Electronic Signatures
Signing electronically with legal certainty
The electronic signature – a good “support” in times of Corona?

In the era of the “digital economy” (more than a third of Germans now prefer shopping done online and even more than half of all Germans shop using a mobile device\(^1\)), companies are increasingly questioning why their contracts and customer/supplier interactions cannot be moved to an entirely paperless model.

Particularly with the insights gained during the Corona crisis, companies will have to think more intensively about this topic in the future. After all, contactless interaction with customers and suppliers is recommended to protect employees, customers, and suppliers from getting ill. Digital business operations that are as contact-free as possible lower the risk of getting an infection. For this reason, electronic signatures can no longer be regarded as a “nice-to-have” but much rather as a “must-have”.

Many banks, insurance companies, retailers, telcos, utility providers, software and app vendors, and airlines have all been successful in shifting some (if not all) of their consumer contracting to an online model; ticking a box is sufficient to confirm a transaction and accept associated terms and conditions.

To tackle the B2B market, encouraged by favourable regulatory regimes in Europe, the US and other countries, the range of services providing electronic signatures has recently increased significantly. In addition to DocuSign, which claims, for example, to have “more than 500,000 customers and hundreds of millions of users in over 180 countries using their services”\(^2\), there are also start-ups such as “Skribble”, which handle signature processes digitally and which – according to their own statements – are legally valid according to Swiss and EU law.\(^3\)

Furthermore, Adobe asserts that an electronic signature solution can “cut the cost and hassle of paper-based tasks” and “speed business transactions.”\(^4\)

Even the business operations of the German justice system are becoming increasingly digital. From 01 January 2022 onwards at the very latest, all lawyers will be obliged to transmit documents to courts electronically. This is done via a special electronic lawyer mailbox (“besonderes elektronische Anwaltspostfach” (“beA”)). Hence in the future, pleadings will only be signed and submitted via electronic signature.

This development shows that companies are building their proceedings on the use of the electronic signature and, therefore, should implement it in their business operations.

However, the absence of globally harmonised legislation, coupled with cumbersome local laws, have, at least historically, led to uncertainty around the scope of application and validity of electronic signatures. Likewise “Cloud” delivery models (employed by the majority of service providers) present challenges, particularly from the point of view of data security and data residency.

We seek to address some of those issues in this briefing.

---

1. PWC-Study „Total Retail 2016 – der Wettlauf um Relevanz“.
What is an electronic signature?

The eIDAS Regulation defines the electronic signature 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”.

According to eIDAS, electronic signatures can be categorised as “simple”, “advanced” or “qualified”. This complex designation hides a much simpler reality – most users may not realise that they are “signing” contracts electronically by:

- chip & pin or contactless transactions;
- ticking “I accept” or “submit” in online purchases;
- signing their name at the end of an email; or
- using biometric signatures (fingerprint and facial recognition).

In the business environment, electronic signatures can be used as a vehicle to expedite, simplify and manage the contract execution process. Electronic contracts can be circulated, signed, authenticated and loaded in a matter of minutes.

Parties to an agreement can select the electronic signature method which best suits their authentication requirements. Good practice dictates that “advanced” or “qualified” signatures should be used for high value or strategic agreements as they:

- identify the signatory with a high degree of certainty;
- limit the risk of 3rd party interference or fraud; and
- limit the risk of subsequent amendment or revocation

and thus enable the parties to validate the integrity of the signature and, in turn, the enforceability of the contract.

“Qualified” electronic signatures supplement “advanced” electronic signatures by mandating the use of software or hardware tools to create codes or cryptographic keys (certificates) issued by trust service providers and used to validate the authenticity of the signature. The devices and trust service providers must be “qualified”, – that is to say they must meet the requirements of eIDAS, be registered with the supervisory body in the relevant member state and notified to the European Commission. According to German law, only a “qualified” electronic signature meets the legal requirements of the statutory written form (see § 126a German Civil Code (Bürgerliches Gesetzbuch (“BGB”))).

---

6 We use the term “simple” to highlight those identification and trust services for which no special conditions apply. For more information on “advanced” and “qualified” electronic signatures, see below.
7 For recommendations, see Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnologie), Fundamentals of Electronic Signature, 2006 (Grundlagen der elektronischen Signatur, 2006) (currently under revision).
8 eIDAS Article 26.
9 eIDAS Article 28 – An “advanced” electronic signature based on a “qualified certificate” issued by a “qualified electronic signature creation device” issued by a “qualified trusted third party service provider”.
10 In Germany, the Federal Network Agency (Bundesnetzagentur) maintains a so-called “Trusted List”, in which all qualified trusted service providers are included, and is responsible for the accreditation of certification service providers (e.g. TÜViT); see also: https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Overview+of+available+attributes+of+pre-notified+and+notified+eID+schemes.
Electronic signatures and the legal landscape

Already in 1997, Germany was the first country to introduce a signature law. In 1999, the European Union\(^1\), Australia and the United States\(^2\) followed with codifying the treatment of electronic signatures.

Subsequently, the German Signature Act was adapted to meet the European standards, as the requirements of German law were too strict.

The European Union, Australia and the United States all recognised the validity of electronic signatures for the conclusion of contracts and their admissibility as evidence in legal proceedings; all stipulate that a contract cannot be denied legal effect solely on the grounds that they are in electronic form.

So far, so good. However:

- the EU and the US model required states or member states to adopt the legislation; in Europe in particular this created a fractured legislative landscape;\(^3\)
- the legislation (in the interests of being technology neutral) did not stipulate what it regarded as an “electronic signature” but defined them by a set of qualifying criteria;
- the European Directive established a two-tier process for “simple” and “advanced” electronic signatures which introduced uncertainty as to the legal effect of the poorer sibling; and
- the legislation was subordinate to existing legislation applicable to specific legal instruments (for example property transfers).

The position in the European Union changed in July 2016 when eIDAS came into force. eIDAS is directly enforceable across member states and replaces the existing Directive. eIDAS is designed firstly to ensure a more harmonised approach with respect to the recognition and enforceability of electronic signatures. eIDAS is also designed to build a consistent framework for secure electronic authentication by defining mutually recognised, pan-EU rules for:

- electronic signatures (simple, advanced and qualified);
- electronic identification schemes (classified low, substantial, high);
- electronic seals (simple, advanced and qualified);
- trust services (simple, advanced and qualified);
- electronic time stamps (simple and qualified);
- electronic registered delivery services (simple and qualified);
- electronic documents (simple); and
- website authentication (qualified).

From a German point of view, this harmonisation leads to a reduction of the legal requirements for electronic business processes in many areas. As a result, under eIDAS, it is possible for the first time in Germany, for example, to use the so-called “remote signature procedures”. Here, a service provider takes over the technical processing of the electronic signing of documents “remotely” and thus considerably facilitates the use of electronic signatures – for both the company and its customers.

\(^1\) Directive 1999/93/EC on electronic signatures.


\(^3\) In Germany, the Digital Signature Act and Digital Signature Ordinance have been particularly relevant so far.
Benefits of
electronic signatures

According to the providers of electronic signature procedures, the electronic conclusion of contracts has numerous advantages.14

Speed
Electronic signatures enable contracts to be executed and returned in a matter of minutes, on any device by geographically-dispersed signatories.

Security
Contracts executed by an electronic signature, particularly when overlaid with authentication tools, are inherently more secure and harder to forge than paper-contracts.

Traceability
Electronic signatures are traceable and auditable; workflow tools enable companies to track the status of contracts in real-time. When using an electronic signature, there is the option to get a time stamp inserted by a third-party provider. Such a time stamp has the advantage that the parties no longer need to rely on the local system’s time and that the signer no longer has to enter the date and time manually. Instead, the date and time at which the signature was inserted is retrieved by a trusted third-party provider from a standardized service (e.g. some certification bodies, such as GlobalSign, offer this service).15 The timestamp enables time-critical transactions, as the time and date when the signature was added can no longer be denied.

Integration
Electronic signatures can be integrated with existing CRM, procurement, accounting, HR and document management systems to provide end-to-end workflow management.

Legally binding
Contracts that are signed by means of a qualified electronic signature are legally binding, as they comply with the statutory written form requirement under German law. Accordingly, declarations made by means of a qualified electronic signature are legally relevant and cannot be withdrawn without further ado.

Ease of use
Execution processes by electronic signature are technology-neutral, intuitive and culturally accepted by the digital generation.

Costs
Whilst there will be inevitable up-front / ongoing charges for implementing an electronic signature solution, vendors argue these will be offset by closing contracts more quickly, introducing certainty, saving management time, facilitating contract management and eliminating courier fees.

---

14 This is a summary of the advantages stated by the providers and does not reflect the opinion of Eversheds Sutherland – the actual benefits depend on individual circumstances.
15 https://www.globalsign.com/de-de/timestamp-service.
Barriers to introduction of electronic signatures

Under the new EU legislative framework, and with technology embedded in popular culture, most documents can be executed electronically – from confidentiality agreements, to contracts of employment.16

Retail banks, for example, can even use electronic signatures for consumer loans.17

However there remain some barriers to the use of electronic signatures for certain documents in some jurisdictions, for example:

- deeds, wills18 and trust documents;
- healthcare proxy;
- guarantee agreements;19
- marriage, birth, divorce, and death certificates;
- certain real estate agreements;20
- other official documents required to be submitted in paper form; and
- agreements which stipulate that they can only be signed or varied by agreement "in writing and signed by hand".21

It is therefore advisable for companies to seek specialized legal advice and develop a corporate policy that takes into consideration the regional legal requirements in the jurisdictions relevant for the company.

This especially applies to companies that are active or intend to become active in the German market, as German law contains some comparatively strict legal requirements in this respect.

In addition, the previous regulations on electronic signatures in Germany have always been subject to strict interpretation. This should be taken into account when making a legal assessment of newly introduced processes due to potential risks of possible ineffectiveness of electronically signed contracts, especially when using innovative, yet completely untested technologies.

---

16 However, according to German law (§ 623 BGB) electronic form and thus the use of electronic signatures is excluded for the termination of employment relationships. Same applies in accordance with § 109 Abs. 3 GewO (German Industrial Code) for issuing an employer’s reference.

17 § 492 (1) BGB in conjunction with § 126a BGB.

18 Under German law, a testament usually needs to be drafted “by hand”, which excludes the signing by means of an electronic signature (§ 2247 BGB).

19 Under German law, however, the Federal Court of Justice (BGH, ruling of 28.10.1963, ref. III ZR 153/62) considers that the conclusion of a guarantee contract is possible without any formality.

20 For example, for the creation of a land charge, German law regularly provides for notarial certification (§§ 873, 1115, 1192 BGB).

21 According to German law, however, an agreed written form can be maintained by transmission by email or fax (§ 127 BGB) or by using a qualified electronic signature (§ 126a BGB).
Selecting a provider for electronic signatures

There are a myriad of electronic signature service providers. Regarding the German market, the ones that stand out are the Bundesdruckerei, DATEV and IDnow. The major global players include DocuSign, Adobe, Silanis and ARX20.22

Some suppliers offer an “on-premise” solution (i.e. where the software is hosted by the customer) but most are now cloud-based.

Furthermore, many solutions are compatible with mobile devices (enabling tablet or smart phone signatures), and offer custom branding so they can be white-labelled or “integrated” with existing CRM or ERP systems.

Most providers offer multiple authentication options (from public/private keys to biometric signature verification).

Many providers warrant that they are compliant with existing legislation (including eIDAS and the US ESIGN Act).23

Given the range of vendors and features, it will be important for businesses to conduct detailed due diligence and vendor selection taking into consideration:

- legal compliance of the certification of provider and solution offered;24
- functionality and ease of use;
- pricing plans and options;
- performance and availability requirements;
- integration and compatibility with existing CRM/ERP systems;
- scalability and flexibility;
- data privacy, data security and data residency requirements;
- compliance with the requirements of regulatory authorities such as the German Federal Financial Supervisory Authority (BaFin) or the requirements of Solvency II24;25 and
- other applicable terms and conditions.

---

22 See the study carried out for the EU Commission by Cavallini et al. (2012), "Study on the supply-side of EU e-signature market", Final Report for the DG Information Society and Media of the European Commission.

23 It is not always certain whether their products meet the requirements for “qualified” electronic signatures.

24 In this respect, companies can, for example, make use of the certification lists of accredited certification service providers; the corresponding list of TÜV IT shows, for example, that the trust service “e-Szignó Qualified Signature” has been certified according to eIDAS for Microsec Ltd.

25 Directive 2009/138/EC, which harmonises the risk and capital requirements for European insurers.
Basic contractual principles apply

It must not be forgotten that traditional legal principles apply to contracts concluded electronically. An electronic signature should therefore be particularly suitable as evidence for the intention to be legally bound.

However, it is also important to define a solution or a process which enables: the incorporation of applicable terms; validation that signatories have adequate capacity and delegated authority to sign; certification that the agreement has not been varied; and an actionable change-control process. It may also be recommended that parties include clauses that recognise the parties’ intention to be bound by an electronic signature.

Some practical considerations

Effective risk management for erroneous (or fraudulent) contracts is particularly important for companies that want to use an electronic signature solution for the purpose of contract signatures.

Robust security procedures and HR policies should control the risk of physical IT assets being left unsecured or the sharing of passwords and access keys. Companies should also review existing contracts, as the terms and conditions for customers, suppliers and/or employees may need to be adapted to allow for electronic signatures. The same applies to internal governance procedures, ensuring that contracts or purchase orders have been authorised and signatories have appropriate delegated authority.
De-Mail and video identification

Under German law, the introduction of the so-called "De-Mail" in a field related to electronic identification had already created a possibility to prove the access and content of electronic mail in court proceedings.

In addition, Deutsche Post AG has been offering the so-called "e-Postbrief" in Germany for many years, which, although not having comparable legal effects, has nevertheless been met with great acceptance among companies. In the meantime, the providers of De-Mail platforms (in particular 1&1, Deutsche Telekom and Mentana) have also had trusted their services for the delivery of electronic registered mail certified according to the requirements of eIDAS. Based on their experience with De-Mail, these companies should be well prepared for the future.

Even though eIDAS was initially associated with a loosening of the requirements for electronic business processes – especially in regards to the first-time possibility of using remote signature procedures – the BaFin caused a stir with its circular 04/2016 (GW) on video identification procedures in the financial services industry. According to this circular, identification via live video transmission – an essential component of current remote signature procedures – should in future only be possible for banks in view of the existing identification obligations under money laundering law. Not least due to strong criticism from all areas of the financial services sector, the BaFin has meanwhile repealed this circular (which had been suspended in the meantime) and replaced it by the circular 3/2017(GW) which came into force on 15 June 2017.

According to this circular, video identification procedures may be used by all entities obliged under the Money Laundering Act who are under the supervision of the BaFin. It also contains detailed requirements for the implementation of such procedures, which should be observed – also regarding remote signature procedures. Due to the different requirements regarding the video identification procedure in the respective EU countries, a precise legal examination of the respective identification procedure under consideration is necessary in each case. In Germany, for example, according to the BaFin, it is necessary to communicate with the person to be identified to be able to check the plausibility of the individual’s details.

Policy review and implementation

Introducing electronic signatures requires a mix of technology, legal advice and practical experience.

Our Technology team can help clients defining business objectives, reviewing and selecting providers of electronic signatures, evaluating legal requirements and introducing streamlined contractual processes. With the strength of our global network, we help multi-national clients define global policies, taking into account local law, custom and practice. For more information on the legal position regarding contracts that are subject to English law, please click here.

The circular is available under the following link: https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Rundschreiben/2017/rs_1703_gw_videoident.html.

Dr. Lutz Schreiber
Partner
T: +49 40 808094 444
F: +49 40 808094 199
lutzschreiber@eversheds-sutherland.com

Sara Ghoroghy
Associate
T: +49 40 808094 446
F: +49 40 808094 199
saraoghoroghy@eversheds-sutherland.com