

ELECTRONIC SIGNATURE PLATFORMS KEY CONTRACTUAL ISSUES

Richard Oliphant of K6 Partners examines the new EU law on electronic signatures and the main legal issues for UK businesses arising when using a contract to use an electronic signature platform.

The EU Regulation on Electronic Identification and Trust Services in the Internal Market (910/2014/EU) (the Regulation) and strong endorsement of electronic signatures by The Law Society and The City of London Law Society (CLLS) have led to rising demand for web-based electronic signature platforms.

The leading platforms, such as DocuSign and Adobe Sign, are transforming the way that business is conducted in the digital era and are integral to the success of the European Commission's (the Commission) digital single market strategy.

This article outlines:

- The new EU law on electronic signatures.
- The three types of electronic signature recognised by EU law and their characteristics.

The key legal issues facing UK businesses when they contract to use an electronic signature platform.

THE LAW ON ELECTRONIC SIGNATURES

The Single Market Act presented by the Commission in 2011 set out 12 policy initiatives to boost growth and strengthen the economy in Europe (www.practicallaw. com/6-513-7368). They included the overhaul of the Directive on Electronic Signatures (1999/93/EC) (the Directive). The Directive gave discretion to EU member states over the implementation of its provisions into their national law. Unfortunately, this resulted in a patchwork of disparate electronic signature laws and a failure to agree common technical standards stymied cross-border e-commerce.

The Commission was also mindful that the Directive had not kept pace with technology. It was no longer fit for the digital age in

which cloud and mobile technologies are transforming how business is conducted. For example, the Directive envisaged the creation of digital signatures using physical smart cards and USB tokens; but cloud technology now enables, and the Regulation explicitly allows, signatories to create and validate digital signatures with a mobile device such as a smartphone.

The Regulation

Given the haze of the fall-out from the 2016 referendum on leaving the EU, it is understandable that the Regulation has passed many people by. It came into force on 1 July 2016, repealing the Directive and establishing an EU-wide legal framework for electronic signatures and a range of other trust services including electronic seals and timestamps.

The aim is to help businesses, consumers and public sector bodies to carry out convenient and secure electronic transactions across the EU and advance the Commission's flagship digital single market strategy (see News brief "A digital single market: the European Commission unveils its strategy", www.practicallaw.com/7-614-4193).

Law Society practice note

With commendable speed, a joint working party of The Law Society and CLLS (the working party) published a practice note at the end of July 2016 endorsing the use of electronic signatures (the practice note) (www.lawsociety.org.uk/support-services/advice/practice-notes/execution-of-adocument-using-an-electronic-signature; see News brief "Electronic signatures: a watershed moment and the rise of platforms", www. practicallaw.com/0-632-8906).

The practice note provides welcome guidance for lawyers on the legal requirements for electronic signatures in commercial transactions under English law. The note was approved by leading counsel, Mark Hapgood QC. It underlines that where English law imposes a statutory requirement for a contract to be in writing or signed, such as a guarantee under section 4 of the Statute of Frauds 1677 or a disposition of an interest in land under section 2 of the Law of Property (Miscellaneous Provisions) Act 1989, this requirement is met with an electronic signature. Golden Ocean Group Ltd v Salgaocar Mining Industries PVT Ltd and another held that an electronic signature in English law has the same legal status as a wet-ink signature, the key question being whether the purpose of the signature is to authenticate the document ([2011] EWHC 56 (Comm); www.practicallaw.com/2-519-6232).

The working party's terms of reference did not extend to consumer contracts, but the rules of authentication are broadly the same as for commercial transactions.

Electronic signature platforms

Where contracting parties are unable to attend and sign documents at a meeting, their lawyers will organise a virtual signing. In May 2009, a joint working party of the CLLS published a guidance note on the options for execution of documents at a virtual signing (www.citysolicitors.org.uk/attachments/article/121/20100226-Advice-prepared-on-guidance-on-execution-of-documents-at-a-virtual-signing-or-closing.pdf).

Requirements for an advanced electronic signature

Article 26 of the Regulation on Electronic Identification and Trust Services in the Internal Market (910/2014/EU) states that an advanced electronic signature must be:

- · Uniquely linked to the signatory.
- · Capable of identifying the signatory.
- Created using electronic signature creation data (that is, a private encryption key)
 that the signatory can, with a high level of confidence, use under his sole control.
- Linked to the signed data in such a way that any subsequent change in the data is detectable.

The parties typically sign the signature page and their lawyers exchange a scanned copy by email to complete the transaction. But innovative law firms are moving away from virtual signings in favour of electronic signature platforms; these platforms create electronic signatures that offer greater authenticity and security than a scanned signature.

The advantages of using an electronic signature platform over other methods of electronic signature and the traditional handwritten signature are compelling: the workflow is faster than a conventional signing, scanning and email process and, as a result, it is more efficient and can save costs.

Perhaps the most significant advantage from a legal perspective is the digital audit trail generated for each transaction, recording who signed the document, including their email and IP address, when and, sometimes, where the document was signed. This audit trail is admissible in legal proceedings under section 7(1) of the Electronic Communications Act 2000 and carries substantial evidential weight in proving the authenticity or integrity of a disputed document.

ELECTRONIC SIGNATURES IN TRANSACTIONS

There are a number of practical issues that a UK business needs to consider when electing to use electronic signatures in its commercial transactions.

Types of electronic signature

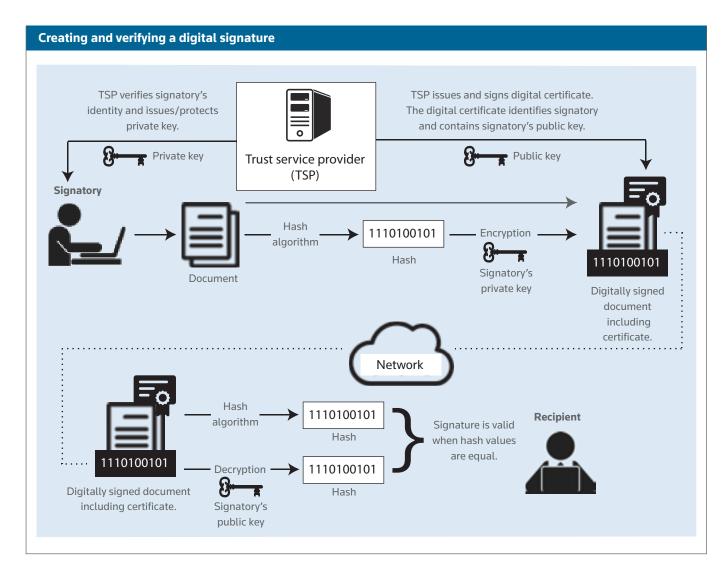
The Regulation defines three types of electronic signature: electronic, advanced and qualified.

Electronic signature. A standard electronic signature means "any 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" (*Article 3(10), the Regulation*). In other words, it is the electronic equivalent of a handwritten signature and can range from a typed name in an email to biometric data, such as a retina scan.

An electronic signature platform typically allows the signatory to write his signature directly on the document (with a stylus or mouse) or to select a computer-generated signature from a variety of fonts and styles. The standard signature product tends not to involve any independent third-party verification of the signatory's identity and corresponds to the definition of electronic signature under the Regulation.

Advanced electronic signature. An advanced electronic signature (AES) is a more sophisticated and secure form of electronic signature. It is a digital signature that is created with public key cryptography (PKI) and inserted into the code of the electronic document. The legal requirements for an AES are laid out in Article 26 of the Regulation (see box "Requirements for an advanced electronic signature").

The Regulation itself is technology-neutral and does not prescribe how these requirements should be met. There is little in the way of guidance from EU courts, but the Forum of European Supervisory Authorities for Electronic Signatures issued a working paper in October 2004 when the Directive was still in force, stating that an AES is usually achieved by using PKI technology.



To create a digital signature like an AES, the platform provider uses a mathematical algorithm to generate a public and private key, known as a key pair. The signatory uses the private key to encrypt a computergenerated fingerprint of the electronic document called a hash. The encrypted hash is the digital signature. It is sent with the electronic document to the recipient. The recipient uses the signatory's public key to decrypt the digital signature and verify that it could only be created by somebody with access to the private key. The recipient also generates their own hash of the electronic document and compares it with the decrypted digital signature. If they match, it means that the digital signature is valid and could not have been tampered with.

One potential drawback is that the key pair could easily be forged, stolen or created using a fictitious identity. Digital certification is used to manage this risk. The platform provider or, in some instances, a trusted third party (trust service provider) generates and manages the key pair, and verifies the signatory's identity by, for example, checking his passport. The trust service provider issues and signs a digital certificate, which affirms the signatory's identity and contains the signatory's public key. The digital certificate is cryptographically bound to the electronic document (now bearing the digital signature). The recipient is assured that the signatory is who he purports to be and uses the signatory's public key to validate the digital signature (see box "Creating and verifying a digital signature").

Qualified electronic signature. The third type is the qualified electronic signature (QES). This is also a digital signature created by a qualified electronic signature creation device. It provides the highest level of admissibility in the EU courts and has the equivalent legal effect of a handwritten signature (Article 25(2), the Regulation).

A QES must meet the requirements for an AES and be supported by a qualified certificate issued by a qualified trust service provider, whose credentials have been

recorded in a trusted list published by a member state (Article 22, the Regulation). A trusted list includes information relating to the qualified trust service provider supervised by the relevant member state, and the scope of the qualified trust services it provides. A trusted list has constitutive effect, meaning that the qualified trust service provider will only be qualified if it appears on a trusted list (https://ec.europa.eu/digital-single-market/ en/eu-trusted-lists-trust-service-providers).

As with an AES, the qualified trust service provider must verify the identity of the signatory and issue a "qualified certificate" to validate that the signatory is who he claims to be (see box "Creating and verifying a digital signature").

A QES is mandatory for certain transactions in civil law countries. For example, in Germany, where the law requires a contract to be in the written form, Article 126 of the German Civil Code provides that this requirement can be fulfilled electronically, but only with a QES. By contrast, there is no contract under English or UK law that would require the use of a QES and they are seldom used to conduct business in the UK.

Choosing a signature

Although all three types of electronic signature are admissible as evidence in legal proceedings before an EU court, a business still needs to consider which form of signature to use. This is where recital 49 of the Regulation comes into play. It says that national law still determines the legal effect of electronic signatures. In practical terms, this means that a UK business and its lawyers must evaluate the use of an electronic signature for each transaction on a country-by-country basis and be aware that the governing law may either:

- Prohibit the use of an electronic signature altogether (for example, a document under German law may have to be signed before a civil notary).
- Require an AES or QES to legally authenticate the transaction.

UK businesses favour, and the working party practice note advocates, standard electronic signatures for most commercial and consumer contracts governed by English law. There are, of course, some exceptions: HM Land Registry and the Stamp Office only register documents bearing a wet-ink signature.

Scottish law diverges from English law and requires an AES for the limited number of transactions that must be put in writing, including documents relating to land or trusts. It should also be noted that there is a preference in certain regulated industries, such as banking and pharmaceuticals, for the added security and more rigorous identity-proofing afforded by AES and QES.

Deeds

The working party confirmed in the practice note that an English deed may be validly executed with an electronic signature. If the deed needs to be witnessed, the working party recommends that the witness physically observes signature of the deed. While caution is advisable with deeds, this seems unduly conservative; there does not appear to be any legal impediment to the witness attesting the signature using video technology. (For background, see feature article "Execution and delivery of deeds: are we all on the same page?", www.practicallaw.com/3-506-6490.)

CONTRACTING ISSUES

Should a business decide to engage an electronic signature platform provider, it will need to agree the contract for the provision of these services. There are a number of key issues that practitioners should be aware of when reviewing and negotiating these terms.

The platform

Although some providers give customers the option to deploy the electronic signature platform on premises or on a private cloud, it is more commonly offered as a public cloud service.

Providers use the software as a service (SaaS) delivery model, which involves hosting the software applications and storing customer data on shared IT infrastructure. The customer and its authorised users typically access the platform with a web browser on a subscription basis for a fixed term of one to three years.

The SaaS model brings obvious benefits for customers, particularly in terms of scalability, lower cost, and operating as a permanent beta (that is, customers access the most upto-date version of the platform without paying for costly upgrades). However, cloud customers relinquish control over the processing and storage of their data. Ensuring compliance, particularly with a customer's obligations under the Data Protection Directive (95/46/EC) (Data Protection Directive) and, where applicable, the FCA Handbook, presents a challenge.

Authentication of signatories

The basic method of authenticating a signatory is to use an email address. This will be sufficient for most transactions under UK law. If the customer wants more certainty, it may opt for two-factor authentication such as an SMS, one-time password or knowledge-based authentication to verify each signatory's identity. In the author's experience, more and more UK businesses are opting for two-factor authentication. It adds rigour to the signature process, but is less cumbersome and significantly cheaper than obtaining an AES or QES.

These additional authentication services are provided by third parties and resold by the platform provider to the customer on an "as is" basis. But customers should push the provider to warrant the performance of these services or insist that any service credits that a provider recovers from the third party are passed on to the customer.

Integration with other enterprise applications

The leading platforms have pre-built integrations with enterprise applications like SalesForce, Microsoft and Google. They also offer application programming interfaces (APIs) that enable customers to integrate electronic signatures with their own proprietary business systems. This functionality is very important for customers but providers' standard terms do not offer a warranty.

The customer should ensure that there is a technical specification for integration of the platform with other applications, and require the provider to warrant that the integration will function substantially in accordance with that specification.

Electronic signature warranty

The warranties offered by a provider are sparse, even by the modest standards of SaaS sellers. If acting for a customer, practitioners will need to redress the balance. The key warranty is that the customer's use of the platform in accordance with the technical specifications(s) will produce an electronic signature that conforms with the requirements of the Regulation, or the Electronic Communications Act 2000, or both. If the signature is an AES, the provider should also warrant that the signature and related digital certificate conform with the requirements of Article 26 of the Regulation.

Providers are understandably reluctant to warrant that the electronic signature creates a valid and enforceable contract. The provider has no visibility of what contract is being signed, the governing law or the jurisdiction where a disputed contract may be enforced. As noted above, national law still determines whether a contract may be concluded by electronic means or if a specific form of electronic signature is necessary. This judgment rests with the customer and its lawyers. Moreover, the provider will require the customer to warrant that its use of the platform is in compliance with all applicable laws and regulations.

The value of technical standards

The Regulation is technology-neutral. This is an important principle. The Commission recognises that technology is not static and that new technologies will emerge to enable the creation and validation of electronic and digital signatures. Therefore, the Regulation does not mandate that platforms use a particular technology.

Nevertheless, the leading providers make bold claims about their adherence to, and importance of, technical standards approved by bodies like ETSI, ISO and CEN. These technical standards do sway the customer's (and its chief technology officer's) choice of platform. But practitioners should recognise that technical standards are really just tools that a provider uses to demonstrate its compliance with the requirements of the Regulation; a warranty that a platform adheres to an ETSI technical standard (for example, CAdES, XAdES, PAdES) has merit, but it is no substitute for a warranty that the platform creates signatures that comply with the requirements of the Regulation.

Service level agreements

A provider will not volunteer a service level agreement (SLA), so customers should ask for one and ensure that the provider is operating the platform to the required standard. If the service falls below this standard, service credits will be payable to the customer. Providers are unlikely to agree to a right of termination, even for persistent breaches of the SLA.

The key metric in the SLA is the availability of the platform. The leading providers host customer data on multiple servers across several data centres. This means that any scheduled or emergency maintenance will not affect the availability of the platform and the leading providers will commit to 99.9% or even 100% availability during the term of the contract.

Limitation of liability

The leading providers look to cap their financial liability to the customer at the amount paid in the 12 months preceding the date on which the claim arose. If pushed, they may agree to raise the cap to reflect all amounts paid by the customer over the duration of the contract. They will habitually exclude special, indirect and consequential losses.

Most providers also look to exclude their liability for loss or corruption of data. They argue that customers should make back-ups of all electronic documents signed through the platform. However, customers should resist this exclusion and argue that data loss or corruption caused by the provider amounts to a breach of contract.

It is rare that a provider agrees to indemnify customers against a breach of data

Related information

This article is at practicallaw.com/1-637-8528

Other links from uk.practicallaw.com/

Topics

E-commerce	topic2-103-1274
General Contract and Boilerplate	topic9-103-1119
Information Technology	topic5-103-2074
Internet	topic8-383-8686
Privacy	topic6-383-8687

Practice notes

Electronic contracts, deeds and signatures	7-598-7269
Contracts: authority	9-107-3963
E-signature legal framework	9-614-7685
Execution of deeds and documents	0-380-8400
Execution of documents: Companies Act 2006	0-202-4594

Previous articles

Privacy shield: protecting data transfers (2016)	1-636-0528
General Data Protection Regulation: a game-changer (2016)	2-632-5285
Data transfers in the cloud: the struggle for compliance (2014)	8-581-9685
Electronic signatures: are we getting there? (2012)	9-517-8343
Execution and delivery of deeds: are we all on the same page? (2011)	3-506-6490

For subscription enquiries to Practical Law web materials please call +44 207 202 1200

protection laws resulting in a regulatory fine or compensation payable to a data subject. The new General Data Protection Regulation (679/2016/EU) (GDPR) will raise the bar for regulatory fines from the current maximum of £500,000 under the Data Protection Act 1998 to the greater of 4% of the customer's annual worldwide turnover and €20 million (see feature article "General Data Protection Regulation: a game-changer", www.practicallaw.com/2-632-5285). This is a game-changer. Providers will continue to resist indemnifying customers for a breach of data protection laws unless the deal value justifies the risk; but there is a growing trend for providers to compromise by agreeing a separate liability cap of between two and five times the deal value.

DATA PROTECTION IN THE CLOUD

Reconciling cloud-based services with EU data protection laws is problematic, and the introduction of the GDPR in May 2018 will make this even more challenging (see feature article "Data transfers in the cloud: the struggle for compliance", www.practicallaw. com/8-581-9685).

The leading platform providers are still evaluating the implications of the GDPR for

their business. At the time of writing, none of those providers have updated their standard terms. However, changes will be necessary to reflect the fact that providers will have direct obligations as data processors under the GDPR, and will have to comply with more onerous requirements to notify data breaches.

Until the GDPR comes into force, the risk and burden of complying with the Data Protection Directive is borne entirely by the customer as the data controller. A customer may not contractually transfer its obligations or liability as a data controller to the platform provider, which is acting as a data processor. It is therefore imperative for the customer that the agreement with the provider contains appropriate provisions to satisfy:

- The data transfer restrictions exporting personal data to a destination outside the EEA under Chapter IV of the Data Protection Directive.
- The data processor security obligation under Article 17 of the Data Protection Directive.

Data transfer restriction

Many providers now offer European customers the option of storing their signed e-contracts

at European data centres. This has helped to allay concerns arising from the Snowden revelations about the extent to which US intelligence and law enforcement agencies gain access to EU citizens' personal data held by US cloud service providers. Customers have drawn further comfort from the recent ruling by the US Court of Appeals for the Second Circuit that a US search warrant issued on behalf of US law enforcement agencies did not have extraterritorial effect and did not permit the seizure of email content held by Microsoft on its servers in Ireland (Microsoft Corp v USA 2016 WL 3770056 (2d Cir Jul14, 2016)).

However, the underlying metadata created by an electronic signature platform (such as the signatories' names, email and IP addresses) and billing information is routinely stored outside the EEA. Technical support for the platform is invariably provided from low-cost jurisdictions outside the EEA which are not on the Commission's white list as providing an adequate level of protection for personal data.

In order to satisfy the restrictions under the Data Protection Directive on transferring personal data to a destination outside the EEA, customers should ensure that the provider either:

- Uses the EC-approved controllerprocessor model clauses (appended to Commission Decision 2010/87/EU) (the model clauses).
- Has adopted binding corporate rules approved by a national data protection authority.

Clause 10 of the model clauses states that the parties may not vary or modify the model clauses. This does not prevent them from adding clauses on business related issues where required as long as they do not contradict the clauses. Like most cloud service providers, platform providers interpret this very liberally and water down their obligations under the model clauses: they are not amenable to audits of their data centres (see below) and it is not practical to obtain a customer's consent to the appointment of new sub-processors after the parties have agreed terms to use a shared platform. There is a

tension between cloud services and EU data protection laws. Practitioners should adopt a pragmatic, risk-based approach. The data transfer arrangements will be acceptable to most customers, but customers regulated by the FCA should proceed more cautiously and heed the FCA's guidance for outsourcing to the cloud (www.fca.org.uk/publications/finalisedauidance/fa16-5-auidance-firms-outsourcina-%E2%80%98cloud%E2%80%99-and-otherthird-party-it).

In July 2016, the Commission approved the Privacy Shield framework which supersedes the safe harbor regime for transatlantic data flows. But customers should be circumspect. Privacy advocacy groups have already sought to challenge the Commission's adequacy decision in the General Court of the EU, and the Privacy Shield is unlikely to fully satisfy the data transfer restriction where an electronic signature platform is deployed globally (see feature article "Privacy shield: protecting data transfers", www.practicallaw. com/1-636-0528).

Data security obligation

Customers should undertake thorough due diligence on the provider's information security and risk management practices. Article 17 of the Data Protection Directive requires the customer, as the data controller, to enter into a written contract with the provider, as data processor, obliging the provider to implement any requisite technical and organisational security measures when processing the customer's personal data. The customer is also expected to take reasonable steps to ensure compliance with these security measures.

The leading providers will readily supply a copy of their certification to the ISO/IEC 27001 standard for information security management systems. US providers may also volunteer their Service Organization Control (SOC) 2 annual audit report. A SOC 2 report focuses on the provider's organisation controls in relation to security, availability, processing integrity, confidentiality and

More generally, providers should provide details of how they keep customer data secure and confidential, both when in transit and at rest in the data centres. These measures would include, for example, encryption standards, physical security controls and notification of data security breaches. Providers are reluctant to give customers and their regulators a right to audit data centres; it is disruptive and risks jeopardising the confidentiality and security of other customers that are sharing the platform. But audit rights can be a deal-breaker for some customers, particularly in the banking and insurance sector, and providers will grudgingly acquiesce to audit rights if the deal is big enough.

BREXIT

The UK has yet to activate the withdrawal process under Article 50 of the Treaty on European Union but in her keynote speech on 17 January 2017, the Prime Minister signalled that the UK will leave the EU single market and customs union. It is not possible to predict the course of the exit negotiations or the nature of the future trading relationship with the EU. At the time of writing, it seems likely that the Regulation would cease to have effect in the UK when it withdraws from the EU or the UK's treaty obligations cease under Article 50.

If the UK were no longer subject to the Regulation, this would not have an adverse impact on the law and market practice for electronic signatures. Under English law, any form of electronic signature (and related certificate) would still be admissible in evidence to determine the authenticity or integrity of an electronic document. Irrespective of the Regulation, the key question for an English or Scottish court is whether the electronic signature demonstrates an authenticating intention; in other words, did the signatory intend to be bound by the terms of the document they have signed?

A farewell to the Regulation would also mean an end of mutual recognition for QES in UK courts. But this is largely academic. In the absence of fraud, a UK court would continue to admit and give legal effect to contracts signed by a QES.

Richard Oliphant is a partner in the K6 Partners, helping businesses with digital transformation. He is the former EMEA General Counsel of DocuSign, Inc.