State Service of Archives on indicator of standard documents and deadlines of their storage for public administration bodies, institutions, organizations and enterprises of the Republic of Moldova and the instruction on the application of the indicator*. At the same time, a draft of a Government Decision on approving the Concept of an informational system Electronic Archive (e-Archive) is currently under public discussion.

With respect to digital archives, the Government shall regulate secondary regulations under *Law no. 124/2022*, and amend other relevant regulations.

d. Is any third party required to participate in the process of digital archiving in your country [e.g., a trusted service provider, government / administrative bodies, etc.]?

Not yet available.

e. Are there any sector-specific requirements and rules for digital archiving [e.g., archiving both the software and the related data to retrieve information in the financial sector]?

There are no sector-specific requirements and rules for digital archiving (as *Law no.124/2022* has yet to enter into force, and respectively secondary regulations are to be drafted). The legal framework allows electronically archiving documents more as an additional option to paper document archives. And, the professionals (such as notaries, bailiffs, attorneys, etc.) are obliged by general rules to ensure integrity, security of data, confidentiality of information, etc.

For example, reporting entities under anti-money laundering rules are obliged to keep and store electronically all the data on suspected transactions for five years. As for electronic archives, they shall be kept under safe conditions and operative availability, to be sufficient to allow the reconstruction of each activity or transaction in such a way as to serve afterward as evidence in criminal, contravention, and other legal proceedings.

Sabina Cerbu
Partner
scerbu@saa.ro
+373 78 888 876

STRATULAT ALBULESCU
ATTORNEYS AT LAW

CEE LEGAL MATTERS COMPARATIVE LEGAL GUIDE: TMT 2022

POLAND

Xawery Konarski
Senior Partner
xawery.konarski@traple.pl
+48 22 850 10 10

Piotr Wasilewski
Partner
piotr.wasilewski@tralple.pl
+48 12 426 05 30

Anna Jelinska-Sabatowska
Managing Associate
anna.jelinska@traple.pl
+48 22 850 10 10

CEE
LEGAL MATTERS

www.ceelegalmatters.com

1. Legal framework for writing and electronic contracts

a. What are the requirements in your jurisdiction to consider a document to be in writing? Are there any formal/technical requirements?

In Polish procedure, the form and validity requirements for documents are governed by the *Polish Civil Code*. For a document to be recognized as having been drawn up in writing, it must contain a handwritten signature on the document covering the content of the declaration of intent. It is, therefore, not required that the document be handwritten in its entirety. A handwritten signature is one that makes it possible to identify the person who affixed it. At the same time, for people whose state of health does not allow for a handwritten signature, the legislator has provided for another form of signature, i.e., an ink fingerprint of the person making the declaration of will, or a signature by a person authorized to do so, with a note that it was made at the request of the person making the declaration of will, whereby the signature must be certified by a notary public or another person authorized to do so. Due to the necessity for the signature to be handwritten, a scan of the signature (printed along with the declaration of intent) or a facsimile will not be recognized as such. The ascertainment of the handwriting of the signature is not prevented by the form in which the signature is affixed. Currently, the possibility to sign with a tablet (which allows the natural movement of the hand of the person making the declaration of will to be reproduced) is noticeable in business transactions and in the literature. While recognizing such a form of a handwritten signature as a proper one, one should note the possibility to recognize as a handwritten signature also a signature made with the use of a touchpad in a laptop, provided that the signature is made with the use of a stylus (or any other device ensuring the highest possible accuracy of the signature. On the other hand, it is doubtful that a signature made using a computer mouse can be considered a handwritten signature, due to technical aspects and accuracy. A handwritten signature cannot be described as a handwritten signature if it was made with the use of software interfering with the mapping of the hand movement of the person making the declaration of will (for example, by rounding off the drawn characters). It should be borne in mind, however, that where the legislator requires a form higher than the written form, for technical reasons (the necessity for the notary to use an official seal with the image of an eagle) the use of such a form of a signature may be questioned.

b. Are electronic documents [e.g., an email] per se considered to be in writing under your law?

The above-mentioned methods of affixing a handwritten signature by means of electronic devices are part of the written form, not part of the electronic form. However, this is not reflected in the validity of the document as the legislator in Article 781 of the *Civil Code* has given the electronic form the same power as the written form. However, it should be noted that the legislator's understanding of electronic form differs from the colloquial one. A document filed in the form of an email, although undoubtedly electronically structured, will be noted as a documentary form, considered to be the least stringent form. In Article 772 of the *Civil Code*, the legislator defined the requirements of the documentary form, stating that it must make it possible to identify the person making the declaration. In the following article, it also emphasized that this form must also allow the content of the declaration of intent to be reconstructed. Thus, it can be a text message as well as an email or a completed web form. This is the form in which most contracts are concluded, including those noting the seller-consumer relationship. However, it should be borne in mind that unless the legislator provides otherwise, it is up to the parties to the contract to decide on the form in which it will be concluded. The choice of form is binding and carries certain consequences, such as the necessity to maintain a given form in the event of changes to the document. Thus, if the contract has been concluded in written form or is required by the Polish legislator, it will not be possible to amend the contract by means of the documentary form, unless it meets the requirements of the higher form. For a contract drawn up electronically to have the force equivalent to the written form, it must be signed with a qualified electronic signature. Such a signature, according to the eIDAS Regulation (*Regulation 910/2014 of the European Parliament and of the Council*), must be made using a qualified device and which is based on a qualified electronic signature certificate issued by an authorized provider. In Poland, there are currently no provisions that would stipulate the invalidity of a legal act in the event of failure to comply with the electronic form.

c. What probative power paper and/or electronic documents have that are to be considered in writing?

As mentioned above, a distinction must be made between the two forms of contract – the agreement in a written document form and the agreement in an electronic form. Where a written or electronic form is reserved for evidentiary purposes, a contract drawn up in the form of a document may have negative consequences in terms of its evidentiary value. The *Civil Code* sets certain limitations in this respect. If the written form was reserved only for evidentiary purposes, evidence from witnesses becomes inadmissible if a specific form was not observed, except for a situation when both parties agreed to it, it is demanded by a consumer in a dispute with a trader, or the fact of an action is substantiated by a document. Such a document may be, for example, a letter, a proof of payment, or a text message. Obviously, failure to observe a specific

form, which was reserved exclusively for evidentiary purposes, does not render the agreement invalid. Importantly, in the case of contracts concluded between entrepreneurs, failure to observe a specific form, including the written form, does not result in evidentiary limitations. This is due to the nature of business dealings, which is undoubtedly dynamic and requires both parties to the dealings to be on an equal footing.

d. What are the general rules and requirements to conclude a contract electronically?

In order to conclude a contract electronically (in documentary form), all the conditions required for documentary form must be met. This means that it must meet two prerequisites: it shall be in a fixed form that allows the declaration of intent to be reproduced and it shall note the identification of the person making the declaration of intent. When entering this type of contract, it should be noted that if the identity of the person making the declaration of will is not undisputed, it requires proof. This is because in Polish legislation there is no legal presumption of the authenticity of a document. However, the fact that a document was sent, for example, from a given email address does not mean that it was sent by a specific person. This is because there is a risk that the phone or account of a given user has been intercepted. This means that such a factual presumption can be overturned. Nevertheless, any form of contract that fulfills the above-mentioned prerequisites shall be deemed valid, unless otherwise provided by law.

Of course, a contract can also be concluded via the means of electronic communication and still be equivalent to a contract concluded in writing – if it has been signed with a qualified electronic signature (as explained above).

e. Are there any sector-specific rules that define further requirements to conclude contracts electronically [e.g., contracting via an authenticated electronic channel, contracting via video chat, etc.]?

There are no such sector-specific rules but there are regulations concerning specific types of contracts. For example, the sale or lease of an enterprise should be made in writing with signatures certified by a notary and the agreement obliging to transfer the ownership of the real estate should be concluded in the form of a notarial deed. Some contracts have to be concluded in written form, under pain of nullity – these are for example contracts limiting an agent's activities of a competitive nature for the period after the termination of the agency contract or contracts on the transfer of proprietary copyrights.

2. Digital signatures

a. Are there any laws regulating the use of digital signatures in your jurisdiction?

As already mentioned, the use of digital signatures in business transactions is mainly determined by the *Civil Code* when it concludes contracts. The procedural framework related to the activity of qualified certificate providers is determined by the *Act of September 5, 2016, on trust services and electronic identification* together with the aforementioned eIDAS Regulation. The trusted profile, which is a publicly accessible advanced electronic signature, is regulated by the *Regulation of the Minister of Digitalization of June 29, 2020*, on trusted profiles and trusted signatures. This regulation governs related to the issuance, extension, and cancellation of a Trusted Profile, as well as the conditions for signing with it.

b. Is there any difference between the different types of digital signatures in your jurisdiction?

Yes, the eIDAS regulation recognizes three types of digital signatures, namely the previously mentioned advanced electronic signature and qualified electronic signature, as well as the least reliable, equivalent under Polish law to an ordinary document form, ordinary electronic signature. Each of them is characterized by a different level of reliability, from the least reliable simple signature to the most reliable qualified signature. A simple signature contains only data in electronic form, which are attached to or logically linked with other data in electronic form (e.g., the content of an e-mail) and which are used by the signatory as a signature. Such a signature may therefore take the form of, for example, a name placed underneath the message. An advanced electronic signature, on the other hand, must meet several requirements, still more lenient than a qualified digital signature, but precise enough to allow theidentification of the person using such a signature. Such a signature must be uniquely attributed to the signatory, be capable of establishing the signatory's identity, be created with data that the signatory can use with a high degree of certainty under his own control, and be linked to the data in such a way that any subsequent change is recognizable. The conditions for such a signature are fulfilled by the Trusted Profile, which is mainly used via the government platform EPUAP and is used to confirm one's identity in contacts with public administration. It should be noted that despite the increased authenticity, where the legislator requires the use of a written or electronic form, it will be necessary to obtain a qualified electronic signature. Such a signature must be created using a qualified device, based on a qualified certificate, which is issued by an institution authorized by the supervisory authority.

c. What probative power each type of digital signature has in your country?

The probative power of an advanced and qualified digital signature is analogous to that of an electronic form.

d. Are there any specific groups of people that are required to have digital signatures [e.g., attorneys, notaries, government officials, etc.]?

There is no general obligation to have an electronic signature for a specific professional group. The exceptions are certain entrepreneurs and accounting offices, as well as, for example, MDs. However, this obligation does not derive from a specific regulation, but from the need to use systems that require a digital signature to authenticate identity. Entrepreneurs who are commercial law companies, as well as, for example, associations and foundations, are obliged to note the information on beneficial owners in the Central Register of Beneficial Owners, which requires a digital signature to accompany the notification. MDs, on the other hand, must have a digital signature, or a certificate issued by the Social Insurance Institution confirming their identity, to authenticate their identity when preparing the Electronic Medical Record.

e. Are non-personalized digital stamps recognized in your country with probative power [e.g., digital stamps used by companies, government, or administrative bodies]?

Electronic seals, once the relevant requirements – similar to those for signatures – have been met, are recognized as valid, analogous to signatures.

3. Digital archiving

a. Are there any laws regulating digital archives and digital archiving in your jurisdiction?

There is no general regulation mandating the digital archiving of documents. However, there are several industries that are introducing electronic document filing systems. Digital circulation and archiving of documents have been introduced, among others, between payers and the tax office (tax forms submitted to the tax office) and in the health care system, through the introduction of the Electronic Medical Records system. Changes for entrepreneurs related to the obligation to keep accounting records will come into force between 2024 and 2026.

b. What are the main legal and technical requirements to digitally archive documents?

There are no special requirements related to the above obligation except for the need for a digital signature (or a special certificate issued by a Social Insurance Institution in the case of MDs) for digital-only documents and the standard requirements related to the launch of the above systems.

c. Is there any difference in your country's regulations between the digital archiving of paper and electronic documents?

In the case of digital archiving of paper documents, if they have handwritten signatures, copies of the originals should be archived as well. It should also be ensured that access to electronic-only documents is as free as it is. in the case of traditional archives and ensure that they can be printed when needed (e.g., in case of an audit).

d. Is any third party required to participate in the process of digital archiving in your country [e.g., a trusted service provider, government / administrative bodies, etc.]?

There are no such requirements.

e. Are there any sector-specific requirements and rules for digital archiving [e.g., archiving both the software and the related data to retrieve information in the financial sector]?

No such sector-specific requirements.

Xawery Konarski
Senior Partner
xawery.konarski@traple.pl
+48 22 850 10 10

Piotr Wasilewski
Partner
piotr.wasilewski@tralple.pl
+48 12 426 05 30

Anna Jelinska-Sabatowska
Managing Associate
anna.jelinska@traple.pl
+48 22 850 10 10

CEE LEGAL MATTERS COMPARATIVE LEGAL GUIDE: TMT 2022

ROMANIA

Adina Chilim-Dumitriu
Partner
adina.chilim-dumitriu@nndkp.ro
+40 21 201 1200

Alina Boureanu
Managing Associate
alina.boureanu@nndkp.ro
+40 21 201 1200

Madalina Vasile Bucur
Senior Associate
madalina.vasile@nndkp.ro
+40 21 201 1200

CEE LEGAL MATTERS

www.ceelegalmatters.com

1. Legal framework for writing and electronic contracts

a. What are the requirements in your jurisdiction to consider a document to be in writing? Are there any formal/technical requirements?

In a broad sense, a document in writing (Tr. *inscris*) is any writing or other record that includes data about a legal act or fact, regardless of its form or the method of preservation and storage.

However, when the law specifically requires the written form of a legal act (e.g., the written form of a contract), for *ad probationem* or *ad validitatem* purposes, the legal act is considered to be in writing when it is under private signature or in authentic form (e.g., signed before a public notary).

The legal act under private signature is the one that bears the signature of a person, regardless of its form. Normally, it is not subject to a specific formality, apart from some exceptions expressly provided by law.

b. Are electronic documents [e.g., an email] per se considered to be in writing under your law?

The legal effects of electronic documents (Tr. *inscris in forma electronica*) are recognized by law, but not any electronic document has per se the same probative power as a document under a private signature.

Depending on the form of the electronic document (e.g., if it is signed by a person or the type of electronic signature associated with it), the electronic document may have the power of a document under private signature or be considered merely as incipient written evidence, which is not in itself sufficient for proving a legal act and needs to be supplemented by other evidence in case of legal proceedings (see Sections 1.c. and 1.d.).

c. What probative power paper and/or electronic documents have that are to be considered in writing?

The signature of a document (regardless of its form, e.g., paper or electronic form) attests, until proven otherwise, the existence of the consent of the person who signed it regarding its content. If the signature belongs to a public official, it gives authenticity to that document.

The written document under private signature, recognized by the one against whom it is invoked, or considered by law as recognized, as the case may be, serves as evidence between the parties until proven otherwise. The mentions in the written document under private signature that are directly linked to the legal relationship of the parties are also proof in the absence of any evidence to the contrary.

Particularly for electronic documents, *Law No. 455/2001 on electronic signatures* (Law No. 455/2001) provides that a document in electronic form is assimilated, as far as its conditions and effects are concerned, to a document under private signature, if an extended electronic signature has been incorporated, attached to or logically associated with it, based on a qualified certificate not suspended or revoked at the relevant time, and generated with the help of a secure electronic signature creation device (QES).

[QES is the equivalent of the "qualified electronic signature" defined by *EU Regulation No. 910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC* (eIDAS Regulation)].

Nevertheless, besides the above general rule laid down by Law No. 455/2001, there are special legal provisions applicable in specific domains (e.g., employment, relation with some public institutions) which assimilate the legal effect of the documents signed with an extended electronic signature (AdES) to that of documents under private signature.

[AdES is the equivalent of the "advanced electronic signature" defined by the eIDAS Regulation].

d. What are the general rules and requirements to conclude a contract electronically?

As a principle, most contracts can be concluded either in writing or verbally and still be binding upon the parties thereto. However, there are certain contracts that must have a written form in order to be considered as validly concluded (*ad validitatem*) or to be able to be proven in case of legal proceedings (*ad probationem*). Failure to observe the *ad validitatem* formality renders the respective legal operation invalid. While failure to observe the *ad probationem* formality will not affect the validity of the parties' agreement or the legal operation in itself, it will however make it impossible to produce evidence with respect to such contract in case of court proceedings.

If the written form of a contract is required by law in order to be able to prove the existence of the document or as a validity condition, concluding such a contract in an electronic form will be considered to satisfy the aforementioned requirement only if the contract has a QES attached. However, there are special legal provisions (e.g., regarding employment relationships) that derogate from the general rule and specifically recognize the signature of a document using an AdES, even when such documents should be concluded in writing.

When contracts are concluded by electronic means, the signature of the parties is valid if it is reproduced under the technical conditions provided by Law No. 455/2001.

The QES is presumed by Law No. 455/2001 as meeting the technical conditions required by law (laid down by Article 4 item 4 of Law No. 455/2001 and which are quite similar to the ones laid down by Article 26 of eIDAS Regulation). The party which does not recognize a QES must prove in Court that the technical conditions of Article 26 of eIDAS Regulation / Article 4 item 4 of Law No. 455/2001 have not been met.

By contrast, AdES is not presumed to meet the technical conditions provided by Article 26 of the eIDAS Regulation / Article 4 item 4 of Law No. 455/2001, and the party invoking an AdES before the Court must prove that the AdES complies with the technical conditions.

Finally, we note that electronic signatures produce their legal effects only when they are attached to a document in electronic form. Once an electronic document is signed with an electronic signature (either QES or AdES), it cannot be printed and signed by the other party using a handwritten signature.

e. Are there any sector-specific rules that define further requirements to conclude contracts electronically [e.g., contracting via an authenticated electronic channel, contracting via video chat, etc.]?

As mentioned before, if the written form of a contract is required by law for *ad validitatem* purposes (e.g., surety, mortgage, donation, mandate in certain cases) or *ad probationem* (e.g., transaction, deposit, legal assistance, insurance, commission, mandate in certain cases, lease for becoming executory title), the electronic contracts must be signed using a QES. Exceptions, when the AdES is recognized as having the same power as documents under private signature, are expressly provided by law.

For instance, from an employment law perspective, according to the most recent legal developments, the use of either AdES or QES has been officially recognized in employment relations for the conclusion, amendment, and termination of individual employment agreements, as well as for addenda and annexes thereof.

From the perspective of the relationship with public authorities and institutions, according to *Government Emergency Ordinance No. 38/2020 on the use of electronic documents at the level of public authorities and institutions* (GEO No. 38/2020), public authorities and institutions have the obligation **(a)** to receive documents signed with electronic signature and **(b)** to determine the type of electronic signature to be used for the service provided by those authorities which are available online.

The documents signed with an AdES, which are transmitted using substantial or high-level authentication mechanisms, are assimilated, in terms of their conditions and effects, to the documents signed under private signature. Consequently, in case of legal proceedings, the documents bearing an AdES, provided it is accepted by the respective public institution, will be considered evidence between the parties until proven otherwise.

2. Digital signatures

a. Are there any laws regulating the use of digital signatures in your jurisdiction?

Yes, assuming that by digital signature it is meant an electronic signature.

The main normative acts regulating electronic signatures are:

(a) *Law No. 455/2001 regarding electronic signature together with the Technical and Methodological Norms of 2001 for the application of Law No. 455/2001 regarding the electronic signature*; and

(b) *EU Regulation no. 910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.*

b. Is there any difference between the different types of digital signatures in your jurisdiction?

Yes, there are three types of electronic signatures recognized by eIDAS Regulation and by Law No. 455/2011. We note that Law No. 455/2011 is not fully aligned with the provisions of the eIDAS Regulation, and some definitions provided by Law No. 455/2001 may slightly differ from the ones provided by the eIDAS Regulation, without affecting however the essence of such definitions. Whereas the eIDAS Regulation is of direct applicability, we refer below to the definitions provided therein:

- (Simple) electronic signature (SES) is defined as data in an electronic form that is attached to or logically associated with other electronic data, and which is used by the signatory to sign.

An email signature or the signature given on certain signature pads has been qualified as a SES by certain authors.

- AdES is defined as an electronic signature that meets the following requirements: **(i)** it is uniquely linked to the signatory; **(ii)** it is capable of identifying the signatory; **(iii)** it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and **(iv)** it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.

Law No. 455/2001 refers to AdES as an "extended electronic signature."

- QES is defined as the extended electronic signature that is created by a qualified electronic signature creation device and which is based on a qualified certificate for electronic signatures.

Law No. 455/2001 refers to QES as an "extended electronic signature based on a qualified certificate."

c. What probative power each type of digital signature has in your country?

The legal effects and admissibility as evidence of the electronic signature differ between QES, on the one hand, and SES/AdES, on the other hand.

As regards QES, the eIDAS Regulation provides that its legal effect is equivalent to the legal effect of a handwritten signature, while Law No. 455/2001 provides that an electronic document that bears a QES is assimilated, in what concerns the conditions and its legal effects, to the document under private signature.

As regards AdES, the eIDAS Regulation does not define its legal effects, but grants a considerable leeway to EU member states in this respect, subject to the condition that EU Member States do not deny the legal effects of an electronic signature, or admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements for QES.

At the national level, contrary to the case of QES, Law No. 455/2001 does not recognize *ab initio* the documents signed with an AdES as a document signed under private signature, but admits its legal effects and accepts its admissibility as evidence in court, as follows:

- When the AdSE is not recognized by the party against whom it is invoked, the electronic document is to be regarded, in our opinion, as "incipient written evidence" (Romanian "*inceput de dovada scrisa*).

Within the meaning of the *Romanian Civil Procedure Code*, any written document (Tr. *inscris*), even unsigned and undated, that comes from a person against whom that written document is opposed to/presented or from the one whose successor in rights that person is, is considered an "incipient written evidence," if the writing makes the claimed fact credible. Incipient written evidence is not in itself sufficient for proving a legal act and needs to be supplemented by other evidence in case of legal proceedings (e.g., additional documents/correspondence, presumptions).

- When the AdSE is recognized by the party against whom it is invoked, the electronic document is considered to have, between the parties thereto, the same legal effect as for an authentic document (i.e., it provides full proof that it was signed under a private signature).

If one of the parties does not recognize the electronic document or the signature (regardless of the type of signature), the court must always order that the verification be done by specialized technical expertise. For this purpose, the expert or specialist must request qualified certificates, as well as any other documents necessary to identify the author of the document, the signatory, or the holder of the certificate.

The burden of proof differs between QES and AdSE. QES is presumed by Law No. 455/2001 as meeting the conditions provided by Article 26 of eIDAS Regulation / Article 4 item 4 of Law no. 455/2001, and therefore, the electronic documents bearing a QES will be considered evidence between the parties until proven otherwise. By contrast, AdES is not presumed to meet the above conditions, the party invoking the AdES before the court having the burden to prove AdES's compliance with such technical conditions.

d. Are there any specific groups of people that are required to have digital signatures [e.g., attorneys, notaries, government officials, etc.]?

The interaction with certain public authorities or institutions requires the mandatory use of electronic signatures. For instance, taxpayers (e.g., companies, associations, or other professionals) can interact with the fiscal authorities only by electronic means and are required to submit fiscal documents using an electronic signature.

e. Are non-personalized digital stamps recognized in your country with probative power [e.g., digital stamps used by companies, government, or administrative bodies]?

[We assume that by digital stamp it is understood electronic seal, as regulated by the eIDAS Regulation: "data in electronic form, which is attached to or logically associated with other data in an electronic form to ensure the latter's origin and integrity."]

Romanian law recognizes the legal effects of the electronic seals, their admissibility as evidence being similar to the one provided for the electronic signature. The qualified electronic seal guarantees the authenticity and integrity of a document issued by a legal person.

As laid down in the recitals to the eIDAS Regulation, when a transaction requires a qualified electronic seal from a legal person, a qualified electronic signature from the authorized representative of the legal person should be equally acceptable.

If the "non-personalized" electronic seal does not ensure certainty of the document's origin and integrity, it cannot serve as evidence that the electronic document was issued by the respective legal person.

3. Digital archiving

a. Are there any laws regulating digital archives and digital archiving in your jurisdiction?

Yes, as follows:

■ *Law No. 135/2007 on archiving documents in electronic form* (Electronic Archiving Law) establishes the legal regime applicable to the creation, preservation, consultation, and use of documents in electronic form archived or to be archived in an electronic archive.

■ *Order No. 493/2009 on the technical and methodological norms for the application of Law No. 135/2007 on archiving documents in electronic form* (Order No. 493/2009) lays down the procedure for granting, suspending, or withdrawing the accreditation of an electronic archive, as well as the conditions for carrying out this activity.

■ *Order No. 489/2009 on the methodological norms for the authorization of data centers* lays down the procedure and conditions for granting, suspending, and withdrawing data centers' authorizations, as well as the content, period of validity, and effects of the suspension or withdrawal of the authorizations.

■ *Law No. 16/1996 on the National Archives* (National Archives Law) and the supplementary legislation that provides rules shall also be observed when archiving documents in an electronic form.

b. What are the main legal and technical requirements to digitally archive documents?

According to the Electronic Archiving Law, any natural or legal person has the right to submit documents in electronic form for archiving within an electronic archive, under the conditions of the law.

The Electronic Archiving Law provides that the receipt of a document in electronic form in the electronic archive is subject to the fulfillment of the following requirements:

■ the person who holds the right to dispose of the document in electronic form (Holder) must sign the document with a QES [we note a discrepancy between the Electronic Archiving Law which refers to an "extended electronic signature" and Order No. 493/2009 which refers to QES; in practice, the competent authority (i.e., the Romanian Digitization Authority) considers that a QES must be attached]

■ the QES used by the Holder should be within its validity term

■ if the case, the encrypted document falling within the scope of the National Archives Law should be submitted together with the encryption and decryption key

■ the document should be submitted together with a set of minimum information expressly required under the Electronic Archiving Law.

The document in electronic form which meets the conditions laid down by the legislation shall be signed electronically by the electronic archive manager, with an electronic signature, which shall also certify that the document in question is an original or a copy, as determined by the Holder. The document in an electronic form identified as such shall be archived in the location determined by the electronic archive manager.

The electronic archive manager shall register and keep a record of all the documents submitted to the electronic archive, by keeping an electronic registry. Once registered, the content of the document cannot be modified. The electronic archive manager shall fill in an electronic file for each document, including details on the conditions of access to the document, as established by the Holder, which will be archived separately from the document.

The electronic archive manager has additional obligations, such as keeping the electronic archive in good condition, observing certain safety rules, ensuring the integrity, security, and confidentiality of the archived documents, keeping the source code of all programs used for the creation and operation of the electronic archive and submitting to the National Archives a copy of such source code, ensuring the destruction of any document upon the expiry of the archiving period, and ensuring financial resources to cover the damages that could be caused during the electronic archiving activities.

The applicable legislation provides additional requirements in respect of archiving documents in electronic form, for instance, as regards the accreditation of the electronic archive manager, the preservation and consultation of the electronic archive, and the data centers that store the electronic archives.

In respect of data centers that store electronic archives, such are subject to prior authorization by the competent authority. To receive such an authorization, the data center must prove it complies with a series of technical criteria that ensure: **(i)** the integrity and security of the electronic documents; **(ii)** the security and integrity of the space where the equipment storing the electronic archive is located; and **(iii)** the retrieval of information in case of natural disaster, according to the law.

c. Is there any difference in your country's regulations between the digital archiving of paper and electronic documents?

There is a requirement that if the document in electronic form was generated by transferring the information from analog

to digital media (i.e., scanned copy of the original paper), the following additional information will also be necessary for including the document in the electronic archives: references to the owner of the original, the location of the original, the transfer method used, and the hardware device and the computer program used.

d. Is any third party required to participate in the process of digital archiving in your country [e.g., a trusted service provider, government / administrative bodies, etc.]?

Yes, for instance:

- a Holder could use the services of a third-party entity acting as an electronic archive manager, in which context that entity would have several obligations as regards the archiving of documents in electronic form.
- the legislation provides several obligations that require the participation of the competent authority (i.e., the Romanian Digitization Authority) and of the National Archives.

We emphasize that the legislation sets forth obligations in relation to the (former) Ministry of Communication and Information Society as the competent authority. However, considering that the Romanian Digitization Authority has taken over the responsibilities of the (former) Ministry of Communication and Information Society, the obligations would now be interpreted as being in relation to the Romanian Digitization Authority.

e. Are there any sector-specific requirements and rules for digital archiving [e.g., archiving both the software and the related data to retrieve information in the financial sector]?

There could be some sector-specific requirements, for instance, in respect of classified documents, in which context an in-depth analysis of the requirements applicable in various sectors should be done.

Adina Chilim-Dumitriu
Partner
adina.chilim-dumitriu@nndkp.ro
+40 21 201 1200

Alina Boureanu
Managing Associate
alina.boureanu@nndkp.ro
+40 21 201 1200

Madalina Vasile Bucur
Senior Associate
madalina.vasile@nndkp.ro
+40 21 201 1200

ŽIVKOVIĆ|SAMARDŽIĆ

CEE LEGAL MATTERS COMPARATIVE LEGAL GUIDE: TMT 2022

SERBIA

Vesna Zivkovic
Associate
vesna.zivkovic@zslaw.rs
+381 11 2636 636

CEE
LEGAL MATTERS

www.ceelegalmatters.com

1. Legal framework for writing and electronic contracts

a. What are the requirements in your jurisdiction to consider a document to be in writing? Are there any formal/technical requirements?

In Serbia, the general rule is that contracts can be made informally. The *Code of Obligations* (*SFRY Official Gazette ns. 29/78, 39/85, 45/89 – decision CCY and 57/89, "Official Gazette SFY", No. 31/93, "Official Gazette SMG", No. 1/2003 – Constitutional Charter and "RS Official Gazette", No. 18/2020*) prescribes this principle and its divergence – when the law specifically envisages otherwise. That is, certain contracts, according to the law must be made in writing: surety contracts, contracts for construction, etc. Contracts lacking the prescribed form shall not have a legal effect.

There are certain technical requirements depending on the contract and prescribed form. When an obligatory written form of a contract is prescribed, a signature of the parties is also one of the elements/conditions to be fulfilled.

b. Are electronic documents [e.g., an email] per se considered to be in writing under your law?

According to the *Law on Electronic Document, Electronic Identification and Trust Services in Electronic Business* (*"Official Gazette of the RS", No 94/2017 and 52/21*) an electronic document shall not be denied legal effect, probative force, and written form solely on the grounds that it is in electronic form. However, this is possible in cases where it is explicitly provided that an electronic form may not be equalized with a written form.

The law further regulates the issue of what documents can be considered originals. Firstly, an electronic document that is originally created in electronic form shall be considered an original. The same applies to an electronic document that has the same digital signature as an original electronic document. A paper copy of an electronic document is made by printing the external form of the electronic document. Scans of a paper document are considered a copy of a paper document.

c. What probative power paper and/or electronic documents have that are to be considered in writing?

The probative power of paper documents depends on whether they are issued by a public body or a private person. If a public body issued a document, it shall be considered true and authentic. However, a party in litigation proceedings can claim otherwise and, if the court has doubts as to the authenticity of the document, the public body may be asked for a statement. If a document is made by a private person, its authenticity, if disputed, must be proven by the party who submitted it as evidence.

Electronic documents have the same probative power as paper documents. Nonetheless, practice regarding the use of electronic documents in court proceedings is scarce.

d. What are the general rules and requirements to conclude a contract electronically?

Electronic contracting in Serbia is regulated by the *Law on Electronic Commerce ("Official Gazette of the RS", Ns 41/2009, 95/2013 and 52/2019*).

There is a general principle that a contract can be concluded by electronic means i.e., in electronic form. An offer and acceptance can be given electronically – that is in electronic form. When an electronic message – electronic form – is used for the formation of a contract, such a contract cannot be denied a legal effect only because it has been made in an electronic form.

There are special requirements imposed on commercial subjects when offering their services and concluding a contract with consumers. Firstly, before the conclusion of a contract, they are obliged to provide information to the consumers on the procedure to be applied in the conclusion of the contract, contractual provisions, general terms and conditions if they are a constitutive part of the contract, languages, and codes of conduct. They must provide the technical means for the potential customer to recognize and correct any wrong input of data.

These requirements are also imposed on the contracting parties that are not consumers, but they can explicitly stipulate not to apply them.

These requirements are not imposed on electronic contracts concluded via email or other types of personal electronic communication.

The provider of goods or services is obliged to also make the text of the contract and general terms of conditions if they are a constituent part of the contract, available to the other contracting party so that they can be stored, used again, and reproduced.

e. Are there any sector-specific rules that define further requirements to conclude contracts electronically [e.g., contracting via an authenticated electronic channel, contracting via video chat, etc.]?

N/A

2. Digital signatures

a. Are there any laws regulating the use of digital signatures in your jurisdiction?

Electronic documents and electronic signatures in Serbia are regulated by the *Law on Electronic Document, Electronic Identification and Trust Services in Electronic Business* (*"Official Gazette of the RS", No 94/2017 and 52/21*) and a number of subordinate pieces of legislation governing these issues in more detail. The Serbian legislator took a technologically neutral position when it comes to the definition of digital signatures. It did not use that exact phrase in the law but introduced a broader phrase – the of a *qualified electronic signature* and prescribed further conditions to be met by a signature to be called a *qualified electronic signature*:

"*Qualified electronic signature means an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures, and which is issued by the provider of a qualified trust service in accordance with this law.*"

For the time being, these conditions are met only by digital signatures.

b. Is there any difference between the different types of digital signatures in your jurisdiction?

Serbian law does recognize different types of electronic signatures, considering the level of security they provide.

First, there are *electronic signatures*. The law prescribes that it shall not be denied a legal effect and probative force solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic signatures. This means that even a lower security level electronic signature shall be valid if it fulfills its purpose – if it is used in communication that does not require a high level of security.

Second, there are *advanced electronic signatures* that must meet the following requirements: 1) they must be uniquely linked to the signatory and/or the creator of the seal; 2) they are capable of identifying the signatory and/or the creator of the seal; 3) they are created using electronic signature/seal creation data that the signatory/creator of the seal can, with a high level of confidence, use under its sole control; 4) they are linked to electronically signed/sealed data in such a way that any subsequent change in the data is detectable. These signatures are more secure than simple electronic signatures.

Third, we have *qualified electronic signatures*, defined as advanced electronic signatures that are created by a qualified electronic signature creation device, are based on a qualified certificate for electronic signatures, and are issued by the provider of a qualified trust service in accordance with this law. This is the most secure signature for the time being, having in mind that the signatory uses a secure creation device and has their signature certified by a qualified trust service, the conditions for the operation of which are strictly prescribed by law. At this moment, these conditions are met by digital signatures.

c. What probative power each type of digital signature has in your country?

As already mentioned, electronic signatures shall not be denied probative power solely on the grounds that they are in an electronic form or that they do not meet the requirements for qualified electronic signatures. In the procedures where a handwritten signature is not required, an electronic signature shall suffice. However, when handwritten signatures are required, only qualified electronic signatures shall have the equivalent legal effect.

There are certain legal transactions that cannot be made in an electronic form and therefore electronic signatures shall not be used either.

d. Are there any specific groups of people that are required to have digital signatures [e.g., attorneys, notaries, government officials, etc.]?

No, there are no specific groups that are required to have a digital signature.

e. Are non-personalized digital stamps recognized in your country with probative power [e.g., digital stamps used by companies, government, or administrative bodies]?

For the time being it is not used in practice.

3. Digital archiving

a. Are there any laws regulating digital archives and digital archiving in your jurisdiction?

Yes. In Serbia, digital archives and digital archiving are regulated by *Law on Archival Material and Archival Activity* (*"RS Official Gazette, No 6/2020*) and *Law on Electronic Document, Electronic Identification and Trust Services in Electronic Business* (*"Official Gazette of the RS", No 94/2017 and 52/21*) and subordinate pieces of legislation to these laws.

b. What are the main legal and technical requirements to digitally archive documents?

Creators and holders of archival material and documents in electronic form are obliged to carry out procedures and activities related to the management of documents and to use information systems that guarantee the protection, authen-

ticity, trustworthiness, integrity, and usability of electronic documents.

As for the technical requirements, they are strictly prescribed by the *Decree on Unique Technical and Technological Requirements and Procedures for the Preservation and Protection of Archival Material and Documents in Electronic Form* (*RS Official Gazette Ns. 107/2021 and 94/2022*). However, the application of this decree has been postponed for 2024 because most of the participants in this procedure were not capable to meet the technical and technological requirements imposed.

c. Is there any difference in your country's regulations between the digital archiving of paper and electronic documents?

In principle, digital archiving of paper and electronic documents is regulated by the same law. The main principles, obligations, and duties of creators and holders of archival material and documents are the same for both archiving both types of documents. Nonetheless, special provisions regarding electronic archiving were inevitable due to the specificity of the technology used for this type of archiving.

On the other hand, our legislator makes a distinction between electronic archiving and qualified electronic archiving. Qualified electronic archiving relates to the keeping of documents that are signed with a qualified electronic signature and stamped with an electronic stamp and documents whose uniformity with the original document and correctness of additionally included information was confirmed by a qualified electronic signature or stamp. The technical and technological standards for this type of keeping are governed by the *Decree on the Procedures and Technological Solutions Used whilst Qualified Keeping of Documents* (*RS Official Gazette, 94/2018 and 87/2020*).

d. Is any third party required to participate in the process of digital archiving in your country [e.g., a trusted service provider, government / administrative bodies, etc.]?

N/A.

e. Are there any sector-specific requirements and rules for digital archiving [e.g., archiving both the software and the related data to retrieve information in the financial sector]?

N/A.

Vesna Zivkovic
Associate
vesna.zivkovic@zslaw.rs
+381 11 2636 636

ŽIVKOVIĆ|SAMARDŽIĆ

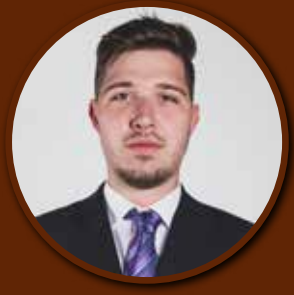
ULČAR & PARTNERJI

CEE LEGAL MATTERS COMPARATIVE LEGAL GUIDE: TMT 2022

SLOVENIA

Matjaz Ulcar
Managing Partner
matjaz@ulcar-op.si
+386 1 560 5300

Sara Oreski
Junior Associate
sara.oreski@ulcar-op.si
+386 1 560 5300



Simon Jancar
Junior Associate
Simon.Jancar@ulcar-op.si
+386 1 560 5300

CEE LEGAL MATTERS

www.ceelegalmatters.com

1. Legal framework for writing and electronic contracts

a. What are the requirements in your jurisdiction to consider a document to be in writing? Are there any formal/technical requirements?

In general, a document is considered to be in writing if it is drafted in a physical form (either typed or handwritten) if not stipulated otherwise.

Such definition is included in Article 76 of the *Criminal Procedure Act* (*Zakon o kazenskem postopku, Official Gazette of RS, No. 176/21 et seq.*), Article 63 of the *General Administrative Procedure Act* (*Zakon o splosnem upravnem postopku, Official Gazette of RS, No. 24/06 et seq.*) and in Article 105b of the *Civil Procedure Act* (*Zakon o pravdnem postopku, Official Gazette of RS, No. 73/07 et seq.*), pursuant to all of which a procedural submission is considered to be in writing if it is handwritten or typed and signed by either the author or the applicant.

Additionally, an electronic document is also considered to be in writing in the aforementioned procedures if it is signed with a secure electronic signature with a qualified digital certificate issued by the trusted provider (qualified signature).

b. Are electronic documents [e.g., an email] per se considered to be in writing under your law?

Pursuant to Article 13 paragraph 1 of the *Electronic Commerce and Electronic Signature Act* (*Zakon o elektronskem poslovanju in elektronskem podpisu, Official Gazette of RS, No. 57/00 et seq.* – Electronic Signature Act) electronic documents are considered to be in writing if the information contained therein is accessible so as to be usable for subsequent reference. This means that the document can be made available to the parties concerned (e.g., downloadable, sent, etc.) and that the parties are able to create additional copies of the document. Similarly, pursuant to Article 16 of the *Civil Procedure Act* electronic documents have the same probative value as written documents in physical form if they are appropriate for processing (i.e., made available by technical means that the court itself employs).

Furthermore, according to Article 4 of the Electronic Signature Act, as well as according to Article 46 of *Regulation (EU) no. 910/2014 of the European Parliament and of the Council* (eIDAS Regulation), an electronic document shall not be denied legal effect and admissibility as evidence in legal procedures solely on the grounds of being in electronic form.

According to case law (decision of Higher Court in Celje, *Ref. No. Cp 294/2019*) a contract concluded in writing and thus requiring a termination to be in the same form may be validly terminated with a written statement sent via an email. All of the above showcases a rather broad interpretation of a written form for legal documents.

However, there are certain exceptions. Rules from Article 13 Paragraph 1 of the Electronic Signature Act do not apply for documents, attesting to individual legal transactions, subject to special formal requirements, such as land registry permits that transfer the ownership right over real estate or that establish other property rights, and testamentary transactions. An electronic form of land registry permission represents an equivalent to the written form and has the same legal effect if the signature of the person who issued it is notarized.

c. What probative power paper and/or electronic documents have that are to be considered in writing?

The probative power, i.e., the degree of value as evidence, of paper documents and electronic documents that are to be considered in writing depends on the nature of the contract or legal transaction that certain documents attest to.

While a written document is sufficient for the majority of documents, as already described above, there are certain dispositions that are subject to stricter formal requirements. While for the majority of contracts written form is merely of probative value and therefore less formal (*forma ad probationem*), there are others, for which written or special form is required in order for the contract to be valid (*forma ad valorem*). In certain cases, an ordinary written form is not sufficient, and the contracts have to be either notarized or concluded in a form of a notary deed, to be valid (for example, the sale of real estate needs to be notarized, share purchase agreements need to be concluded in the form of a notary deed, etc.). Testamentary dispositions are also subject to special requirements and are considered valid, if they are drafted in writing and signed in front of witnesses, before a court or a notary public, or if they are handwritten and signed by an intestate. Technically it does not matter where the testament is written, the only requirement is that it is in a physical (not electronic) form and signed by the intestate. In the case of a handwritten testament, the copy of such a document is not considered to be in writing and valid, unless the purpose of a copy is to restore the original document.

d. What are the general rules and requirements to conclude a contract electronically?

As a rule, contracts can be concluded by electronic means, whereby it is important that **(i)** the signatories can be identified (the identification or authentication of signatories is executed via electronic signatures, further explained below) and that **(ii)** the integrity of the contract is preserved during its creation and conservation.

Additional rules for conducting business and concluding

contracts electronically depend on the nature of an individual contractual relationship.

For example, in the case of consumer contracts, the rules of Article 7 of the *Electronic Commerce Market Act* (*Official Gazette of RS, No. 96/09 et seq.*– ECMA) apply. A general requirement, stipulated in the aforementioned provision is, that contractual provisions and general terms of a contract are provided in a form, which allows for the saving and reproduction of contractual terms.

In the case of contracts that do not require a written form, the contract may very well be concluded via email or other forms of electronic communication. However, the *forma ad valorem* contracts ought to be concluded in a more formal manner, in accordance with the prescribed requirements.

e. Are there any sector-specific rules that define further requirements to conclude contracts electronically [e.g., contracting via an authenticated electronic channel, contracting via video chat, etc.]?

For most contracts, legislation has adopted a rather hands-off approach, when it comes to contract conclusion regulations. Unless specifically restricted, further authentication requirements are left for the parties to decide.

However, there are certain sector-specific instances, where the regulations provide additional requirements for the conclusion of electronic contracts, for example:

- Conclusion of car insurance – in accordance with Article 5 of the *Compulsory Motor Third-Party Liability Insurance Act* (*Official Gazette of RS, No. 93/07 et seq.*) the insurance company is required to conduct online business and enable insurance contract conclusion via the internet; although the government has the option to stipulate additional requirements for the authentication of such contracts, no such additional requirements have been issued yet and in practice, the authentication process is usually performed via a combination of e-mail and SMS (the draft of the contract is uploaded to a virtual folder by an insurance company and a link to the folder is sent to the customer, who can access the folder only by typing in a code, received previously via an SMS.

- Contracts in the form of notarial deeds – Article 31 of the *Notary Act* (*Zakon o notariatu, Official Gazette of RS, No. 2/07 et seq.*) foresees the possibility of a notarial document in an electronic form, which can be composed via a secure video call with the notary public; prior to the drafting of a notarial document via a video call, the notary public verifies the identity of participants in accordance with Article 39 of the *Notary Act*; notarial documents in electronic form have to be secured with a qualified electronic signature, qualified electronic seal and time stamp in such a way that the integrity of the data in the document is ensured and the time of the creation of the document is evident; additionally, the form of a notarial deed has to meet the conditions for secure and long-term storage of data in digital form, as determined by the regulations on the protection of documentary and archival material and archives. In accordance with Article 38 of the *Notary Act*, a notarial document in electronic form can be signed with a qualified digital signature of participants via a secure video call with a notary or in the physical presence of the notary. The notary verifies the validity of qualified electronic signatures and signs the document with their qualified electronic signature, qualified electronic seal, and qualified electronic stamp. The method of verification of the signatures has to be specified in the notarial document. In accordance with applicable provisions of the *Notary Act*, notarial documents in an electronic form have the same legal effect as notarial documents in a physical form.

2. Digital signatures

a. Are there any laws regulating the use of digital signatures in your jurisdiction?

In the Slovenian jurisdiction, digital signatures are regulated by the following legislation:

- *Electronic Identification and Trust Services Act* (*Zakon o elektronski identifikaciji in storitvah zaupanja, Official Gazette of RS, No. 121/21 et seq.* – Trust Services Act), which governs personal electronic identity, means of electronic identification, electronic identification scheme, and trust services, which include electronic signatures;

- *Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market* (eIDAS Regulation);

- *Electronic Business and Electronic Signature Act* (*Zakon o elektronskem poslovanju in elektronskem podpisu, Official Gazette of RS, No. 98/04 et seq.*), which governed the electronic signatures, but most of its provisions on electronic signatures were annulled with the adoption of the Trust Services Act;

- *Decree on the Determination of Means of Electronic Identification and the Use of a Central Service for Online Registration and Electronic Signature* (*Uredba o dolocitvi sredstev elektronske identifikacije in uporabi centralne storitve za spletno prijavo in elektronski podpis, Official Gazzete of RS, No. 29/22*).

The use of digital signatures is further regulated by various field-specific regulations, as the type of digital signature required for a particular legal act depends on the field of the legal act and thus, laws regulating relevant fields.

b. Is there any difference between the different types of digital signatures in your jurisdiction?

Electronic Signature Act which was adopted before the eIDAS Regulation entered into force, differentiated between:

- an "electronic signature" – a set of data in electronic form, which is contained, added, or logically connected with other data, with the purpose to verify the authenticity of this data and identify the signatory and
- a "secure electronic signature" – an electronic signature which is **(i)** exclusively related to the signatory, **(ii)** the signatory can be reliably identified from it, and **(iii)** is created with means for secure electronic signing, which are exclusively under the signer's control.

As mentioned above, the Trust Services Act annulled some of the Electronic Signature Act provisions, including the provisions on the differentiation between an electronic signature and a secure electronic signature.

Please note that the Trust Services Act does not define electronic signatures or different types of electronic signatures anymore, therefore the definitions of electronic signatures, as defined by the eIDAS Regulation now apply. In accordance with Article 3 of the eIDAS Regulation, there are three different types of digital signatures, namely:

- An "electronic signature" – data in electronic form which is attached to or logically associated with other data in electronic form, and which is used by the signatory to sign.

- An "advanced electronic signature" – an electronic signature that is uniquely linked to the signatory, capable of identifying the signatory, created using electronic signature creation data that the signatory can, with a high level of confidence, use under his control and is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.

- A "qualified electronic signature" – an advanced electronic signature that is created by a qualified electronic signature creation device, and is based on a qualified certificate for electronic signatures.

However, please note that even though Electronic Signature Act provisions on the differentiation between an electronic signature and a secure electronic signature are no longer valid, the term secure electronic signature is still heavily present in the Slovenian jurisdiction, since various laws, adopted prior to eIDAS Regulation's entry into force (and some even after it), still refer to the term "secure digital signature," for instance Article 63 of the *General Administrative Procedure Act*, Article 58 of the *Public Procurement in the Defence and Security Sector Act* (*"Zakon o javnem narocanju na podrocju obrambe in varnosti Official Gazzete of RS, No. 90/12 et seq.*), Article 13 of the *Legal Protection in Public Procurement Procedures Act* (*Zakon o pravnem varstvu v postopkih javnega narocanja, Official Gazzete of RS, No. 43/11, et seq.*), etc.

The Trust Services Act addresses the terminological discrepancy in Article 62, Paragraph 2, in which it stipulates that if the regulation requires the use of a secure electronic signature based on a qualified digital certificate, it is considered that a qualified electronic signature is required.

c. What probative power each type of digital signature has in your country?

The qualified electronic signature is considered an equivalent to a handwritten signature and is the most widely used electronic signature in Slovenia, considered the most reliable, while its authenticity is presumed. There are various recognized providers of qualified digital certificates in Slovenia, most notably *SIGOV-CA*, *SIGEN-CA*, and *POSTA®CA*. As for ordinary and advanced electronic signatures, the burden of proof lies with the person claiming the authenticity of such signatures.

The types of digital signatures, necessary for particular legal acts, depending on the field of such legal acts, and are subject to various field regulations, for example:

- Pursuant to Article 84, Paragraph 4 of the *Value Added Tax Act* (*Zakon o davku na dodano vrednost, Official Gazzete of RS, No. 13/11 et seq.*), an advanced signature is foreseen as a possible form to ensure the authenticity of the origin and the integrity of an electronic invoice.

- Pursuant to Article 37, Paragraph 11 of the *Public Procurement Act* (*Zakon o javnem narocanju, Official Gazzete of RS, No. 91/15 et seq.*) the use of an advanced electronic signature, based on a qualified certificate, is foreseen in connection with electronic communication and tender submission.

- Pursuant to Article 105, Paragraph 3 of the *Civil Procedure Act*, the applicant's signature is considered to be authentic if it is handwritten or in a form of an electronic signature, equivalent to a handwritten signature.

- Pursuant to Article 76, Paragraph 2 of the *Criminal Procedure Act*, in case of submission of an application in electronic form, an electronic signature equivalent to a handwritten counterpart is required.

d. Are there any specific groups of people that are required to have digital signatures [e.g., attorneys, notaries, government officials, etc.]?

Yes, pursuant to Article 15 of the *Notary Act*, notaries are obliged to obtain **(i)** a qualified certificate for an electronic signature and **(ii)** a qualified certificate for an electronic seal

through the Chamber of Notaries of Slovenia.

On the other hand, attorneys in Slovenia are not obliged to obtain a qualified digital signature per se, however, they still need to do so, if they wish to submit certain applications and/or requests in an electronic form (for example, in insolvency and execution proceedings). In insolvency proceedings attorneys are obliged to file all filings in an electronic form, signed with a secure electronic signature, based on a qualified certificate, otherwise, the filings are rejected by the court. Consequently, the majority of attorneys are still required to obtain a qualified digital signature.

In addition, digital signatures are also required for:

- Insolvency administrators or liquidators in insolvency proceedings, for the purpose of submitting reports, lists of tested claims, and other written documents.
- Any applicants submitting proposals for registration of title to land, as those may only be submitted electronically.
- Judicial and Administrative Authorities in Slovenia (pursuant to various legal acts).

e. Are non-personalized digital stamps recognized in your country with probative power [e.g., digital stamps used by companies, government, or administrative bodies]?

The probative power of digital seals and digital time stamps is recognized in Slovenia. Similar to the terminological issues of electronic signatures explained above (Section 2.b.), national legislation in some cases still refers to the Electronic Signature Act terminology when regulating electronic seals and electronic time stamps (See Rules on electronic operations in civil procedures and in criminal procedure, Article 3 for example).

The Electronic Signature Act defined a "time stamp" as an electronically signed certificate of a certifier that confirms the content of the data to which it refers at the particular time and a "secure time stamp" as an electronically signed certificate of a certifier that meets certain conditions (mutatis mutandis conditions for secure electronic signature). As aforementioned, those provisions are no longer valid and provisions of the eIDAS Regulation apply.

According to the eIDAS Regulation, an "electronic time stamp" is electronic data binding other electronic data to a particular time to establish evidence that the latter data existed at that time. As follows from Article 42 of the eIDAS Regulation, a "qualified electronic time stamp" is a timestamp that binds the date and time to data in such a manner as to reasonably preclude the possibility of the data being changed undetectably; is based on an accurate time source linked to coordinated universal time; and is signed using an advanced electronic signature or sealed with an advanced electronic seal of the qualified service provider or some equivalent method. The eIDAS Regulation further regulates an "electronic seal," an "advanced electronic seal" and a "qualified electronic seal." A qualified electronic seal is defined as an advanced electronic seal, which is created by a qualified electronic seal creation device, and based on a qualified certificate for electronic seal. In accordance with Article 35, Paragraph 2 of the eIDAS Regulation, such a seal enjoys the presumption of integrity of the data and correctness of the origin of that data to which the qualified electronic seal is linked.

In Slovenia, the use of electronic seals and electronic time stamps is required for notaries. Notary documents in an electronic form have to be secured with a qualified electronic signature as well as with a qualified electronic seal and a qualified electronic time stamp of the notary public. A document in an electronic form, without a qualified electronic signature of the notary public, their qualified electronic seal, and qualified timestamp, does not have the legal validity of a public document (Article 38 of the *Notary act*).

Additionally, other regulations also contain provisions in relation to time stamps and electronic seals, namely:

- According to Article 112 of the *Civil Procedure Act*, in case of submitting an application in electronic form with the assistance of an electronic provider, which signs the application with an electronic time stamp, the time of the electronic time stamp is considered as the time of receipt.
- Pursuant to Article 14 of the *Rules on the envelope, the proof of service, and other notifications regarding personal service in administrative procedures* (*Pravilnik o ovojnici, vrocilnici in drugih sporocilih za vrocanje v upravnem postopku, Official Gazzete of RS, No. 89/22*), the electronic proof of service has to be confirmed with the electronic seal of the service information system and equipped with a qualified time stamp.
- In accordance with Article 65.a. of the *Decree on Administrative Operations*, a certificate of compliance of the electronic copy with the document in physical form can be automatically confirmed by the information system, with a qualified electronic seal of the authority. Similarly, a qualified electronic seal of an administrative body is required for the confirmation of excerpts or other documents in an electronic form, which is automatically produced by the information system.
- Pursuant to Article 11 of the *Rules on criminal records* (*Pravilnik o kazenskih evidencah, Official Gazzete of RS, No. 3/18*), legal entities have to use digital seals when requesting to obtain data from criminal records in an electronic form. In such a case, a request signed with an electronic seal is considered a hand-

signed request.

3. Digital archiving

a. Are there any laws regulating digital archives and digital archiving in your jurisdiction?

In Slovenia, digital archives and digital archiving are predominantly regulated by the following legislation:

- *Protection of Documents and Archives and Archival Institutions Act* (*Official Gazzete of RS, No. 30/06 et seq.* – Archival Institutions Act);
- *Decree on the Protection of Documentary and Archive Material* (*Uredba o varstvu dokumentarnega in arhivskega gradiva, Official Gazzete of RS, No. 42/17*);
- *Rules on Uniform Technological Requirements for Capture and Storage of Materials in Digital Form* (*Pravilnik o enotnih tehnoloskih zahtevah za zajem in hrambo gradiva v digitalni obliki, Official Gazzete of RS, No. 118/20* – Uniform Technological Requirements).

The field-specific regulations, such as the *Companies Act* (*Zakon o gospodarskih druzbah, Official Gazzete of RS, No. 65/09 et seq.*), *Tax Procedure Act* (*Zakon o davcnem postopku, Official Gazzete of RS, No. 13/11 et seq.*), *Value Added Tax Act* (*Zakon o davku na dodano vrednost, Official Gazzete of RS, No. 13/11 et seq.*), *Rules on the implementation of the Value Added Tax Act (Pravilnik o izvajanju Zakona o davku na dodano vrednost, Official Gazzete of RS, No. 141/06 et seq.*), *Accounting Act* (*Zakon o racunovodstvu, Official Gazzete of RS, No. 23/99 et seq.*), *Slovenian Accounting Standards* (*Slovenski racunovodski standardi (2006) Official Gazzete of RS, No. 95/15 et seq.*), *Personal Data Protection Act* (*Zakon o varstvu osebnih podatkov, Official Gazzete of RS, No. 94/07 et seq.*), *Decree on Administrative Operations* (*Uredba o upravnem poslovanju, Official Gazzete of RS, No. 9/18 et seq.*), *Rules determining the retention period for documents of public administration authorities* (*Pravilnik o dolocanju rokov hrambe dokumentarnega gradiva v javni upravi, Official Gazzete of RS, No. 49/19*), etc. also contain some specific provisions on archiving of field-specific documents.

b. What are the main legal and technical requirements to digitally archive documents?

Archiving and keeping of the business documentation is a legal obligation of every taxable (legal or natural) person that is conducting any economic activity regardless of the profitability or revenue generation ability of said activity.

The Archival Institutions Act differentiates between two main groups of documents that are subject to archiving; **i)** electronic and **ii)** non-electronic or physical (paper) documents. Electronic documents are further divided into digital and analog documents. The legislation allows for the digital archiving of all (originally digital and non-digital) documents to avoid the keeping of multiple different archives and the associated additional unnecessary costs.

Analog and physical documents that are to be digitally archived, have to be converted to a digital form (i.e., digitalized) and digitally archived by an organization or an individual, that has obtained permission for digital archiving, issued by the Archives of the Republic of Slovenia for the digital archive keeping. For more information regarding digital archiving permissions please refer to Section 3.d.

Digitalization

The documents have to be selected, reviewed, and compiled in accordance with internal rules for the digitalization and digital archiving of the organization that is carrying out the digitalization process. On top of that, prior to digital conversion, the original documents in physical form have to be stacked, cleaned, restored (if necessary), and classified. Afterward, the documents are converted and digitalized in line with the minimum technical requirements and specifications listed in Article 38, Points 5 and 6 of the Uniform Technological Requirements that ensure a minimum quality threshold for the converted documents.

After the digitalization process, the documents have to be automatically or manually checked for correctness and, if need be, corrected to eliminate potential errors or deviations.

Archiving

Digitalized documents are scheduled and stored on an appropriate storage medium that ensures reliable capture and safekeeping of digital form for the duration of the archiving period. The Archiving Institutions Act differentiates between short-term and long-term archiving. Short-term archiving is archiving for a period shorter than five years, whereas long-term archiving is archiving for a period longer than five years. The act itself does not stipulate which documents have to be stored for a certain period of time as this is subject to field-specific regulations.

In general, the documents have to be archived for a period equal to the limitation period of potential obligations arising from the archived documents. The vast majority of financial documents have to be archived for a long-term period. Invoices and payment confirmation receipts have to be archived for a period of 10 years, starting from the end of the issuing year. Book-keeping documents, general ledgers, and other books of account have to be archived for at least 10 years starting from the day of the taxable obligation while contracts and receipts for the sales and purchase of real estate and inventory records have to be archived for at least 20 years. Some documents such

as business books and annual reports, original annual financial records and statements, payrolls, and data on employees have to be archived permanently.

Archiving digitally-signed documents

Additionally, for the electronic documents that have been signed using an electronic signature the supplementing data and signature verification tools have to be kept as well, for the entire archiving period of the document in question.

c. Is there any difference in your country's regulations between the digital archiving of paper and electronic documents?

Although the Archival Institutions Act differentiates between documents in digital, analog, and physical form, there are no major differences when it comes to digital archiving itself. As already described in more detail in Section 3.b., if analog and physical documents are converted and digitalized in accordance with the Archival Institutions Act, they are treated and handled in the same manner as digital documents.

Moreover, according to Article 13 of the aforementioned act, digitalized documents are a complete substitute for the original non-digital documents which may be disposed of and destroyed after being digitalized, under the condition that the digitalized or converted form of a document ensures equal probative value as original documents.

d. Is any third party required to participate in the process of digital archiving in your country [e.g., a trusted service provider, government / administrative bodies, etc.]?

A person who wants to digitally archive documents can either digitally archive documents themself or entrust a third party (trusted service provider) for said services. In either case, everyone (a person or a trusted service provider) who wants to conduct digital archiving has to adopt internal rules on the capture and digitalization of documents and apply for confirmation of said rules at the Archives of the Republic of Slovenia, which is a competent body for issuing digital archiving permissions.

e. Are there any sector-specific requirements and rules for digital archiving [e.g., archiving both the software and the related data to retrieve information in the financial sector]?

In accordance with *Regulation (EU) 2015/2365 of the European Parliament and of the Council on transparency of securities financing transactions and of reuse*, the parties, including the banks and financial institutions, are obliged to keep records regarding the conclusion, changes, and completion of all transactions for at least five years.

Additionally, in accordance with Article 28 of the Trust Services Act, notarial documents in an electronic form have to be archived together with the information for confirmation of the validity of an electronic signature, electronic seal, or electronic time stamp, as well as the tool for the verification of trust services.

Matjaz Ulcar
Managing Partner
matjaz@ulcar-op.si
+386 1 560 5300

Sara Oreski
Junior Associate
sara.oreski@ulcar-op.si
+386 1 560 5300

Simon Jancar
Junior Associate
Simon.Jancar@ulcar-op.si
+386 1 560 5300

CEE LEGAL MATTERS COMPARATIVE LEGAL GUIDE: TMT 2022

TURKEY

Onur Kucuk
Managing Partner
onur.kucuk@kplawtr.com
+90 507 709 68 07

Melodi Ozer
Associate
melodi.ozer@kplawtr.com
+90 507 709 68 07

CEE LEGAL MATTERS

www.ceelegalmatters.com

1. Legal framework for writing and electronic contracts

a. What are the requirements in your jurisdiction to consider a document to be in writing? Are there any formal/technical requirements?

The *Turkish Code of Obligations* (TCO), which is the main source of contract law, is based on freedom of contract and, in connection with this, freedom of form in contracts; however, the validity of some contracts can be conditional on the form it is concluded in. There are two types of forms foreseen in the TCO for documents in written form. These are the "basic written form" otherwise known as the "written form" and the "official written form,' which as the name suggests, requires an additional ceremony.

When a written form is deemed necessary, contracts must be signed by the debtor. If more than one party is in debt, the text must be signed by all parties. Unless otherwise stipulated by law, a signed letter, a telegram, the originals of which are signed by the parties of the contracts, faxes, or similar communication tools, provided that they are confirmed, or texts that can be sent and stored with a secure electronic signature are also considered in written form.

The "official written form" on the other hand, must be done in front of a competent authority or person in accordance with the procedures and conditions stipulated by law. Unless otherwise stated by law, contracts subject to the official written form requirement are made in the presence of a notary public. Otherwise, the contract will be ineffective. Pursuant to article 60 of the *Notary Law*, notary publics are obliged to fulfill all legal transactions that will be made in official writing and whose authorities are not specified in the law. However, in some cases, the law has authorized officials other than notaries to perform the official written form. For instance, according to article 26 of the *Land Registry Law*, land registry guards and officers are authorized to carry out the transactions that impose the debt of the transfer of immovable property and the establishment of limited real rights, which find the most application area among the contract types for which the official written form requirement is sought. Real estate promise contracts can be formally drawn up by notaries in accordance with the *Notary Law*.

b. Are electronic documents [e.g., an email] per se considered to be in writing under your law?

There is no other mandatory element sought for the basic written form other than the condition of having the signature of the debtor on the contract for it to be considered in writing. In other words, for any document to be considered in writing, it must be signed. As a rule, there is no requirement that the text of the document must be written by hand, and there is no restriction on a certain font unless otherwise stipulated. Again, there is no limitation in terms of the body in which the text should be written. The fact that paper is generally used in daily life does not mean that this is a legal obligation.

Since there is no limitation in the law, any object or surface could be used for writing the text. The only limitation here is that the text should reflect the declaration of will, especially in terms of the signatory, and that the intention of the person's declaration of will can be clearly understood. Considering this, the signature is accepted as an essential and sufficient element for written form rather than the structure of the text and where the test takes place. In this case, whether the text is created in the computer environment, by e-mail, by hand, with a typewriter or any other similar device, or by directly using the finger, as long as the text gives a meaning that reflects the declaration of will, it will be considered as a 'document'.

However, for this 'document' to be considered as in 'written form' we must further take a look at the signature. In terms of written form, it is the signature that determines whether the requirements of the written form are fulfilled, rather than the document itself.

Article 15 of the TCO regulates the "signature," which is the essential element for the written form. However, the regulation here does not contain detailed provisions regarding the signature. It solely mentioned that the signature should be written in the handwriting of the debtor as the only element. TCO requires no other element in order to fulfill the written form requirement other than a signature.

Turning back to the question, whether an electronic document is also considered in written form under Turkish law depends on whether the electronic document is signed. The TCO provides that the signature must be in the handwriting of the debtor. Along with this the TCO also accepts a secure electronic signature to have all the legal consequences of a handwritten signature. As stated in article 14/2 of the TCO, unless otherwise stipulated by law, a signed letter, a telegram, the originals of which are signed by the borrowers, faxes or similar communication tools, provided that they are confirmed, or texts that can be sent and stored with a secure electronic signature are also considered written forms.

To better understand the Turkish Government's policy on switching to e-documentation rather than physical paperwork, looking at tax regulations would be helpful. In terms of electronic documents, although these are not directly considered within the scope of "written form,' there are also some documents that must be arranged electronically in terms of Turkish Laws. These should be mentioned briefly;

Pursuant to the *General Communique of the Tax Procedure Law*, it is regulated that some documents specified in the communiqué are created electronically. Accordingly, e-Documents prepared in accordance with the format and standards determined within the scope of e-Documentation applications are not considered as a novel type of document, but rather an electronic one having the same legal qualifications as documents issued in paper form. Documents issued within the scope of e-Documentation applications are created in the information processing system and notified to the Revenue Administration, through the data processing system/system of private integrators.

Here are some of the documents that are required to be prepared electronically for taxpayers;

- A regulation has been made for taxpayers, who are obliged to switch to the e-Invoice application to use the e-Archive invoice application.
- Internet sales platforms, advertisers, and internet advertising intermediaries that are e-Commerce stakeholders have to use e-Invoice and e-Archive Invoice applications.
- All self-employed people (lawyers, financial advisers, self-employed doctors, architects, engineers, etc.) must issue their self-employment receipts as e-Self-employment Receipts.
- Traders and brokers engaged in the trade of vegetables and fruits within the scope of the state registration system must participate in e-Invoice, e-Archive Invoice, e-Waybill, e-Producer Receipt, and e-Ledger applications.
- Insurance, pension, and reinsurance companies are able to issue Insurance Policies and Insurance Commission Expense Documents, banks' bank receipts, foreign exchange buying and selling documents of authorized foreign exchange institutions, and Expense Compass documents used by all taxpayers as an e-Document.
- All taxpayers who have a license to operate in the fuel sector, including fuel stations, are obliged to use e-Invoice, e-Archive Invoice, e-Waybill, and e-Ledger applications.
- It is obligatory to use e-Waybills in the shipment of goods within the scope of the system carried out by the taxpayers within the scope of the fertilizer tracking systems.
- In the iron and steel industry, in order to reduce tax loss and evasion in the mining field and to prevent unfair competition in the industry, taxpayers engaged in manufacturing, export, or import activities are required to switch to e-Waybill applications.
- It has been made obligatory for taxpayers, who are included in the e-Invoice application, to issue the producer receipts issued in paper form as an e-Producer Receipt in an electronic environment in their agricultural product purchases from the farmers.

c. What probative power paper and/or electronic documents have that are to be considered in writing?

The general rule of Article 12 of the TCO on the validity of contracts states that "*the validity of contracts is not dependent on any form, unless otherwise provided by law. The form envisaged for contracts in the law is the form of validity as a rule. Contracts concluded without complying with the prescribed form shall not be valid.*" Hence, there is freedom of form in terms of the establishment and validity of a contract. Therefore, the parties to a contract can establish the contractual relationship by expressing their will to each other in written, verbal, or even implicit form.

However, although the general rule is that of freedom of form, the legislator has made the validity of some contracts subject to the fulfillment of a certain form condition. In this case, a contract cannot be considered valid unless it is made in accordance with the specified form. Such contracts are referred to as contracts subject to form and may appear as an "ordinary written form" or "official written form" (See Section 1.a.).

The form stipulated in the TCO is a condition of validity as a rule, and the form that is a condition of proof can be either determined by the will of the parties or may arise from the law. The form of proof is not a form of validity and is not a matter regulated in the TCO.

Probative power is regulated under the *Turkish Code of Civil Procedure* (CCP). Very briefly, any paper and/or electronic document that is "in writing" will hold some probative power to some extent. According to Article 199 of the CCP, the word "document" is defined as "*a carrier of data such as written or printed text, promissory notes, drawings, plans, sketches, photographs, films, images or sound recordings, data in electronic media and similar information that are suitable for proving the facts of the dispute.*" Whereas a promissory note is considered a written document that constitutes evidence against the issuing person and has the power of definitive proof. It should be noted that the promissory note is a more qualified version of a "document." Each of these categoric documentations shall have a separate effect in the proof of evidence.

For instance, Article 205 of the CCP defines the legal nature of documents created using secure electronic signatures. According to this, "*electronic data duly created with a secure electronic signature are in the form of promissory notes. These data are considered as definitive evidence until proven otherwise.*" Contracts signed with a digital signature will be considered within the scope of the "document" defined in the CCP and will fulfill the proof

required in cases where there is no obligation to prove by a promissory note in the same law.

To give an example, since documents signed with a digital signature only contain a digital image and are not handwritten or secure electronic signatures, they can only be treated as documents and not promissory notes, under the CCP. In this case, it is necessary to evaluate two alternative situations:

- In cases where there is no obligation to prove with a promissory note, a document signed with a digital signature can be accepted as a "document" and have the quality of evidence.

- In cases where there is an obligation to prove with a promissory note since a document signed with a digital signature is not a promissory note, it can only constitute the beginning of evidence.

Ordinary promissory notes admitted before the court or accepted by the court to be from the denier are considered conclusive evidence unless proven otherwise. As mentioned above, electronic data that are duly created with a secure electronic signature are also considered promissory notes. The judge can *ex officio* examine whether the electronically signed document presented to the court as evidence has been created with a secure electronic signature or not.

d. What are the general rules and requirements to conclude a contract electronically?

Electronic contracts can be expressed as contracts made in an electronic environment using internet tools. The term "electronic" in the concept of electronic contract refers to the tools used in the establishment and/or performance of the contract. Therefore, just because of this feature, there is no need to create a separate and unique contract category in the form of electronic contracts and to create special rules to be applied to these contracts. In the TCO, provisions regarding the establishment, validity, and performance of contracts can also be applied to electronic contracts to the extent that they comply with their nature.

In terms of its subject, electronic contracts are classified as electronic contracts for "the sale of goods," "the sale of digital products," and "the provision of services."

Pursuant to Article 1 of the TCO, a contract is established by mutual and appropriate declaration of the will of the parties. Unless there is a contrary provision in the law, it does not matter how this will is established. It is sufficient for the parties to declare their will statements mutually and in accordance with each other. Accordingly, in the establishment of electronic contracts, the parties must declare their mutual will in an electronic environment. By using the communication tools provided by technology, the parties have the opportunity to conclude contracts without the need to come together physically.

Provisions in the TCO applicable to the establishment and performance of contracts can also be applied to electronic contracts. Since the TCO will be used to the extent appropriate, there will be no need for special rules for electronic contracts.

As with the contracts within the scope of the TCO, the parties must make a mutual declaration of will to establish electronic contracts. In terms of Turkish law, it is important for the declaration of will to reach the other party, and since there is no obligation to express wills in a certain way, there is no obstacle to the establishment of electronic contracts by electronic means. In other words, the only difference between electronic contracts and traditional on-paper contracts is the method of establishment.

Electronic contracts are established by electronic means, unlike traditional methods. In traditional on-paper contracts, there is no need for a tool to communicate between the parties. However, there is a need for a tool that will enable the parties to transfer their statements to each other in electronic contracts.

For electronic contracts to occur, the proposal and acceptance phase must be completed. Electronic declaration of will is the "electronic form" of the declaration of will. In this respect, in order to be able to talk about an electronic declaration of will, the will to act, the consciousness of the declaration, and the will for legal consequences must be disclosed to the outside world in the electronic environment.

The explanations regarding the proposal and acceptance in electronic contracts can be grouped under four main titles: **(1)** proposal and acceptance via e-mail, **(2)** proposal and acceptance via websites, **(3)** proposal and acceptance via simultaneous communication channels, and **(4)** proposal and acceptance via social media sites.

The most emphasized issue in all of these is whether the contract is established between those who are ready or between those who are not. As a rule, agreements made via e-mail and websites are between those who are not ready. However, the TCO indicates that contracts concluded with simultaneous communication channels are accepted ad contracts between those who are ready. Although there are various doctrinal discussions about which definition and within which legal legislation the concept of an electronic contract will be evaluated, the TCO clearly states that "*any proposal made during direct communication with means of communication such as telephone and computer shall be deemed to have been made among those who are ready*." This provision clearly indicates that the electronic contract can be considered *inter praesentes*, meaning that it is conducted

among those who are ready, with the condition that the contract is concluded through electronic means that provide direct communication.

Contracts made over social media sites may be between those who are ready or those who are not ready, depending on the nature of the communication, and the binding period of the proposal in the agreements made with this tool should be determined according to this determination. Whereas contracts concluded through the website are contracts between those who are not ready as a rule. The debate about whether the website, which is also quite controversial, is considered a suggestion or an invitation to a proposal. However, this has not been definitively resolved.

On the other hand, other conditions should also be sought for the contract to be valid for the parties. These conditions can be briefly listed as; the competence of the parties, the fact that the contract is not contrary to the mandatory provisions of the law in general, the subject of the contract is not impossible, and the will of the authorized parties to conclude the contract is healthy. In this context, it can be stated that in contracts where many dynamics are sought, it is possible for more than two parties to form contracts in which they will impose debts and rights on each other, provided that all the above-mentioned terms and conditions are fully met.

In summary, while an electronic contract is no different than an ordinary contract, it is necessary to evaluate it within the framework of the TCO and see if it meets the essential elements of being a contract under the TCO. This assessment should be made for each concrete case.

e. Are there any sector-specific rules that define further requirements to conclude contracts electronically [e.g., contracting via an authenticated electronic channel, contracting via video chat, etc.]?

In light of the above, it should also be briefly mentioned that the obligation to inform before the conclusion of electronic contracts brought by the *Law on the Regulation of Electronic Commerce* (E-Commerce Law) is extremely important. Now, before the establishment of electronic contracts, service providers are obliged to pre-inform the other party with regard to the electronic contract. Although failure to fulfill this obligation to pre-inform does not prevent the establishment of an electronic contract, criminal and legal liabilities of service providers may arise due to the failure to provide this information.

If one of the parties to electronic contracts is a consumer, the electronic contract will also be considered a distance contract. This also leads to the *Turkish Consumer Protection Law*. Distance contract pursuant to Article 48 of the *Consumer Protection Law* is considered a contract concluded by using remote communication tools between the parties until and including the moment the contract is established, within the framework of a system created for the remote marketing of goods or services, without the simultaneous physical presence of the seller or supplier and the consumer.

The *Regulation on Distance Contracts* stipulates that distance contracts refer to contracts made in writing, visual, telephone, and electronic media or using other communication tools and without confronting the consumers, and the delivery or performance of the goods or services to the consumer is agreed upon immediately or afterward. The same is valid for distance contracts for financial services. The *Distance Contracts Regulation on Financial Services* defines such contracts as financial contracts established between the provider and the consumer through the use of remote communication tools within the framework of a system established for the remote marketing of financial services.

During the pandemic, the Turkish Banking Regulation and Supervision Authority (BRSA) has onboarded a new regulation with regard to distance contracts called the *Regulation on Remote Identification Methods to be Used by Banks and Establishment of Contractual Relationship in Electronic Environment*. According to this regulation, provisions regarding the establishment of a contractual relationship in the electronic environment are set forth. It is established that, following the identification (for KYC purposes) stage, in cases where the customer's declaration of intent to establish the contract is established remotely, "the written form" requirement for these contracts is deemed to have been fulfilled.

Before the contractual process is commenced, remote identification from the customer is required. Remote identification can take place with the customer representative and customer by video calling and communicating with each other online, without the need to be physically in the same environment.

Similar to the BRSA, the *Insurance and Private Pensions Regulation* and Supervision Agency introduced a *Regulation on the Activities to be Evaluated within the Scope of Insurance and the Insurance Contracts Concluded at a Distance*, entering into force last year. Accordingly, within the framework of a system established for the remote marketing of insurance products, insurance companies will be able to conclude a contract with the pension company or insurance intermediary that provides insurance, by using a remote communication tool without the simultaneous physical presence of the persons. In line with this regulation, authorized institutions that conclude or mediate a distance insurance contract through a remote communication tool will have to have the necessary and sufficient organization and technical infrastructure.

Another area where remote electronic contracts take place is

Payment and Securities Settlement Systems, Payment Services, and Electronic Money Institutions. According to the *Law on Payment and Securities Settlement Systems, Payment Services and Electronic Money Institutions* (Payment Services Law), the framework agreement of payment services, shall be executed in "written form" or by the use of distance communication tools, whether at a distance or not, over an information or electronic communication device, which the Central Bank of the Republic of Turkey determines can replace the written form and can be arranged in a way that will be established through methods that will allow the verification of the customer's identity. This is also a huge step forward in the digitization of all the physical paperwork and documentation to take place electronically.

2. Digital signatures

a. Are there any laws regulating the use of digital signatures in your jurisdiction?

As a result of the increase in transactions in the electronic environment, the question arose as to whether the declarations of will declared in this environment really belong to the said person. Various methods have been developed in order to determine the identity of the person in a computer environment and to ensure that it can be known that the declaration they convey really belongs to them. The most common and reliable of these methods is the method of expressing the declaration of will with a personal encryption method, which is also reflected in the *Electronic Signature Law*.

The existence of a law called *Electronic Signature Law* (ESL) may lead to the suspicion that all signatures to be created in the electronic environment are subject to this law and therefore must meet the conditions set forth in it, otherwise the signature effect cannot be exerted in the electronic environment. Indeed, since the legislator felt the need to make a law regarding the signature in the electronic environment, they should have dealt with this area specifically and subjected it to an exclusive regulation. However, when the law is examined, it is understood that this conclusion or determination is not correct because the law has regulated only one of the many signature types that can be brought to the agenda in the electronic environment.

b. Is there any difference between the different types of digital signatures in your jurisdiction?

An "electronic signature" is defined in the ESL as "*electronic data that is added to another electronic data or has a logical connection with electronic data and is used for authentication purposes*." Although the law prefers a broad definition, it regulates the details and principles regarding the type of signature that it accepts as a "secure electronic signature" in its following articles and throughout the law.

Electronic signatures can be created using different techniques, from the simplest to the most complex. For example, the simplest electronic signature technique is to transfer the handwritten signature of the person to the computer environment by being read in the scanner and added to the prepared texts or messages. The biometric method, which is obtained by using body features such as fingerprint, palm, voice, and retina, is another electronic signature technique.

The electronic signature method that can fulfill the functions of a handwritten signature in legal terms is considered a digital signature. A digital signature is based on the encryption of documents created and sent electronically with the double-key encryption technique. In the digital signature method, the signer has two keys, public and private, which have a mathematical connection between them and are functionally united. The secret key, known only to the signer, is used to encrypt a prepared text, that is, to sign it. If the public key is known by everyone, it is used to read the signature created with the private key, in other words, to determine whether it belongs to the signer.

A "secure electronic signature," on the other hand, does not meet the broad definition of a digital signature. In accordance with Article 4 of the ESL, a "secure electronic signature:"

a) depends exclusively on the signatory,

b) is created with the secure electronic signature creation tool only at the disposal of the signer,

c) enables the identification of the signer based on the qualified electronic certificate, and

d) enables the determination of whether any changes have been made to the signed electronic data afterward, signature.

All the remaining articles of the ESL cover "secure electronic signatures" and not "electronic signatures." Therefore, although a broad definition was provided in the law for electronic signatures, a "secure electronic signature," which expresses a narrower meaning, is not considered an electronic signature in the sense given in the definitions section. As a natural consequence of this determination, signatures other than a secure electronic signature are not considered within the scope of the ESL and are excluded from the scope of this regulation. More precisely, the ESL does not regulate that other signatures will be invalid but rather limits its scope to secure electronic signatures. Thus, the law does not contain regulations for other signatures and excludes them from its scope.

In this case, since there is no other special regulation regarding other types of signatures, general provisions should provide guidance and whether other signatures will be valid or not should be evaluated according to the TCO, not according to the ESL.

c. What probative power each type of digital signature has in your country?

As mentioned in Section 2.b., an "electronic signature" is defined as an umbrella expression in the ESL. An electronic signature is defined as electronic data that is attached to another electronic data or has a logical connection with electronic data and is used for authentication purposes. Whereas a "secure electronic signature" is exclusive to the signatory, created with the secure electronic signature creation tool only at the disposal of the signer, enables the identification of the signer based on the qualified electronic certificate, and enables the determination of whether any changes have been made to the signed electronic data afterward.

A digital signature, on the other hand, also falls under the category of an electronic signature. This type of signature refers to electronic records or traces created to perform the function of signing electronic documents with a virtual visual image or sign, which is not based on a qualified electronic certificate produced by electronic certificate providers and does not need to go through a competent authority.

Although it is possible to determine by whom, when, and where the documents have been signed with this signature, it should be accepted that since Article 14 of the TCO stipulates that contracts in written form must obtain the signatures of those who undertake debt, a digital signature will not be accepted suitable for such cases.

Accordingly, the following transactions cannot be completed with a digital signature:

- An assignment of receivables
- Pre-emptive rights
- Installment sales contracts
- Promises of reward
- Real estate brokerage contracts
- Intellectual property license agreements

The following transactions, on the other hand, cannot be performed with a secure electronic signature or digital signature, but will be carried out with a wet signature in the presence of official institutions such as a notary public or land registry office:

- Real estate sales premise agreements
- Getting married
- Inheritance and successions
- Official wills
- Companies' articles of association
- Transfers of intellectual property rights

Unless otherwise stated by law, contracts can be concluded with an electronic signature, and the signature made in this way will replace the written form specified in the TCO.

Finally, yet importantly, a type of e-signature that should be mentioned is the mobile electronic signature. Mobile e-signature is an application that enables secure electronic signature transactions as wet signatures in accordance with the ESL and the relevant legislation using a mobile phone and GSM SIM card. The only difference between a mobile electronic signature and an electronic signature is the use of a SIM card inserted in a mobile device as an electronic signature creation tool. Since the legislation on electronic signature also covers mobile electronic signatures, the mobile electronic signature also provides the legal validity provided by secure electronic signatures in an electronic environment.

d. Are there any specific groups of people that are required to have digital signatures [e.g., attorneys, notaries, government officials, etc.]?

Anyone who wishes can apply individually for an e-Signature. In particular, taxpayers who will use e-Self-employment Receipts must obtain an e-Signature in order to register with the Private Integrator or RA systems. Apart from this, the places where e-Signatures are used are:

- E-Government Applications
- E-EIAs (Environmental Impact Assessments)
- The UYAP (National Judicial Network Project)
- Ensuring Inter-Institutional Communication (Police Departments, Population, and Directorates of Citizenship Affairs)
- Registered Electronic Mail Systems (KEP)
- Commercial registry transactions within the scope of MERSIS (Central Registry System)
- Applications (YGS, KPSS, LES, Passports, etc.)
- MERNIS (ID Number) transactions
- EKAP (Electronic Public Procurement Platform) transactions
- e-Prescription Project & e-Pulse & TITCK Project (Ministry of Health) transactions

- e-Foreclosure Project (Social Security Institution) transactions
- e-OKUL (Ministry of National Education) transactions
- POLNET (Police Computer Network) operations
- GIMOP (Customs Administrations Modernization Project) transactions
- TAKBIS (Land Registry and Cadastre Information System) transactions
- TPE (Turkish Patent Institute) transactions
- TPE (Turkish Patent Institute) transactions
- DMO (Electronic sales application) transactions
- RTUK (Radio and Television Supreme Council) procedures
- In sending bank instructions
- In e-Signing electronic archives
- UTS (Product Tracking System) transactions
- Trademark patent applications,
- Expert applications for conciliators
- Export support payment applications
- Foreigners' work permit applications
- Authorized obligee applications
- Employee service contracts and all other contracts
- Participation in tenders

e. Are non-personalized digital stamps recognized in your country with probative power [e.g., digital stamps used by companies, government, or administrative bodies]?

The ESL refers to a timestamp as a record of electronic data verified with an electronic signature by the electronic certificate service provider in order to identify when it was produced, modified, sent, received, and/or recorded. It is used to prove that electronic data such as documents, records, and contracts existed before a certain time in electronic media. It ensures that reliable time information can be added to transactions in the electronic environment. It can be used on all kinds of electronic data such as electronic applications, minutes, contracts, and similar electronic data that should have time information on it.

However, it should be separately mentioned that currently Turkey does not have a specific law on non-personalized digital stamps.

3. Digital archiving

a. Are there any laws regulating digital archives and digital archiving in your jurisdiction?

The Regulation on Government Archive Services partially regulates digital archiving. The purpose of this regulation is to manage the arrangement of documents resulting from the work and transactions of public institutions and organizations; to ensure that they are protected under the necessary conditions, to prevent loss for any reason, to ensure that they are evaluated in the service of the state, real and legal persons, and people of science, to identify the archived documents held by institutions, organizations, and individuals and the documents that will become archival documents in the future, to sort out the documents that do not need to be kept and last but not least, to regulate the procedures and principles regarding the destruction of archival documents and the transfer of archival documents to the Administration of State Archives.

b. What are the main legal and technical requirements to digitally archive documents?

The digitization of documents is carried out in accordance with the procedures and principles determined by the Administration of State Archives. Pursuant to the *Regulation on Government Archive Services*, documents in hard copy can be incorporated into an electronic document management system in order to preserve the integrity of the transactions and files. In all kinds of digital imaging operations, the *Electronic Document and Archive Management System* and the standard numbered *TS13298* is taken into account. The *Electronic Document and Archive Management System* is a system that enables the archiving and management of all kinds of documentation created by institutions during their activities, from their production to their final liquidation, whereas the *TS13298* standard is a standard prepared for the purpose of protecting and keeping the document quality of the documents produced or to be produced.

When digitizing archival documents, the relevancy between digitalized documents and their tangible copies/ hard copies should be kept during the process. Similarly, the relevancy between digitalized images and their metadata should be preserved as well. When deemed necessary, the obliged parties can digitize their hard-copy documents that are in their possession, which have the quality of archival documents, to save them from being a single copy, to prevent the documents other than the archive documents from being worn out and to be able to use them effectively. Documents that are not used frequently or those documents that do not need to be stored at the end of their storage periods or those documents that will be destroyed are not subjected to the digitization process.

c. Is there any difference in your country's regulations between the digital archiving of paper and electronic documents?

An archive document, according to the *Regulation on Government Archive Services*, is a document produced 20 years after its last transaction date or 15 years after being finalized in use. This is a document that does not function in the daily workflow and has completed its storage periods and storage plans if any. This document can be in written form, drawn, illustrated, visual, audio, or electronic media, as to any political, social, cultural, legal, administrative, military, economic, religious, scientific, literary, aesthetic, biographical, geological, and technical value and contain information.

The *Regulation on Government Archive Services* sets forth that the obliged parties of this regulations (obligors) have the liability to protect all kinds of documents they behold, against fires, theft, humidity, heat, flood, dust, and destruction of all kinds, from animals and insects and keeping them in their current original order. As for documents created and/or stored in an electronic environment, which clearly indicates digital documentation, the obligor must take necessary security measures against all kinds of disasters, cyber-attacks, software/hardware origin, or other possible threats/risks. Along with this, the obligor must execute a disaster recovery plan and establish its backup units in order to prevent possible document loss.

Also, all kinds of information and documents in electronic form or electronic environment are kept in electronic archives in a way that can be accessed, stored, cleared, and transferred. Apart from physical archives, electronic documents are expected to be stored in the electronic document management system, where the documents are stored in the file/folder they belong to, according to the hierarchical structure and file codes they are defined in. Whereas the arrangement of different types of documents such as film, photograph, record, audio and video tape, and similar documents can be done according to different systems and processes.

While there is no direct statement openly indicating the differences between the digital archiving of paper and electronic documents, the above-stated regulations set forth the indirect separations of the archiving of electronic documents from physical/tangible documents within the *Regulation on Government Archive Services*.

d. Is any third party required to participate in the process of digital archiving in your country [e.g., a trusted service provider, government / administrative bodies, etc.]?

Pursuant to the *Presidential Decree on The Department of State Archives*, the Administration of State Archives (Administration), is subject to a general budget and is established under the Administration in order to organize archive services and activities and to provide document management in the public sector (the Department of Information Processing and Electronic Archives is one of the service units).

e. Are there any sector-specific requirements and rules for digital archiving [e.g., archiving both the software and the related data to retrieve information in the financial sector]?

N/A

Onur Kucuk
Managing Partner
onur.kucuk@kplawtr.com
+90 507 709 68 07

Melodi Ozer
Associate
melodi.ozer@kplawtr.com
+90 507 709 68 07

CEE
LEGAL MATTERS

www.ceelegalmatters.com