



# Brexit briefing

What is the impact on electronic signature laws in the UK?

2021

# Contents

- 3**    [Brexit briefing: what is the impact on electronic signature laws in the UK?](#)
- 4**    [Executive summary](#)
- 5**    [The UK legal framework \(before 1 January 2021\)](#)
- 7**    [How does eIDAS apply to the UK from 1 January 2021?](#)
- 8**    [Repeal of the electronic identification provisions of eIDAS](#)
- 9**    [Mutual recognition of electronic signatures and other trust services in the UK and EU from 1 January 2021](#)
- 10**   [Are electronic signatures still valid and admissible in evidence from 1 January 2021?](#)
- 11**   [What does the EU-UK Trade and Cooperation Agreement 2020 say about electronic signatures?](#)

# Brexit briefing: what is the impact on electronic signature laws in the UK?

Consumers and businesses in the UK routinely use EU-based e-signing platforms to sign electronic documents. Platforms have grown in importance as social distancing restrictions to combat COVID-19 have made face-to-face signing largely impracticable.

In the UK, electronic signatures have been regulated by both EU and UK laws. In this briefing note, leading European law firm, CMS, has partnered with Adobe to examine how the UK's departure from the EU (**Brexit**)<sup>1</sup> affects the legal standing of electronic signatures under UK law from 1 January 2021.



<sup>1</sup> The UK technically left the EU at 11:00pm (UK time) on 31 January 2020 pursuant to the [EU-UK Withdrawal Agreement 2019](#). However, the parties agreed a 'transition period' which ended at 11:00pm on 31 December 2020. During the transition period, the UK was treated for most purposes as if it were still a member of the EU and most EU law continued to apply to the UK. This briefing note concerns UK law after the transition period.





# Executive summary

- In 2016, [Regulation \(EU\) No 910/2014 \(eIDAS\)](#) created a Europe-wide legal framework for electronic signatures. Section 3 of the [European Union \(Withdrawal\) Act 2018](#) converted eIDAS into UK law (**UK eIDAS**). Those provisions of UK eIDAS which the UK government has deemed '*inappropriate or redundant*' following Brexit have been amended by a [Brexit statutory instrument \(eIDAS SI\)](#).
- The electronic identification (**e-ID**) provisions in eIDAS are repealed by the eIDAS SI and not incorporated into UK eIDAS. This means that the UK's national e-ID scheme, [GOV.UK Verify](#), is no longer able to participate in the EU's interoperability framework for national e-ID schemes. e-ID is integral to the EU Commission's [Digital Single Market](#) strategy and to removing barriers to cross-border trade-commerce. The UK government has signalled its intention to develop a new national 'digital ID' scheme. It is important that the UK's digital ID scheme is interoperable with eIDAS (and other international digital ID systems) if the UK's digital economy is to stay competitive.
- UK eIDAS preserves the mutual recognition of electronic signatures and other trust services. This is achieved by allowing the technical standards and specifications in UK eIDAS to mirror those in eIDAS. This is welcome news. It means that e-signing platforms (and trust service providers) established in the EU can continue to provide their trust services to UK customers.
- A 'qualified electronic signature' (**QES**) has the equivalent legal standing of a handwritten signature and is the gold standard of electronic signatures in EU law (see *Article 25, eIDAS*). It provides more security and a higher level of authentication than a standard electronic signature. The elevated status of the QES is maintained by UK eIDAS. As cloud and mobile signing technology advances, the use of QES in cross-border transactions between UK and EU parties is set to increase.
- The combination of UK eIDAS, the [Electronic Communications Act 2000](#) and case law supports the continued use of electronic signatures to execute **domestic transactions** (under English law). This is dependent on (i) the signatory demonstrating their intention to authenticate the transaction (which is evidenced by the workflow and digital audit trail generated by Adobe Sign) and (ii) satisfying any legal formalities for executing the transaction (for example, witness attestation of the signature). There are of course exceptions, such as wills and lasting powers of attorney, which cannot be executed using an electronic signature. *For a more comprehensive list of transactions or use cases that cannot be executed electronically, or for which UK law prescribes a particular form of electronic signature such as a QES, please refer to the [CMS guide to electronic signatures and e-signing platforms](#).*
- eIDAS did not fully harmonise electronic signature laws in the EU. It left some discretion to EU member states to prohibit electronic signatures or to require a particular type of electronic signature such as a QES. For **cross-border transactions**, a UK party must always consider on a case-by-case basis whether an electronic signature will be recognised, and the document be registrable and enforceable, in every jurisdiction relevant to the transaction.
- The [UK-EU Trade and Cooperation Agreement 2020 \(TCA\)](#) contains provisions to promote digital trade and '*ensure an open, secure and trustworthy online environment for businesses and consumers*.' The TCA includes a guarantee that neither the UK nor the EU may discriminate against electronic signatures and electronic documents **solely** on the grounds that they are in an electronic form. Somewhat surprisingly, the TCA has adopted a new definition of electronic signature that diverges from the common definition in eIDAS and UK eIDAS. The TCA's definition introduces a strict requirement for 'data integrity'. Adobe confirms that all electronic (and digital) signatures available for use on the Adobe Sign platform satisfy this requirement. This is significant. Although the TCA excludes certain categories of contract (including real estate contracts, wills and notarial documents), the TCA broadly aligns the future development of UK and EU laws in relation to the type of electronic and digital signatures available on the Adobe Sign platform (and, one assumes, other reputable e-signing platforms). This is reassuring to UK customers, especially for cross-border transactions with EU parties.



# The UK legal framework

(before 1 January 2021)

To understand the repercussions of Brexit for electronic signatures, we must first consider how domestic and EU legislation combined with case law to govern the admissibility and validity of electronic signatures in the UK prior to 1 January 2021.

## eIDAS

[Regulation \(EU\) No 910/2014 \(eIDAS\)](#) took direct effect in EU member states in July 2016. It established an EU-wide legal framework for electronic signatures (and other 'trust services', such as electronic seals and time stamps, which are outside the scope of this note).

eIDAS defines:

1. An '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'.<sup>2</sup>
2. An 'advanced electronic signature'<sup>3</sup> (**AdES**) as an electronic signature which meets the following requirements:
  - it is uniquely linked to the signatory;
  - it is capable of identifying the signatory;
  - it is created using electronic signature-creation data<sup>4</sup> that the signatory can, with a high level of confidence, use under his sole control; and
  - it is linked to the signed data in such a way that any subsequent change in the data is detectable.
3. A 'qualified electronic signature' (**QES**) as an 'advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures'.<sup>5</sup>

Article 25(1) of eIDAS states that an electronic signature is admissible in evidence in legal proceedings and shall not be denied legal effect on the grounds that it is in an electronic form. Articles 25(2) and (3) of eIDAS further provide that only a QES has the equivalent legal standing of a handwritten signature and is mutually recognised in every EU member state. The QES is presumed to be authentic and is therefore the gold standard for electronic signatures.

<sup>2</sup> Article 3(10) eIDAS.

<sup>3</sup> Article 26 eIDAS.

<sup>4</sup> Electronic-signature creation data refers to the encryption key used by the signatory to create the electronic signature. An AdES is usually created using 'Public Key Infrastructure' or 'PKI' encryption technology. PKI is a system in which a signatory's public key is the subject of a digitally-signed certificate by a trust service provider (or certification authority). The electronic document is signed with the private key and may be decrypted by the corresponding public key. The certificate identifies the owner of the public key and provides assurance that the signatory is who they claim to be.

<sup>5</sup> Article 3(12) eIDAS. A qualified electronic signature creation device may be a physical device such as a smartcard or USB stick; or, in the context of remote or cloud signing services, the device is a 'hardware security module' operated by a 'qualified trust service provider'.



Like many e-signing platforms, Adobe works with a wide array of ‘qualified trust service providers’ (**QTSPs**)<sup>6</sup> such as [Digidentity B.V.](#) and [Intesi Group S.p.A.](#) QTSPs provide customers with cloud-based digital certificates for signing documents on the platform with a QES. They are subject to a comprehensive regulatory regime under eIDAS which is designed to ensure that they meet strict security standards. This includes submitting a conformity assessment report to a supervisory body in an EU member state and demonstrating that the QTSP complies with the requirements under eIDAS (*Articles 20 and 24, eIDAS*). The regulatory regime enhances trust in QES and the digital certificates that underpin them.

Notwithstanding Article 25, it is important to recognise that eIDAS has fallen short of fully harmonising electronic signature laws across the EU. Recital 49 of eIDAS is key. It states that – save in the case of QES – it is still national law that defines the legal effect of electronic signatures. This means that an EU member state may prohibit the use of an electronic signature for certain transactions (for example, wills<sup>7</sup>) **or** prescribe the use of a higher form of signature (such as a QES) to approve that transaction. Furthermore, public registries are still at liberty to require a handwritten (or wet ink) signature for registration purposes.

#### **b. ECA 2000**

The [Electronic Communications Act 2000](#) (**ECA 2000**) lays out a statutory framework for the admissibility of electronic signatures in UK law. Section 7(1) of the ECA 2000 says that an electronic signature (and any certification) is admissible in legal proceedings in relation to any question concerning the ‘authenticity’<sup>8</sup> or ‘integrity’<sup>9</sup> of an electronic document.

Although the ECA 2000 deals with the admissibility of electronic signatures, it does not expressly provide for their legal validity in UK law. This is primarily determined by principles of common law.<sup>10</sup>

#### **c. Case law**

The leading cases<sup>11</sup> (and the Law Commission in its [2019 report on electronic execution](#)) have confirmed that a majority of consumer and commercial transactions may be validly executed with an electronic signature in UK law<sup>12</sup> *provided that* the signatory intends to authenticate the document and any execution formalities (such as witnessing) are satisfied.

*For a more comprehensive list of transactions or use cases that cannot be executed electronically, or for which UK law (notably, Scots law) prescribes a particular form of electronic signature such as a QES, please refer to the [CMS guide to electronic signatures and e-signing platforms](#).*

6 A trust service provider which appears in an EU member state’s trusted list and has been certified by a supervisory body to provide qualified certificates and/or other qualified trust services (Article 3(20) eIDAS).

7 In the UK and in many other EU jurisdictions, electronic execution of wills is not permitted.

8 Authenticity is defined in section 15(2)(b) of the ECA 2000 as a reference to (i) whether the communication or data comes from a particular person or other source; (ii) whether it is accurately timed and dated; or (iii) whether it is intended to have legal effect.

9 Integrity is defined in section 15(2)(b) of the ECA 2000 as a reference to whether there has been any tampering with or other modification of the communication or data.

10 Note, however, that in Scotland, the Requirements of Writing (Scotland) Act 1995 and the Electronic Documents (Scotland) Regulations 2014 have established a separate statutory regime governing electronic signatures which is outside the scope of this note. Please refer to the [CMS guide to electronic signatures and e-signing platforms](#) for further information.

11 *J Pereira Fernandes SA v Mehta* [2006] EWHC 813 (Ch), [2006] 1 WLR 1543; *WS Tankship II BV v Kwangju Bank Ltd* [2011] EWHC 3103 (Comm); *Golden Ocean Group Ltd v Sagoacar Mining Industries PVT Ltd* [2012] EWCA Civ 265, [2012] 1 WLR 3674; *Bassano v Toft* [2014] EWHC 377 (QB); *Re Stealth Construction Ltd*; *Green (Liquidator of Stealth Construction Ltd) v Ireland* [2011] EWHC 1305 (Ch); *Lindsay v O’Loughnane* [2010] EWHC 529 (QB); and *Orton v Collins* [2007] EWHC 803 (Ch), [2007] 1 WLR 2953.

12 Again, practitioners should note that Scots law differs from English law and prescribes that certain categories of transaction may only be executed electronically using an AdES (for legal validity) or a QES (for self-proving status). The relevant provisions are set out in the Requirements of Writing (Scotland) Act 1995 and The Electronic Documents (Scotland) Regulations 2014.



# How does eIDAS apply to the UK from 1 January 2021?

The UK left the EU on 31 January 2020 (**exit day**). Under the terms of the [EU-UK Withdrawal Agreement 2019](#), the EU and the UK agreed a transitional arrangement from exit day which ended at 11:00 pm (UK time) on 31 December 2020 (**transition period**).

During the transition period, the UK continued to be treated for most purposes as if it were still an EU member state. It participated in the EU customs union and single market, and the four freedoms (goods, services, persons and capital) also remained in place.

EU law in its entirety – including eIDAS – continued to apply to the UK during the transition period.

But at the end of the transition period, the UK became a ‘third country’ and a new body of ‘retained EU law’ was created under sections 2 to 4 of the [European Union \(Withdrawal Act\) 2018 \(EUWA\)](#). The EUWA:

- retained domestic legislation deriving from the implementation of EU Directives; and
- saved and converted into UK law every EU Regulation including eIDAS.

What this means is that, from 1 January 2021, eIDAS was incorporated into UK domestic law (**UK eIDAS**). However, the UK Parliament approved a [statutory instrument](#) to modify those provisions of UK eIDAS that were deemed ‘inappropriate or redundant’, with effect from 1 January 2021 (**eIDAS SI**).<sup>13</sup> The key modifications introduced by the eIDAS SI are explained in sections 3 and 4 below.



<sup>13</sup> The Electronic Identification and Trust Services for Electronic Transactions (Amendment etc.) (EU Exit) Regulations 2019.

# Repeal of the electronic identification provisions of eIDAS

From 1 January 2021, the electronic identification (**e-ID**) provisions of eIDAS were repealed and the UK lost access to the interoperability framework for e-ID. This scheme was intended to enable EU citizens to use their national e-ID to access public sector digital services in other EU member states. On 2 May 2019, GOV.UK Verify had been [notified](#) by the UK as the national e-ID scheme pursuant to Article 9 of eIDAS.

On 26 May 2020, the European Commission issued a [notice](#) that GOV.UK Verify would no longer be recognised by EU member states as the UK's national e-ID scheme from the end of the transition period. This aligned with the eIDAS SI, which provided that the e-ID sections of eIDAS would not be part of retained EU law (UK eIDAS). It is tempting to dismiss this as inconsequential. But e-ID is highly valued by the European Commission as a key driver of its flagship digital single market strategy. At the time of writing (February 2021), 19 EU member states have completed the notification process that paves the way for citizens to use their national e-IDs for cross-border access to online public sector services. The use of national e-IDs will extend to the private sector and one can understand why they are so central to the digital single market strategy.

To compensate for the UK's exclusion from the interoperability framework for national e-IDs, the government has appointed a Digital Identity Strategy Board. The Board will be tasked with updating current laws and developing new consumer protection legislation to support the use of digital identities in the UK.

To maintain the competitiveness of the UK's digital economy, it is important that the digital identity scheme is interoperable with national e-ID schemes notified by EU member states under Article 9 of eIDAS (and with other international digital ID schemes). The omens are positive. In a new [policy paper](#) on the '*UK digital identity and attributes trust framework*' published on 11 February 2021, the Minister for Digital Infrastructure, Matt Warman, commented:

*'We will continue to work with our international partners to make sure our standards are interoperable with those adopted abroad, so in the future you can use your digital identity around the world and UK businesses can trust digital identities created elsewhere.'*



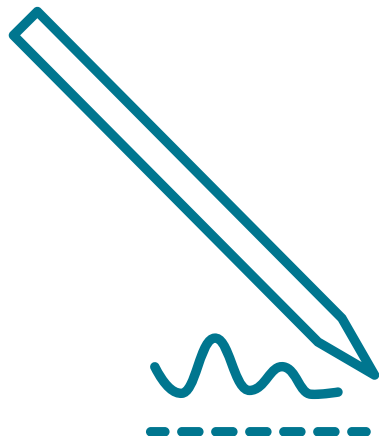
# Mutual recognition of electronic signatures and other trust services in the UK and EU from 1 January 2021

The eIDAS SI has preserved the mutual recognition and interoperability of electronic signatures and other trust services. It does this by allowing the technical standards and specifications in UK eIDAS to mirror those in eIDAS. Thus, if a QES is issued by a QTSP in any EU member state, it will still be recognised as a QES in the UK.

This is welcome news for platforms (and their networks of QTSPs) that are established in EU member states (in the case of Adobe , in the Republic of Ireland) who provide trust services to UK businesses and public sector bodies. **The eIDAS SI ensures that all EU trust services may continue to be used in the UK beyond the transition period.**

By contrast, the European Commission's notice of 26 May 2020 made clear that one consequence of Brexit is that a QES (and other qualified trust services) provided by a QTSP established in the UK will **no longer be recognised in the EU**. There are currently no UK-based QTSPs on the [UK Trusted List](#) (administered by tScheme), and this restriction on EU market access is unproblematic at the present time; but it is clearly a disincentive for trust service providers to acquire qualified status in the UK if their qualified trust services are not recognised in the EU.

Future recognition of qualified trust services from UK QTSPs will be dependent on the EU and the UK concluding an 'international agreement' in accordance with Article 14 of eIDAS.



# Are electronic signatures still valid and admissible in evidence from 1 January 2021?

Brexit will not have any **material impact** on the legal validity and admissibility of electronic signatures under UK law. The ECA 2000 remains unchanged and the provisions on electronic signatures in eIDAS (as amended in the UK by the eIDAS SI) have been retained in UK eIDAS, including Article 25 relating to QES.

Furthermore, the English common law has always adopted a pragmatic approach to electronic signatures. As we noted in section 1 above, subject to a small number of exceptions<sup>14</sup>, an electronic signature is capable in UK law of being used to execute a document (including a deed) provided that:

- the signatory demonstrates an intention to authenticate (or approve) the document; and
- any formalities<sup>15</sup> relating to execution of that document are satisfied (for example, executing it as a deed).

In view of the above, Brexit should have no adverse effect on UK consumers and businesses continuing to use e-signing platforms for **domestic transactions**.

For **cross-border transactions** with overseas parties, a UK party must always evaluate on a case-by-case basis whether an electronic signature will be recognised, and the document will be registrable and enforceable, in every jurisdiction relevant to the transaction. Brexit has not changed this fundamental requirement. Practitioners should also be aware that in certain EU jurisdictions there may be a legal requirement or a cultural preference for using digital signatures such as AdES and QES.

*For more information about electronic signature laws overseas, please refer to Adobe Sign's multi-jurisdictional [legality guides](#). CMS has also published a [guide to electronic signature laws in overseas commercial contracts](#).*

<sup>14</sup> There are certain transactions under English law where electronic execution is not permitted (for example, wills and lasting powers of attorney). There are certain transactions under Scots law which will only be 'self-proving' if they are executed with a QES.

<sup>15</sup> A procedure which a party must follow to give legal effect to a transaction. Formalities include requirements that certain transactions are made 'in writing' or 'signed' or made by deed.



# What does the EU-UK Trade and Cooperation Agreement 2020 say about electronic signatures?

The [EU-UK Trade and Cooperation Agreement 2020 \(TCA\)](#) came into force on 1 January 2021. The TCA governs the new trade relationship and includes provisions aimed at promoting digital trade between the parties. Article DIGIT.1, Chapter 1 of Title III (Digital Trade) commits the UK and the EU to *'ensure an open, secure and trustworthy online environment for businesses and consumers.'*

The TCA includes a guarantee that neither the UK nor the EU will discriminate against electronic signatures or electronic documents solely on the basis that they are in an electronic form (**non-discrimination principle**) (see *Title III, Chapter 3, Articles DIGIT.10 and 11*). This is consistent with the non-discrimination provisions in Articles 25(1) and 46 of eIDAS (see section 1 above).

However, whilst the TCA upholds the 'non-discrimination principle'<sup>16</sup> it is more explicit than recital 49 of eIDAS in setting out exceptions to the non-discrimination principle.

Article DIGIT.10(2), Chapter 3 of Title III (*Conclusion of contracts by electronic means*) lists [several categories of contract](#) which are exempt from the non-discrimination principle. These include the services of lawyers and notaries, real estate contracts, family law contracts and contracts requiring in-person witnesses.

Article DIGIT.11(3), Chapter 3 of Title III (Electronic authentication and electronic trust services) allows the UK or EU to require that:

*'for a particular category of transactions, the method of electronic authentication or trust service is certified by an authority accredited in accordance with its law or meets certain performance standards which shall be objective, transparent and non-discriminatory and only relate to the specific characteristics of the category of transactions concerned.'*



The [EU-UK Trade and Cooperation Agreement 2020 \(TCA\)](#) came into force on 1 January 2021. The TCA governs the new trade relationship and includes provisions aimed at promoting digital trade between the parties. Article DIGIT.1, Chapter 1 of Title III (Digital Trade) commits the UK and the EU to *'ensure an open, secure and trustworthy online environment for businesses and consumers.'*

The TCA includes a guarantee that neither the UK nor the EU will discriminate against electronic signatures or electronic documents solely on the basis that they are in an electronic form (**non-discrimination principle**) (see *Title III, Chapter 3, Articles DIGIT.10 and 11*). This is consistent with the non-discrimination provisions in Articles 25(1) and 46 of eIDAS (see section 1 above).

However, whilst the TCA upholds the 'non-discrimination principle'<sup>16</sup> it is more explicit than recital 49 of eIDAS in setting out exceptions to the non-discrimination principle.

Article DIGIT.10(2), Chapter 3 of Title III (*Conclusion of contracts by electronic means*) lists [several categories of contract](#) which are exempt from the non-discrimination principle. These include the services of lawyers and notaries, real estate contracts, family law contracts and contracts requiring in-person witnesses.

Article DIGIT.11(3), Chapter 3 of Title III (Electronic authentication and electronic trust services) allows the UK or EU to require that:

*'for a particular category of transactions, the method of electronic authentication or trust service is certified by an authority accredited in accordance with its law or meets certain performance standards which shall be objective, transparent and non-discriminatory and only relate to the specific characteristics of the category of transactions concerned.'*

We interpret this to mean that UK or EU law **may** prescribe the use of an AdES or a QES where it is felt that a higher degree of security or identity assurance is required for particular transactions. The Article also envisages the possibility of supervisory bodies such as the ICO<sup>17</sup> in the UK establishing technical standards for electronic signatures and other trust services.

One oddity of the TCA is the introduction of a new definition of 'electronic signature':

*"electronic signature" means 'data in electronic form which is attached to or logically associated with other data in electronic form that: (i) is used by a natural person to agree on the data in electronic form to which it relates; and (ii) is linked to the data in electronic form to which it relates in such a way that any subsequent alteration in the data is detectable.'* (Title III, Chapter 1, Article DIGIT.5(f))

This definition diverges from the definition used in both Article 3(10) of eIDAS and section 7 of the ECA 2000, and it is somewhat puzzling. The requirement in the TCA that the electronic signature be *'linked to the data in electronic form to which it relates in such a way that any subsequent alteration in the data is detectable'* effectively narrows the definition to electronic signatures that guarantee data integrity.

Data integrity is *not guaranteed* by a basic form of electronic signature such as the typing of the signatory's name at the foot of an email. But data integrity is a characteristic of electronic signatures generated by those e-signing platforms like Adobe Sign which are certified with a tamper-evident seal. An AdES and QES – which rely on the use of Public Key Infrastructure<sup>18</sup> technologies – afford an even greater level of data integrity because cryptographic signatures protect the integrity directly. In fact, the new definition of electronic signature in the TCA mirrors the language used in Article 25 to define the properties of an AdES.

<sup>16</sup> The non-discrimination principle means that neither an electronic document nor an electronic signature should be denied legal effect or admissibility in evidence in legal proceedings solely on the basis they are in an electronic form.

<sup>17</sup> Information Commissioner's Office - <https://ico.org.uk/>

<sup>18</sup> See definition of PKI in footnote 4.

### So, what are we to make of the discrepancy between the definition of electronic signature under eIDAS and the ECA 2000, and under the TCA?

How will it shape or influence the future evolution of electronic signature laws in both the UK and EU? Let us try to draw some conclusions:

- If the TCA had said nothing about signatures, both the EU and UK would be free to diverge in the future in respect of all kinds of signature, electronic or otherwise. They could be as liberal or as restrictive in their laws as they liked. That is the default position.
- But for a subset of electronic signatures (i.e. those which guarantee data integrity) the TCA has restricted the possibility of future divergence. This will cover an electronic signature, AdES and QES used to sign documents (including deeds) on the Adobe Sign and, potentially, e-signing platforms.
- For electronic signatures outside the defined subset (i.e. those which do not guarantee data integrity, such as typing a name in an email), the UK and EU are free to be as liberal or restrictive in their laws as they like, because they fall outside the scope of the TCA.
- The TCA's emphasis on data integrity sets the direction for electronic signature laws in the UK and EU. In response, we anticipate rising demand from customers for AdES and QES which, coupled with data integrity, offer a higher level of authenticity than an electronic signature.

**Richard Oliphant** is a consultant to CMS and Adobe. He specialises in electronic and digital signature law and practice.

### For further information please contact:



**Ian Stevens**

Partner

T +44 20 7367 2597

E [ian.stevens@cms-cmno.com](mailto:ian.stevens@cms-cmno.com)



**John Jolliffe**

Senior Manager, Strategic Development, Document Cloud

T +32 2 416 40 91

E [jjolliff@adobe.com](mailto:jjolliff@adobe.com)



**Richard Oliphant**

Consultant

T +44 20 7367 3566

E [richard.oliphant@cms-cmno.com](mailto:richard.oliphant@cms-cmno.com)

### About CMS

With more than 70 offices in over 40 countries and 4,800+ lawyers worldwide, CMS is a law firm that offers deep local market understanding with a global perspective. We are focused on building strong relationships with our clients, our people, our industry sectors and wider communities. As a Future Facing firm we take a bold, dynamic and agile approach to help clients of every size face the future with confidence. We have an immense depth of understanding of the sectors in which we operate. Our lawyers are genuine experts in their fields and are able to advise on current challenges as well as anticipate those on the horizon that are likely to shape the future.

### About Adobe

Adobe is the global leader in digital experience and digital media solutions. Our tools and services allow our customers to create groundbreaking digital content, deploy it across media and devices, measure and optimize it over time and achieve greater business success. We help our customers make, manage, measure and monetize their content across every channel and screen.



**Your free online legal information service.**

A subscription service for legal articles  
on a variety of topics delivered by email.

**[cms-lawnow.com](http://cms-lawnow.com)**

.....  
CMS Cameron McKenna Nabarro Olswang LLP  
Cannon Place  
78 Cannon Street  
London EC4N 6AF

T +44 (0)20 7367 3000  
F +44 (0)20 7367 2000

The information held in this publication is for general purposes and guidance only and does not purport to constitute legal or professional advice.

CMS Cameron McKenna Nabarro Olswang LLP is a limited liability partnership registered in England and Wales with registration number OC310335. It is a body corporate which uses the word "partner" to refer to a member, or an employee or consultant with equivalent standing and qualifications. It is authorised and regulated by the Solicitors Regulation Authority of England and Wales with SRA number 423370 and by the Law Society of Scotland with registered number 47313. It is able to provide international legal services to clients utilising, where appropriate, the services of its associated international offices. The associated international offices of CMS Cameron McKenna Nabarro Olswang LLP are separate and distinct from it. A list of members and their professional qualifications is open to inspection at the registered office, Cannon Place, 78 Cannon Street, London EC4N 6AF. Members are either solicitors or registered foreign lawyers. VAT registration number: 974 899 925. Further information about the firm can be found at [cms.law](http://cms.law)

© CMS Cameron McKenna Nabarro Olswang LLP

CMS Cameron McKenna Nabarro Olswang LLP is a member of CMS Legal Services EEIG (CMS EEIG), a European Economic Interest Grouping that coordinates an organisation of independent law firms. CMS EEIG provides no client services. Such services are solely provided by CMS EEIG's member firms in their respective jurisdictions. CMS EEIG and each of its member firms are separate and legally distinct entities, and no such entity has any authority to bind any other. CMS EEIG and each member firm are liable only for their own acts or omissions and not those of each other. The brand name "CMS" and the term "firm" are used to refer to some or all of the member firms or their offices. Further information can be found at [cms.law](http://cms.law)