YOUR GUIDE TO SAFE DIGITAL CONTRACTING

THE NEED TO ADAPT

Ask yourself: has your business been hit by the coronavirus pandemic? Even if the answer is a definite 'no', you have probably already been thinking about how to prepare your business for such events.

We have all witnessed how the Covid-19 outbreak affected the industry in the form of lockdowns, disrupted logistic routes, bankrupt suppliers and fluctuation in demand. Regular business management routines might be insufficient to tackle these challenges at the same time. And make no mistake, similar crises are more likely to follow in the coming years.

What the epidemic has certainly taught us is that *flexibility* is most needed when things go wrong. *'Go digital, this is the future',* they say. Indeed, if done properly, digitisation of your contracting could be a key component of your company's adaptation skills, since it is fast, cost-effective and does not need the physical presence of the parties.

The bad news is that some popular electronic forms, such as simple emails or images of signatures in a pdf file, are not considered legally secure at all. If you keep using them, your enterprise might face risky trades and unexpected financial losses.

If you want your contracts to be safe and sound, or in the legal language, valid, binding and enforceable, you may want to look for better practices. In this article, we will present the legal background of digital methods and their ranking from the worst to the best, to help you make the shift to proper e-contracting.

WHAT IS A CONTRACT AND HOW IS IT MADE?

To put it simply, a contract is the legal form of expression of at least two parties' mutual intent to accomplish something. It is more than just a friendly chat: the commitments the parties make

will oblige one of the parties to perform the service while entitling the other to demand the consideration in return. If either or any of them breaches the contract, the damaged party will be authorized by law to pursue a claim against the wrongdoer.

It is important to know that only those types of communication will create – or in legal terms, constitute – a contract which are intended to have legal effect. We call these declarations legal statements. When you address your comment 'I like this warehouse' to Julia, who has just started advertising her premises for business purposes, that remark will be merely an opinion with no particular legitimate consequence. But if you continue it with '... and I'd like to rent it for storing company products', then it will become a legal statement, a business offer in fact, waiting for Julia's reply. If she accepts it, then the contract is concluded.

Agreements can be made orally, by implicit conduct or in writing. The first two options are quite rare in business life, and they mostly appear in the course of everyday errands. For example, you typically enter into a contract by implicit conduct with the grocery shop when you unload the products you wish to buy at the cashier. We will now focus on the third option.

THE IMPORTANCE OF WRITTEN FORM

There are several reasons why it is essential to constitute business arrangements in writing. You not only need to remember the details of the deal, but a written document should also be capable of verifying that its legal statements have not been modified since the time of declaration and that they have been indeed made by the signing parties. A person's contractual will is usually confirmed by a handwritten signature which, by consensus, serves as proof of the authenticity of the legal statement.

A document must be authentic enough to be enforceable in court by the damaged party if needed, following a court proceeding. This level of authenticity is called full probative force in legal terminology, which can be guaranteed, for example, by the additional signing of witnesses, the countersignature of an attorney or the certification of signature by a notary public.

Besides the authenticity and enforceability, the written form is mandatory by law for certain types of contracts. For instance, this is the case when your company wishes to employ someone, manage its corporate affairs, license a work under copyright, establish a lien over a company asset or eventually buy Julia's warehouse. If this compulsory rule of written form is disregarded, then the contract will become invalid, which means that the agreement itself cannot be enforced in court.

Based on the above, a legally secure business arrangement, either on paper or in electronic form, must be made in writing with full probative force in order to have a valid, authentic and enforceable document as a result.

IN SEARCH FOR A PROPER E-SIGNATURE

According to the concept of the Hungarian Civil Code, a legal statement in digital form is considered written only if the declarer of the statement is identified somehow and furthermore, the content and the time of the declaration are recorded and can be retrieved later without any changes. This definition is platform-neutral which means that any digital service that provides these features can be potentially used to sign a legal statement electronically.

The requirement of storing and recalling information is rather easy to achieve since even an email can indicate the content and exact date of a message. The difficult part is how to identify the declarer, and this is where the use of emails in business contracting usually raises doubts as to whether it can be considered legally secure.

The e-signature service we wish to use, must be able to create a unique connection between the signing person and their e-signature in such a way that the person can be identified by the digital signature before other parties. The problem lies within the nature of digital contracting: the signing parties are in different locations and they cannot check the other party's identity in person. That is how a simple signing session may turn into a matter of (dis)trust.

The problem of trust has been recognized and managed by Regulation No. 910/2014 of the European Union (usually referred to as the eIDAS Regulation) which serves as the legal framework for using e-signatures in the EU. It introduces the definition of trust service, an electronic process normally provided for a fee by registered trust service providers, with the aim to create and validate digital signatures, also known as advanced electronic signatures (AdES).

Within the terms of the eIDAS Regulation, an AdES is a password-protected digital code, individually created and linked to the client by a software. Signing an electronic document is basically a coding procedure. The digital imprint of the document is encrypted by the software using the AdES in the form of a verification file. The verification file can be read within the software by third persons using a public decryption key. The success of the decoding will prove that the AdES-signed legal statement has been indeed issued by the owner of the AdES, and its content has not been changed since the placing of the signature.

There are higher levels of the AdES in terms of probative force and digital security, such as the AdES with qualified certificate (AdESQ), and the qualified electronic signature (QES). Both require the preliminary and personal verification of the client's identity performed by the trust service provider using public registers, and they equally grant full probative force in return. In case of the QES, the personalized signing code is stored on a separate physical device, a USB token for instance, which is manufactured specifically for the client, hence the 'qualified' tag.

It is important that any kind of electronic signature under the eIDAS Regulation is created and exists only in electronic form by definition. Once printed on paper, they will lose their digital features together with their associated legal effects. And vice versa, a signature appearing on a scanned document will not automatically qualify as an authentic e-signature. In this regard, printers and scanners do not serve as a kind of gateway between paper and electronic forms.

To have a clear picture of which kind of digital devices can be used safely based on the above and which should be avoided, let us have a look at these self-explanatory rankings below.

THE WARNING ZONE

Emails, social media or phone messages, scanned signatures inserted as images into a pdf file, and the so-called online 'document management tools' are considered the 'worst' practices because they all seem to fail the person identification requirement.

This means that these popular platforms usually do not involve a third party who could confirm the identity of the signing person before the first e-signature takes place. The fact that the signer and their digital stamp are not connected in a direct and authentic way, will question whether the platform is able to provide valid legal statements with full probative force and might also raise further legal issues as illustrated below.

Potential identity theft

Skipping the identification stage certainly makes these methods more comfortable to use, but it might also lead to potential abuse with your identity if the login data of your online account is leaked, stolen or simply stored by your browser by default. In such cases, an unauthorized person may create a fake declaration of commitment or a waiver of a right in the name of your company without your consent which might cause serious harm to you.

It has been also proved that those online document management services, which operate automatically by using artificial intelligence (AI), can also be tricked. In this case, an AI-driven algorithm is responsible for the person identification by checking a scanned and uploaded ID card. It may happen that the algorithm cannot recognize the replacement of the ID photo with another person's image as an act of fraud. There is no question that these smart solutions will be more reliable as technology advances, but for now they do not seem to provide secure e-signing in the absence of human control.

Strict judicial interpretation of authenticity

Next comes the lack of full probative force: the Hungarian Code of Civil Procedure defines which categories of e-signing methods, such as the AdESQ and the QES, have full probative force. Hungarian courts have the right to ultimately decide the level of probative force of any electronic document, with the help of an expert, if necessary, as it happened in a recent press-related case. A request for the correction of a published article was sent to a news agency by email, however, such requests must be made in writing by law. The court stated in its judgement that a simple email does not provide 'absolute authenticity', arguing that an email cannot be associated with its sender without a doubt. Therefore, an electronic document must be signed at least with an AdES in order to reach this required level of authenticity.

We must note that there are some disputes going on over this judicial approach. Some jurists say that the standard for 'absolute authenticity' is an extra requirement compared to the definition of the Civil Code, as the law does not specify any level of certainty regarding identification. It has also been argued that in today's corporate environment emails sent from password-protected business accounts should be accepted as valid and authentic electronic legal statements. They usually indicate the full name and title of the sender, together with the contact details of the company and the previous emails. This additional information should be sufficient for the identification of a person in theory, however, there is always a chance of misuse if the sender's desktop is left unattended or their email account is hacked.

Partial invalidity of a contract

To have a closer look at the concept of partial invalidity, let us presume that you run an online store selling ice cream, seafood and other perishable foods which must be stored at low temperatures in a warehouse until delivery. Your company has already signed a lease agreement with Julia whose office building is used as your depot. You also engage her to ensure the operation of the cooling equipment and the security cameras in the form of a service agreement. Since these types of contracts do not have to comply with the standard formal requirements for written contracts, you both agree to conclude it by simply agreeing on the matter through emails.

However, an agreement could also contain a particular term that must be made in writing by law, such as the so-called compensation for non-performance clause. This kind of compensation means that in case a party fails to fulfil a particular contractual obligation, they must pay a fixed fee to the damaged party, unless their non-performance is excused. This is certainly one of the legal terms with serious legal consequences, hence the mandatory written form.

As your products are perishable, you definitely want the power supply of the cooling system and the security cameras working around the clock. Therefore, you agree with Julia in that separate service agreement that she will pay your company 100,000 HUF per day as compensation for non-performance if the power supply does not operate due to her fault.

Unfortunately, there are some power outages in the electricity system and Julia forgets to have it repaired for 5 days. As a result, some of your goods become unusable or are stolen because both the cooling and security systems are out of order during the shutoff. Based on what was agreed upon, you send Julia a request to pay the said compensation for non-performance in the sum of 500,000 HUF. Although she admits her fault, Julia refuses to pay based on her – otherwise correct

– argument that this particular clause of the contract is invalid and thus, cannot be enforced since it was not made in writing.

This example of partial invalidity illustrates that despite the fact that your company suffers significant financial loss, you cannot pursue a claim against the other party because that clause of the contract is considered invalid, therefore, it cannot be breached either.

THE 'GREY' ZONE

This category refers to those online digital services which have been created in response to the need for convenient e-signing methods, for example when you draw your signature on a tablet with an e-pen, place your fingerprint on a sensor, or make hand gestures or verbal confirmation to a camera.

The reason for placing those between the worst and best practices is that it is yet unclear which of them qualifies as authentic e-signature within the terms of the eIDAS Regulation. Many companies, which provide these e-signing tools, are registered under the laws of the United States. Since their products have to comply with the relevant U.S. regulation in the first place, it is not obvious whether they would also satisfy the demanding legal specifications of an AdES, an AdESQ or a QES.

Until judicial guidelines or other certificate procedures have made it clear which of these practices provide legally secure and authentic e-signatures, we have some 'better than nothing' tips to use for emergency.

You should always settle in advance with your business partners what form of digital communication is accepted during the negotiations, the signing sessions, and throughout the whole performance of the contract. It could create confusion in performance if different communication channels are being used, or if particular instructions on delivery, takeover or bank transfer details are not in line with the wording of the agreement.

In case one of the parties has no access to authentic e-signature, then the contract may be concluded in a semi-digital form. To this end the agreement must indicate the fact that one party will use digital signing, while the other will sign their copy on paper, and that these separate copies will jointly constitute the entire contract when exchanged between the parties. Both the digital and hard copy of the contract must be stored in the same form as they are signed, in order to preserve the validity and the full probative force of the complete agreement.

'AVDH', a Hungarian speciality

Before we move on to the top section of our list, we need to present the AVDH service, a central document authentication method which is provided by NISZ Zrt., a Hungarian state-owned organization (NISZ).

The AVDH service grants full probative force by law. It is available free of charge for anyone who has registered an account on the Client Gate portal, which is an online interface to communicate with public administration, primarily in private matters of citizens. In order to activate the account, the client must make an appointment at one of the government offices in Hungary, go through a self-identification process in person and provide a password. When using the service, the client must enter their Client Gate and upload the legal statement where the signature is placed on the document by NISZ. Although the AVDH-signed document is recognized by law as having full probative force, there are several reasons why this solution is not listed among the best practices.

The AVDH is basically a password-based online platform which only confirms that a document was uploaded for certification through the Client Gate of the user. Therefore, there is a chance of abuse with one's identity if the Client Gate login data is compromised.

In addition, the scope of use of AVDH is debated among jurists when it comes to the authentication of corporate documents. Some experts argue that a company representative can only use their e-signature if the digital reference data of that particular e-signature is recorded in the company register. This ensures that an e-signature of a document can be compared with this reference data in case of doubt. If there is a match, then the legal statement made on behalf of the company is authentic and valid. To our best knowledge, the AVDH cannot be technically recorded in the company register. Others argue that the respective legal provisions do not restrict the use of AVDH in case of corporate representation. As matters stand, the use of AVDH on behalf of a company is not without legal concerns.

THE BEST PRACTICE

From among those listed so far, we think that the QES is the best option available for your company. According to the eIDAS Regulation, its full probative force is recognized throughout the whole European Union with the same legal effect as that of a handwritten signature. Furthermore, the fact that it can only be used with the separate 'offline' signing device, significantly reduces the chance of unauthorized use.

Although it is true that the initial registration and personal identification process might seem inconvenient, not to speak of the subscription-based service fees, which are usually more expensive than those of the 'online document management' tools. Still, among the plenty of electronic signing services out there, only a few, including the QES, work in a transparent and legally secure manner.

Go digital, with caution

It is true that digitisation is not only a useful practice, but the inevitable next step in the evolution of contracting for enterprises wishing to remain competitive in the digital era.

We may run our usual everyday errands online with confidence as a matter of habit. And still, concluding electronic business arrangements should always be made with care with and attention to legal formalities, even if circumstances force us to make company decisions urgently. We hope that the above will help your company in this endeavour in the future.

***

Sources:
- Dr. Kósa Ferenc: Elektronikus okiratok közérthetően I. (in: Pesti Ügyvéd, 2021. október);
- Dr. Lovas Lilla: Elektronikus aláírás – elméletben és gyakorlatban (Elérhető a Magyar Ügyvédi Kamara Kötelező Ügyvédi Továbbképzési Rendszer felületén);
- Dr. Rostás Péter LL.M.: Elektronikus jognyilatkozatok, távollevők társasági jogi nyilatkozatai és az e-mail írásbelisége (in: Ügyvédek Lapja, 2021. március-április).

* * *

Budapest, 17 May, 2022.

Author: dr. Edmond Kerényi

CERHA HEMPEL
CONSTRUCTION PAPERS

If you are interested in other professional materials from the world of construction law, visit our website, click: **Construction Papers**

Postal address:
CERHA HEMPEL Dezső és Társai Ügyvédi Iroda
H-1011 Budapest
Fő utca 14-18.
Hungary

E-mail:
andras.fenyohazi@cerhahempel.hu
bence.rajkai@cerhahempel.hu