E-SIGNING IN HUNGARY: A PRACTICAL GUIDE

Administration. Everyone wants to do it faster and easier, preferably in a paperless, contactless, and environmentally friendly way. e-Signature is a key aspect of digital transformation projects, yet we found that there is still lack of clarity as to the legally binding effect of e-signing tools in a given jurisdiction. In this report, we focused on Hungary and analyzed six locally available, electronic alternatives to traditional ink-on-paper signing. We also briefly looked at international, borderless platform solutions.

Anyone can create authentic official documents not only on paper, but also electronically -- even free of charge, using widely available technologies in Hungary and beyond. Due to the continuous development of e-signature technologies, global digitization efforts, and the legal effects of the EU eIDAS (Electronic Identification, Authentication and Trust Services) regulation[1] ("**eIDAS Regulation**"), individuals and businesses increasingly consider fully electronic management of their affairs as a viable alternative to paper-based solutions. **While the eIDAS Regulation recognises the authenticity of e-signatures throughout the EU since September 2014, this legal technology report aims to offer clear guidance as to legally binding and officially accepted e-signature solutions in Hungarian business and private affairs.**

What is an electronic signature? Which types are legally binding?

For centuries, handwritten signatures in ink have traditionally proven that a document was indeed signed by the named signatory. The legally binding effect has been attributed to the handwriting's unique graphics and (relatively) indelible attachment to the paper document. Just like a traditional handwritten signature, an e-signature is also specific to the signatory and is inseparably linked to the signed or authenticated electronic document. However, in the case of e-signatures the proofing requirements are met by digitally secure, cryptographic means: with an **encoding or e-clause (also referred to as a digital stamp) embedded in the structure of the e-document** and an attached **e-certificate about the e-signature**, verifiable by anyone.

While there are many e-signature solutions available locally and globally, these tools were not created to be equally relevant irrespective of context and jurisdiction. The eIDAS Regulation differentiates between three types of electronic signatures which are all legally valid but serve different purpose:

- ✓ **Standard e-Signatures** have been available for many years but are not appropriate for complex transactions like high-risk contracts. This basic form of e-signature can be manually drawn on a desktop screen or scanned from a handwritten signature, yet one cannot be certain that the signature is linked to the individual authorized to sign. Accordingly, in the case of doubt (lack of trust) standard form e-signatures may raise some valid questions in relation to the identity of the signatory and the legal validity of the undertakings signed in this form.
- ✓ **Advanced e-Signature (AES)** provides a higher level of security because it protects the signed document by cryptographic means. In Hungary, an e-document with an attaching AES classifies as a simple private document, i.e., it is equivalent to an undertaking made on paper with a simple handwritten signature. Simple private documents do not have the same probative value as a private document with full power of evidence (enabled by QES as defined below),

[1] 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

yet undertakings under an AES are equally binding between the parties by the force of law. AES has the following properties:

- it is tamper-evident, i.e., once it is signed, the executed document cannot be changed without it being detected;
- ensures signature identification, i.e., there is certainty that the signature is uniquely linked back to the signer; and
- requires the involvement of a **secure electronic environment (a tool and/or a virtual platform only available to registered users)** where the e-signature is provided, stored and managed. For security reasons, such platforms need to be operated by a **trust service provider**, i.e., an entity responsible for assuring the electronic identification of signatories by using powerful technology for authentication, issuing digital certificates (e.g., time stamps) and e-signatures. The eIDAS Regulation defines how trust service providers perform authentication and non-repudiation services and how they are to be regulated and recognized throughout EU member states.[2]

✓ **Qualified e-Signature (QES)** adds an additional layer of security on top of AES: a qualified certificate, issued by a qualified trust service provider. This certificate is used to prove the identity of the signatory and confirm the authenticity of the e-signature attached to an electronic document. In Hungary, an e-document with an attaching QES qualifies as a private document with full power of evidence which has a higher probative value than a simple private document (enabled by AES). For a QES, the e-signature itself must be created through a special equipment (hardware) and/or software tool. Such **qualified e-signature creation device** ensures that:

- the signatory is the only one with control of the key used to create the electronic signature (i.e., the signatory "owns" the private key attached to his/her e-signature);
- the signature data is unique and protected from forgery; and
- the signature data is managed by a **qualified trust service provider**, i.e., an entity approved by the competent authorities in each jurisdiction responsible for assuring the qualified electronic environment for authentication, digital certificates, and e-signatures. Jurisdiction specific laws and the eIDAS Regulation define how qualified trust service providers perform their services.

Both standard e-signatures and AES have their place in business and private life use cases where trust between the parties is without doubt. Yet QES enables the strongest legal evidence when it comes to less (or possibly lack of) trust or even potential disputes between the parties. Also, when it comes to communication with government entities, public authorities in Hungary will typically require e-documentation to be submitted in a qualified form, i.e., accompanied by a QES.

Accordingly, while the eIDAS Regulation confirms the validity of each form of e-signature listed above, managing the legal risks related to e-documentation requires a careful, case-by-case evaluation of the context in which e-signature is to be applied.

This report provides a comparative overview of six electronic solutions to execute legally binding and officially acceptable e-documents in Hungary, followed by an in-depth analysis of each of these solutions and a brief insight on international e-signature tools.

[2] The list of EU trust service providers is published by the EU on this website: https://webgate.ec.europa.eu/tl-browser/#/

Comparative chart: electronic solutions to execute legally binding and officially acceptable e-documents in Hungary

	Available free of charge	No equipment is required for e-signing, e.g. no card or token needed	The e-signed document qualifies as a private document with full power of evidence in Hungary	Qualified e-signature recognised in all EU Member States	Qualified trust service provider registered in Hungary	Can also be used for corporate repre-sentation purposes without any limitation	The service provider enables very quick and 100% contact- and paperless onboarding of new users
1. AVDH	***X***	***X***	***X***		***X***		***X***
2. e-ID*	***X***		***X***	***X***	***X***		
3. NetLock*			***X***	***X***	***X***	***X***	
4. Microsec*			***X***	***X***	***X***	***X***	
5. Digitoll**						***X***	
6. TrustChain*		***X***	***X***	***X***		***X***	***X***

* Qualified Electronic Signature (QES)

**Advanced Electronic Signature (AES)

Six electronic solutions to execute legally binding and officially acceptable e-documents in Hungary

This section is an in-depth analysis of the advantages, need-to-know aspects, operational requirements, and scope of use of six tech-assisted solutions that we identified to have legally binding effect currently recognized by the Hungarian authorities.

1. e-Document authentication enabled by the Government ("AVDH")

The first item on our list is a smart trick-shot: AVDH is technically not an e-signature, but an e-document authentication solution provided by the Hungarian government for individuals who do not otherwise have access to e-signature solutions. While AVDH does not fall into either of the e-signature types listed by the eIDAS Regulation, it does enable identified private individuals to prove the authenticity of e-documents that they personally generated and submit these to public authorities (for example, to register company changes with the Court of Registration). The technology behind AVDH is enabled by NISZ Zrt., a state-owned entity that is both a qualified trust service provider and a government authentication service provider.

In order to use AVDH, individuals must be duly registered with the central electronic administration web portal in Hungary (in Hungarian: "*Ügyfélkapu*")[3] ("**Client Gate**"). The Client Gate is a virtual contact point created to enable direct connection between individuals and the government. It provides services not only to Hungarian citizens but also to other EU citizens who conduct business in Hungary or file their tax returns there.

The e-document uploaded to and e-authenticated through the AVDH platform will be (a) inseparably linked to the identity of the person identified through the Client Gate, and (b) certified and time-stamped by NISZ Zrt. In this case, the encoded key attached to the digital stamp is owned by NISZ Zrt. and used ("borrowed") by individuals for e-document authentication purposes. Accordingly, in the case of AVDH, individuals do not possess the private key attached to the digital stamp as would be the case with a private key offered by AES and QES solution providers (hence AVDH does not technically qualify as an e-signature, but basically serves the same purpose).

Advantages:

- **Free-of-charge and easy to use:** AVDH is highly popular because it is a free service that can be easily used by anyone with a Client Gate registration to create[4] a private e-document with full power of evidence[5] in Hungary. In practice, this means that any e-document authenticated with AVDH has the same legal effect as a paper-based document

[3] https://ugyfelkapu.gov.hu/
[4] Based on Section 325 (1) (g) of Act CXXX of 2016 on the Code of Civil Procedure.
[5] Unless proven to the contrary, a private document with full power of evidence proves with full probative value that the signatory of the document has made, accepted or agreed to be bound by the statement recorded therein.

executed between private parties in front of (and co-signed by) two witnesses in Hungary. Yet with AVDH, the creation of legally binding documentation is far more convenient as it sets aside the need for witnesses, printing or mailing paper-based documents or arranging any matter personally.

- **Immediately available solution:** accessing AVDH is instantaneous, i.e., it does not require any lengthy onboarding process that generally comes together with in-person identification, user registration or hardware and software installation requirements of e-signature service providers.
- **100% contact- and paperless process:** AVDH operates in a fully virtual environment.
- **No special equipment or software tool required for authenticating e-documents.**
- **Unlimited liability from the trust service provider:** with regard to potential damages resulting from incorrect electronic signatures, trust service providers typically limit their liability arising from the usability and conformity of the e-signature certificates they issue. Usually, higher liability limits come at a higher service price. In the case of AVDH, however, the trust service provider did not limit its liability for damages in connection with the free e-signature service[6], which is therefore a highly beneficial solution for users based in Hungary.

Need to know:

- **Data security considerations:** the technology behind AVDH operates in a highly protected government cloud. Further, the trust service provider is bound by professional secrecy obligations and must erase e-documents from its systems 24 hours after the upload. While these factors enable for a highly secure electronic environment, in the case of critically confidential e-documents, one shall carefully assess the data security risks given the uploaded e-documents' exposure to data breach during the 24-hour timeframe.
- **Client Gate registration requirements:** given the use of AVDH requires prior registration with the Client Gate, AVDH does not benefit users who were not previously identified by the Hungarian Government through the Client Gate.

How to start using AVDH? 7-step process that only takes a few minutes

With AVDH, a digital stamp can be easily placed on an e-document (PDF or other format) in just seven steps, provided that a computer, internet connection and Client Gate registration are available. We advise users to follow the below 7-step process:

1. Click on the government website provided by NISZ Zrt.;
2. Upload an electronic file from their device;
3. Choose one of the two options for e-document authentication (depending on the format and size of the file, as well as the form of authentication required by the public entity to which submission is made);
4. Accept the general terms and conditions with a checkmark;
5. Click on "Send Document";
6. Confirm identity through the Client Gate; and
7. Download the ready-to-use authenticated e-document (or send it to a selected e-mail address).

Scope of use: electronic public administration, as well as business and private electronic administration use cases where QES is not a mandatory legal requirement. For example, AVDH is appropriate for the purposes of company formation,

[6] General Terms and Conditions of NISZ Zrt. for Identification Based Document Authentication (AVDH)

registration of company changes, submission of a valid power of attorney or an application to any Hungarian authority, and also for the signing of employment-related documents.

2. QES linked to the e-identification card of Hungarian citizens ("e-ID") enabled by the Government

The new type of Hungarian identity card (personal e-ID) contains an electronic storage item (a chip) which also enables private users to apply for a free QES recognised in all EU Member States. The QES created with the e-ID enables Hungarian citizens to undertake legal commitments in their private or public administration matters by e-signing private e-documents with full power of evidence[7] in Hungary.

Advantages:

- **Free-of-charge QES:** the technology behind the e-ID is offered free-of-charge by the state-owned qualified trust service provider NISZ Zrt.

Need to know:

- **Exclusively created for the private use of Hungarian citizens:** the e-signature associated with the e-ID can only be used by Hungarian citizens in their capacity as private individuals. For example, it is a perfect solution for signing contracts with personal undertakings (e.g., purchasing a car or property) or submitting documentation to the public authorities as a private individual (e.g., public administration or employment-related filing). However, the e-ID must not be used for the public filing of e-documents in a business context, for instance it cannot be used by company representatives acting as authorized signatories of a legal entity. Certainly, the QES created by the e-ID will remain valid (and recognised in all EU Member States), but will not be accepted by government entities unless the submission is made in the capacity as a private individual.
- **Limited to a maximum commitment of HUF 50 million:** use cases for the e-signature created with the e-ID are limited by a transaction threshold of HUF 50 million. This limit applies to one e-document electronically signed with the e-ID, such as a sales contract.
- **Preliminary identification requires a one-time in-person meeting:** in order to use the QES attached to the e-ID, individuals must first obtain a valid e-signature certificate by applying in person to a public record office or a local government authority.
- **Requires special hardware and software tool:** in addition to a computer used for e-signing, individuals need to purchase an e-ID card reader device (to be connected to the computer) and install a suitable card reader application on the device used, as per the service provider's instructions.

Scope of use: limited to personal use in private or public administration matters, such as e-signing of sale and purchase contracts, employment agreements or filings with public authorities.

[7] Based on Section 325 (1) (f) of Act CXXX of 2016 on the Code of Civil Procedure

3. QES enabled by NetLock Kft. and Microsec Zrt.

NetLock Kft. and Microsec Zrt. are privately held qualified trust service providers registered in Hungary that issue e-signature certificates for the remote creation of QES. Both entities are certified EU trust service providers, as well. Their solutions enable QES suitable for creating private documents with full power of evidence in Hungary[8]. (*Note: both NetLock Kft. and Microsec Zrt. offer AES to their customers, yet for the purposes of this report we only looked at their QES services).*

Advantages:

- **QES suitable for both business and private use cases:** as qualified trust service providers, both NetLock Kft. and Microsec Zrt. guarantee adequate security for signatories in their business or individual capacity, from both legal and technical point of view.
- **Using QES via a web browser:** with a NetLock Kft. or Microsec Zrt. enabled card and card reader or token at hand, individuals can attach their QES to any e-document by using any web browser, irrespective of their location.

Need to know:

- **Requires prior in-person identification:** to certify the identity of the signatory and issue their private keys attached to the e-signature, both service providers require individuals to personally show up before handing over their e-signature certificates. This traditional and certainly one of the most secure ways of personal identification is currently the statutory minimum requirement for Hungarian trust service providers. (*Note: the Hungarian Ministry of Interior is currently working on a new piece of legislation allowing remote (video) identification by the Hungarian trust service providers beyond the temporary period allowed due to the Covid-19 pandemic).*
- **Requires special hardware and software tool:** NetLock Kft. and Microsec Zrt. provide customers with the technical devices (e.g., a card or token) and other accessories (e.g., the card reader if you choose a card) necessary for creating the QES. In addition, customers will also need to install applications on their computer to adequately manage their card or token, and then register their e-signature certificates via such applications. Both service providers provide detailed instructions on these steps.
- **Cost-based solution:** the QES enabled by both Netlock Kft. and Microsec Zrt. is a paid service. Prices reflect the software functionalities and trust services offered to users and range from basic to platinum level packages. (*Note: AES services have a lower price range at both NetLock Kft. and Microsec Zrt.*).

Scope of use: unlimited in both business and private context. The QES solutions enabled by the two Hungarian qualified trust service providers can be used without any restrictions for both corporate representation and private purposes. Most attorneys and in-house legal counsels practicing in Hungary also use one of these two QES solutions for e-signing.

[8] Based on Section 325 (1) (f) of Act CXXX of 2016 on the Code of Civil Procedure

4. AES enabled by Digitoll Kft.

Digitoll Kft. ("**Digitoll**") is a privately held non-qualified trust service provider registered in Hungary that issues e-signature certificates for the remote creation of AES. Digitoll is also a certified EU trust service provider. Its technology enables AES that is suitable for both business purposes (e.g., corporate representation) and private use.

In Hungary, an e-document with an attaching AES enabled by Digitoll qualifies as a simple private document signed on paper. While simple private documents have a lower probative value than a private document with full power of evidence (enabled by QES), the undertakings included in a simple private document are equally binding between the parties by the force of law. Accordingly, by using AES enabled by Digitoll, individuals can generate legally binding electronic statements equal to paper-based "written statements" acknowledged by Hungarian legislation[9] and case law[10] (as opposed to a simple e-mail for example which does not qualify as a "written statement" from a legal point of view).

Advantages:

- **AES suitable for both business and private use cases:** as a non-qualified trust service provider, Digitoll guarantees adequate security for signatories in their business or individual capacity, from both legal and technical point of view.
- **Cost-effective solution compared to QES:** AES solution providers (including Digitoll) generally offer lower prices to customers, given their solutions and trust services result in e-documents with lower probative value than e-documents attached with a QES. Accordingly, while Hungarian law confirms the validity of both AES and QES, managing costs and risks related to generating e-documentation will require a careful evaluation on a case-by-case basis.

Need to know:

- **More relaxed minimum legal requirements than those applicable for QES:** Digitoll is a non-qualified trust service provider and therefore -- from a liability and security point of view -- its services are subject to less strict minimum legal requirements than those applicable to qualified trust service providers.
- **Requires prior in-person identification:** Digitoll requires customers to show up in person for the purpose of certifying their identity. The process is similar to that described in Section 3 above and results in the issuance of a non-qualified e-signature certificate by Digitoll.
- **Requires special hardware and software tool:** Digitoll provides customers with a secure signature creation device (e.g., a card or token) and other accessories (e.g., the card reader if you choose a card) necessary for creating the AES. In addition, customers will also need to install an application on their computer to adequately manage their card or token, as per the instructions of the service provider.

[9] Based on Section 6:7 of Act V of 2013 on the Civil Code
[10] Court decision nr. ÍH 2005.164

- **Cost-based solution:** the AES enabled by Digitoll is a paid service. Prices reflect the software functionalities and trust services offered to users and range from individual customer to corporate level packages.

Scope of use: unlimited in both business and private context. The AES solution enabled by Digitoll can be used without any restrictions for both corporate representation and private purposes. For example, if there is a requirement for written statements to be made under certain contractual undertakings (while the full power of evidence is not needed for the entire document), Digitoll offers an adequate and cost-effective solution for issuing legally binding statements in an electronic format.

5. QES enabled by TrustChain Systems Kft.

TrustChain Systems Kft. ("**TrustChain**") is a privately held company registered in Hungary that operates a digital contracting platform and enables QES as part of their service offering to subscribers. The qualified trust service provider behind TrustChain is Bulgaria-based Evrotrust Technologies JSC ("**Evrotrust**").

Any document created on the TrustChain platform (or edited elsewhere but subsequently uploaded to TrustChain), may be signed by one or several persons using QES. The service is available not only in all EU Member States, but for citizens of 38 countries around the world, for both corporate representation and private purposes.

Advantages:

- **100% contact- and paperless onboarding:** TrustChain operates in a fully virtual environment. To use QES on the TrustChain platform, individuals do not need to show up in-person for certifying their identity, but can benefit from the video identification solution offered by Evrotrust (also conducted in Hungarian language by Hungarian-speaking operators).
- **Quick onboarding process:** accessing TrustChain is time-efficient, as users are saved from in-person identification meetings or hardware installation requirements.
- **No equipment (i.e., card, card reader or token) required:** registered users only need a computer, a smartphone, and internet connection. The TrustChain platform is accessible from any web browser, while the QES is applied via a smartphone application.
- **Integrated solutions for business purposes:** besides QES, TrustChain enables registered users to identify their business partners in an online, partially automated environment, enter into contracts, and also manage their financial processes virtually.

Need to know:

- **QES cannot be used independently from the TrustChain platform:** the e-signature solution is embedded into the business environment operated by TrustChain and can only be used for executing e-documents uploaded to the platform.
- **Executing e-documents is a cost-based service:** while identification and obtaining a QES are free of charge, executing an e-document via TrustChain has a net cost of 0.7 EUR per signature.

- **Requires software installation:** to complete the identification process (required for the issuance of the QES certificate), users are required to download the Evrotrust application to their smartphone and create their own Evrotrust account. Users will also need to link their TrustChain business account with their Evrotrust account by signing the Account Linking Statement sent to the Evrotrust application. Platform users can use their QES through the Evrotrust smartphone application.

Scope of use: the QES enabled by TrustChain can be used without any restrictions or limitations for both corporate representation and private purposes, yet limited to e-documents managed via the TrustChain platform, i.e. only accessible for TrustChain and Evrotrust customers.

Further e-signature solutions in international business context

While local laws (in Hungary and in other jurisdictions) will strictly define the legal and public administration context in which QES is required, trusted private and business relations generally allow for more flexibility among the parties when it comes to the security of e-signature and e-documentation. In fact, **the optimal flow of private and business relations requires that individuals engage with more trust and mutually accept more relaxed legal and technical requirements than those applicable for QES**. Hence standard e-signatures and AES may indeed have a widespread application in our everyday lives, in particular in a local business context or a multinational trade environment.

In addition to the e-signature solutions listed in the previous section of this report, each of which comply with the highest security standards in Hungary, individuals may as well access several other e-signature technologies. Under the eIDAS Regulation, most of these publicly available solutions qualify as **standard e-signature or AES services**, with the level of security set forth in each trust service provider's own terms and conditions.

With more than 500,000 customers and millions of signatures executed, currently **DocuSign** is the leading e-signature solution provider worldwide. Given e-signatures do not exist in a vacuum, but imbedded in complex legal and business workflows, technology vendors increasingly offer platform environments with value-added features accessible to their subscribers. For example, in addition to its AES tool, **Dealsign** enables users to create or upload document templates, manage clause variations within templates, negotiate contracts real-time in a virtual environment, track changes by all parties in the activity log, and securely store and search agreements in a cloud-based repository. Technology vendors will often help connect with several existing applications and offer software integrations.

Businesses that implement e-signature solutions need to consider the operational and strategic impact both in their local and international environments. The impact of adopting e-signatures may be significant and therefore requires consultation on the key aspects before implementation, or wider roll-out in an organization.

Conclusions

In the current times of change, when we are rapidly moving to a digital economy that increasingly relies on data and electronic workflows, using e-signatures is becoming a standard practice in everyday private and business matters. To manage the legal risks related to e-documentation and choose the adequate e-signature solution for local and international trade in Hungary, we advise as follows:

- carefully evaluate on a case-by-case basis the actual context in which e-signature is to be applied;
- make sure to understand the mandatory local laws that require for QES – remember, QES enables the strongest legal evidence when it comes to less (or possibly lack of) trust or even potential disputes between the parties and communication with the public authorities; and
- where appropriate, consider using standard e-signatures and AES in business and private life use cases – compared to QES, these solutions offer flexibility and cost efficiency in exchange for lower levels of security.

Overall, each e-signature service provider's goal is to create better customer and employee experiences, while enabling electronic administration faster, with less risk and at lower costs. Yet the adoption of e-signatures is not just a legal and information security issue. In fact, an essential aspect to consider is how technology changes the way we manage everyday matters, how legal and business teams perform work, and what risks and costs may be involved in digital transformation projects. Individuals and businesses need to place e-signature solutions into context and consider the operational and strategic impact they have. The impact of adopting e-signatures may be significant and therefore requires consultation on the key aspects before implementation, or wider roll-out in an organization.

Resources

Applicable legislation:

eIDAS Regulation - 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

Act CCXXII of 2015 on the general rules for electronic administration and trust services

Decree 24/2016 (VI.30) of the Ministry of the Interior on the detailed requirements concerning trust services and their providers

Government decree 451/2016 (XII. 19) on the detailed rules of electronic administration.

Act CXXX of 2016 on the Code of Civil Procedure

Act V of 2013 on the Civil Code

Other sources:

The professional opinion of the Hungarian Electronic Signature Association on the use of AVDH, dated on 31 March 2020

The list of EU trust service providers is published by the EU in a publicly accessible way, their list is available by clicking here

Hungarian qualified trust service providers are registered by the National Media and Infocommunications Authority, their list is available by clicking here

NISZ GovCA Regulations - Trust Service Regulations for Qualified Certificates Issued for Identity Cards (BSZ-ESZIG)

Official website of NISZ Zrt.

General Terms and Conditions of NISZ Zrt. for Identification Based Document Authentication (AVDH)

Electronic document authentication in practice: this is how AVDH works (magyarorszag.hu)

eszemelyi.hu

NISZ Zrt. information on the services related to e-signature that are available with a personal identity card

Official website of NetLock Kft.

Official website of Microsec Zrt.

Official website of Digitoll Kft.

Official website of TrustChain

Official website of DocuSign

Official website of Dealsign

About the Authors

Dr. Orsolya Szabó is a lawyer-entrepreneur who launched **InvestCEE LegalTech Consultancy** in 2017 to help legal teams succeed on their digital transformation journey. Following a legal career with global law firms' M&A teams working on cross-border transactions across Central Eastern Europe (CEE), Orsolya now advises corporate legal departments and law firms in the CEE region to optimize legal work with technology. She regularly holds workshops and webinars on digital legal services and manages technology implementation in client projects.

Contact: orsolya.szabo@investcee.hu

To enable legaltech implementation projects, **InvestCEE LegalTech Consultancy** carefully selects legal technology tools (some of which are sourced via the **InvestCEE LegalTech Marketplace**) and facilitates pilot projects in close collaboration with the client teams. By helping clients meaningfully engage with legal technology, InvestCEE empowers corporate legal departments and law firms to offer increasingly value-added services.

To find out more information, please visit **investcee.hu**.

Dr. Kinga Madocsai is an attorney in Hungary and alternative dispute resolution expert with a special focus on civil & corporate matters, commercial law, asset management, insolvency and environmental law practice areas. She co-founded **SimpLEGAL**, a new generation digital law firm based in Hungary that aims to be the colloquial synonym of being completely client- and solution focused legal service, keeping an eye on all possible alternative and state-of-the art legal solutions. SimpLEGAL is the only law firm member of the **Hungarian Electronic Signature Association**, a group of experts in e-signing in Hungary.

Contact: madocsai.kinga@simplegal.hu

With the aim of delivering results by making the most of digital technologies for clients in any 21st century scenario, **SimpLEGAL** was designed to be a full service digital law firm. SimpLEGAL offers solutions and special expertise in IP, technology, privacy and data protection law. The SimpLEGAL team particularly focuses on comparative digital privacy, the international regulation on AI, novel technologies and cybersecurity.

To find out more information and contact details, please visit **simplegal.hu**.