Flynn O'Driscoll Legal Update

Updated EU Law on Electronic Signatures

Introduction

The Digital Single Market strategy of the European Union has taken another step forward in recent months with Regulation 910/2014 (the "eIDAS Regulation") coming into effect on the 1st July 2016. The eIDAS Regulation seeks to update the current EU law in the area, repealing the eSignatures Directive, dating back to 1999.

The eSignatures Directive failed to develop the market for electronic signatures for a number of reasons, such as variance in how Member States implemented the directive which led to differing definitions for electronic signatures and uncertainty as to their legal validity in certain contexts. The eIDAS Regulation immediately addresses this problem by ensuring uniformity of application throughout the European Union. It also introduces a variety of new measures in order to keep pace with developing technologies. For example, electronic signatures can now be provided on mobile devices, as well as on traditional desktop computers.

The eIDAS Regulation sets out three types of electronic signatures that may be used.

Electronic signatures

These are data in electronic form which are attached to or logically associated with other electronic data and are used for signing. These can be as simple as typing your name into a text box in a computer or system, or your signature block in your email.

Advanced electronic signatures

These allow unique identification of the person who signs the document. They act as a tamper-evident seal which can reveal any unauthorised changes to its content. They are designed using signature creation data, that the signatory can, with a high level of confidence, use under his sole control. The requirements of an advanced electronics signature are:-

i. it is uniquely linked to the signatory
ii. it is capable of identifying the signatory
iii. it is created using electronic signature-creation data that the signatory can,

with a high level of confidence, use under his sole control, and

iv. it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.

Currently there are three related technologies that meet the criteria for qualified electronic signatures. These are:-

- XAdES – this is set extensions for XML Digital Signatures, ensuring compliance with the requirements of the eIDAS Regulation.
- CAdES – enhancing the IETF's (Internet Engineering Task Force) Cryptographic Message Syntax, these extensions meet the requirements of the eIDAS Regulation.
- PAdES – similar to XAdES and CAdES, this sets out a set of profiles to the PDF standard. This sets out the requirements that PDF software must following in order to ensure that signautues in PDF signatures comply with the eIDAS Regulation requirements of advanced electronic signatures. Unlike XAdES and CAdES, PAdES is more often used in applications that involve human-readable documents.

Qualified electronic signatures

These are similar to advanced electronic signatures, however they include additional security requirements. Qualified electronic signatures are based on "Qualified Certificates", which can only be issued by a "Certificate Authority". A Certificate duly accredited and supervised by EU member state designated authorities, tasked with ensuring that the requirements of eIDAS are met. Qualified Certificates must be stored on a qualified signature creation device (such as a USB token, a cloud-based trust service, etc.). This is the only type of signature which has the equivalent legal effect of a handwritten 'wet ink' signature, and ensures mutual recognition across the EU.

Qualified electronic signatures provide a higher level of security (e.g., the signing process creates a tamper-evident seal), and combined with its mutual recognition across the EU, gives rise to a variety of different applications. For example, it could be particularly beneficial in the Health and FinTech industries; it provides a secure method of obtaining the consent of mobile app users for processing their sensitive personal data.

Electronic time stamps

The eIDAS Regulation also provides for the legal recognition of electronic time stamps. These are defined as data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time. Similar to electronic signatures, these shall not be denied legal effect and admissibility as evidence in legal proceedings, solely on the grounds that they are in an electronic form.

Provision is also made for a qualified electronic time stamp, which will automatically enjoy a presumption that the date and time indicated in the time stamp is accurate. A time stamp shall be designated as qualified where:-

i. it binds the date and time to data in such a manner as to reasonably preclude the possibility of the data being changed undetectably;

ii. it is based on an accurate time source linked to Coordinated Universal Time; and
iii. it is signed using an advanced electronic signature or sealed with an advanced electronic seal of the qualified trust service provider, or by some equivalent method.

Such validated time stamps will have a variety of uses and will evidence the time and date on which a transaction took place.

Electronic seals

The eIDAS Regulation also includes provision for the recognition of electronic seals. An electronic seals shall not be denied legal effect and admissibility in court proceedings solely on the grounds that it is in electronic form. There are three different types of electronic seal recognised under the eIDAS Regulation, similar to electronic signatures (an electronic seal, an advanced electronic seal and a qualified electronic seal).

'Mutual recognition'

The eIDAS Regulation introduces mutual recognition of electronic identification ("eID") and electronic trust services (including e-signatures, electronic seals, electronic time stamps and website authentication). Member States are required to recognise and accept any means of eIDs issued in another Member State which has been notified to the Commission. The notification of schemes to the Commission is voluntary, however, once notified, the recognition of notified schemes is mandatory.

Mutual recognition will apply if the notifying Member State's eID scheme meets the European Commission's conditions of notification. eIDs which have been notified will be published in the Official Journal of the European Union.

Trust Service Providers and Supervision

Under the eIDAS Regulation, Member States are to designate a supervisory body to regulate qualified trust service providers. These replace the "certification service providers" under the previous regime. Qualified trust service providers are required to take appropriate measures to manage the risks posed to the security of the trust services they provide. For example, if any breach of security is likely to adversely affect a person or company, the trust service provider must notify them without undue delay. Qualified trust service providers can either be qualified or non-qualified.

The eIDAS Regulation also introduces an EU 'Trust Mark' allowing users to differentiate themselves with other trust service providers. Where a trust service provider acquires qualified status, they may use the EU Trust Mark to indicate a higher standard of security. Qualified trust service providers are required to abide by stricter rules and are more closely monitored by the supervisory body.

The supervisory bodies shall be established to supervise both forms of trust service providers to ensure that they meet the requirements as set out in the eIDAS Regulation. Both trust service providers are required to take technical and organizational measures to manage the risks posed to the security of the trust services they provide, and notify the supervisory body in case of a security breach. Where the security breach is likely to affect a natural or legal person, the trust service provider is required to notify the affected party. The supervisory body shall report on a yearly basis the security

breaches to ENISA, the European Union Agency for Network and Information Security.

Conclusion

It is hoped that eIDAS will help to develop the digital economy and develop confidence in certain transactions that may primarily take place online.

Electronic signature providers have sought to rely on eIDAS to show the value in their services. The introduction of an even playing field across the EU should help develop further confidence in the use of electronic signing in business transactions.

Should you have any queries arising out of the foregoing please contact Barry Connolly who will be happy to assist.

Barry Connolly

Solicitor

E: *barryconnolly@fod.ie*
P: 01 6424253

Dublin:

1 Grants Row, Lower Mount Street,
Dublin 2, Ireland

Phone: +353 1 6424220
Fax: +353 1 6618918

Galway:

Unit 23, Galway Technology Centre,
Mervue Business Park, Galway, Ireland

Phone: +353 91 396540
Fax: +353 91 792649