Signaturit Solutions
by Signaturit Group

Departamento Legal

Validez legal del proceso de Firma Electrónica de Signaturit

Signaturit Group

Índice

01. Introducción y alcance.

El presente informe tiene como objetivo establecer cuál es la validez jurídica de los servicios de confianza proporcionados por Signaturit, en especial atención a los servicios de firma electrónica y la entrega electrónica certificada

Cabe señalar que el presente documento no tendría como objetivo determinar la valoración que posteriormente pudiera llevar a cabo un tribunal competente o cualquier autoridad con capacidad para ello.

02. Validez legal de la Firma Electrónica y de la Entrega electrónica certificada

02.1. Marco Legal

A nivel europeo, la validez y los efectos legales de la firma electrónica se encuentran regulados por el Reglamento (UE) Nº910/2014, de 23 de julio, regulador de la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior, derogando la anterior Directiva Nº1999/93/EC (Reglamento eIDAS).

En este sentido, hay que tener en cuenta que la mayor diferencia existente entre los Reglamentos y las Directivas en la UE es que, mientras que la Directiva debe ser traspuesta previamente al ordenamiento jurídico nacional de cada Estado Miembro para poder ser aplicada, el Reglamento es directamente aplicable a todos los Estados.

02.1.1. Reglamento (UE) 910/2014

El Reglamento eIDAS busca mejorar la confianza en las transacciones electrónicas dentro del mercado interior estableciendo una base común segura para la interacción electrónica entre ciudadanos, empresas y entidades públicas, aumentando, con ello, la efectividad de los servicios en línea públicos y privados, los negocios electrónicos y el comercio electrónico europeos. El Reglamento eIDAS, que es directamente aplicable en España y en toda la UE, establece los requisitos mínimos para considerar válida una firma electrónica o una entrega electrónica certificada, así como sus efectos legales.

FIRMA ELECTRÓNICA

El principal criterio a tener en cuenta es el que refleja el **Artículo 25**:

> *"No se denegarán efectos jurídicos ni admisibilidad como prueba en procedimientos judiciales a una firma electrónica por el mero hecho de ser una firma electrónica o porque no cumpla los requisitos de la firma electrónica cualificada*".

De acuerdo con lo establecido en el Reglamento eIDAS existen tres tipos de firmas electrónicas, cada una de ellas con un nivel de protección diferente:

a) **Firma electrónica simple**: es la forma más simple de firma electrónica. Como mero ejemplo, una firma electrónica simple puede ser una simple aceptación o un "checkbox".

b) **Firma electrónica avanzada**: se trata de una firma electrónica que requiere mayores requisitos que la firma electrónica simple, por lo que goza de un mayor grado de protección.

Dichos requisitos son:

- Es única y exclusiva para cada firmante;
- Es posible la identificación del firmante a través de los datos ofrecidos por ella;
- Se crea utilizando datos para la creación de firmas electrónicas, que el firmante puede utilizar, con un alto grado de confianza, bajo su propio control; y
- Está conectada, de tal manera, con los datos del documento firmado que cualquier cambio ulterior en el documento es detectable.

c) **Firma electrónica cualificada**: Es el tipo de firma electrónica que ofrece una mayor protección puesto que, para ser así considerada, debe cumplir los requisitos establecidos en el Anexo I del Reglamento (UE) 910/2014. A este tipo de firma electrónica se le han atribuido los mismos efectos legales que los otorgados para la firma manuscrita.

La principal diferencia entre la firma electrónica avanzada y la firma electrónica cualificada es, que esta última:

- Necesita ser creada a través de un dispositivo cualificado para la creación de firmas electrónicas, es decir, un dispositivo que garantice que la firma creada es segura y está protegida contra el fraude;
- Debe estar registrada en un sistema certificado de firmas electrónicas ofrecido por un proveedor fiable y certificado, concretamente un Prestador Cualificado de Servicios de Confianza.

ENTREGA ELECTRÓNICA CERTIFICADA

La entrega electrónica certificada es "un servicio que permite transmitir datos entre terceras partes por medios electrónicos y aporta pruebas relacionadas con la gestión de los datos transmitidos, incluida la prueba del envío y la recepción de los datos, y que protege los datos transmitidos frente a los riesgos de pérdida, robo, deterioro o alteración no autorizada" (definición del art. 3.36) eIDAS).

Este servicio se encuentra reconocido por el Reglamento (UE) 910/2014, otorgándole los siguientes efectos jurídicos, en base a lo dispuesto por su artículo 43:

> *"A los datos enviados y recibidos mediante un servicio de entrega electrónica certificada no se les denegarán efectos jurídicos ni admisibilidad como prueba en procedimientos judiciales por el mero hecho de que estén en formato electrónico o no cumplan los requisitos de servicio cualificado de entrega electrónica certificada."*

02.1.2. Ley de Servicios de Confianza, LSSI y LEC

La Ley 6/2020 de 11 de noviembre, tiene como objetivo determinar ciertos aspectos relativos a los Servicios de Confianza, como complemento de lo dispuesto por el Reglamento eIDAS.

Entre otras cuestiones, la Ley de Servicios de Confianza ha modificado el **Artículo 326.3 de la Ley de Enjuiciamiento Civil** (LEC) estableciendo lo siguiente:

> *"Cuando la parte a quien interese la eficacia de un documento electrónico lo solicite o se impugne su autenticidad, integridad, precisión de fecha y hora u otras características del documento electrónico que un servicio electrónico de confianza no cualificado de los previstos en el Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior, permita acreditar, se procederá con arreglo a lo establecido en el apartado 2 del presente artículo y en el Reglamento (UE) n.º 910/2014".*

Otra de las modificaciones que la Ley de Servicios de Confianza ha venido a traer es la carga probatoria de aquellos documentos electrónicos que hubiesen sido emitido en base a algún servicio de confianza cualificado. En concreto, la Disposición Final Segunda de la Ley de Servicios de Confianza modifica el **Artículo 326.4 de la LEC** otorgándole una presunción de validez a los servicios de confianza cualificados de la siguiente manera:

> "*Si se hubiera utilizado algún servicio de confianza cualificado de los previstos en el Reglamento citado en el apartado anterior, se presumirá que el documento reúne la característica cuestionada y que el servicio de confianza se ha prestado correctamente si figuraba, en el momento relevante a los efectos de la discrepancia, en la lista de confianza de prestadores y servicios cualificados*".

Por su parte, el **Artículo 299.2 de la LEC** estipula que:

> *"También se admitirán, conforme a lo dispuesto en esta Ley, los medios de reproducción de la palabra, el sonido y la imagen, así como los instrumentos que permiten archivar y conocer o reproducir palabras, datos, cifras y operaciones matemáticas llevadas a cabo con fines contables o de otra clase, relevantes para el proceso".*

Asimismo, la Ley 34/2002 de 11 de julio de servicios de la sociedad de la información y de comercio electrónico (LSSI) en su **Artículo 23** establece que:

> "*1. Los contratos celebrados por vía electrónica producirán todos los efectos previstos por el ordenamiento jurídico, **cuando concurran el consentimiento** y los demás requisitos necesarios para su validez.*
> *Los contratos electrónicos se regirán por lo dispuesto en este Título, por los Códigos Civil y de Comercio y por las restantes normas civiles o mercantiles sobre contratos, en especial, las normas de protección de los consumidores y usuarios y de ordenación de la actividad comercial.*
> *2. Para que sea válida la celebración de contratos por vía electrónica **no será necesario el previo acuerdo de las partes sobre la utilización de medios electrónicos**.*

3. ***Siempre que la Ley exija que el contrato o cualquier información relacionada con el mismo conste por escrito, este requisito se entenderá satisfecho si el contrato o la información se contiene en un soporte electrónico."***

Por lo tanto, serán válidos siempre y cuando las partes presten su consentimiento libre a la celebración de contratos con un fin y causa lícita.

Por último, es importante citar íntegramente el **Artículo 24 de la LSSI** sobre la 'Prueba de los contratos celebrados por vía electrónica', que estipula lo siguiente:

"1. La prueba de la celebración de un contrato por vía electrónica y la de las obligaciones que tienen su origen en él se sujetará a las reglas generales del ordenamiento jurídico.
Cuando los contratos celebrados por vía electrónica estén ***firmados electrónicamente*** *se estará a lo establecido en el artículo 3 de la Ley 59/2003, de 19 de diciembre, de firma electrónica*[1]*.*
2. En todo caso, el soporte electrónico en que conste un contrato celebrado por vía electrónica será admisible en juicio como prueba documental."

02.1.3. Código Civil

Como se ha estipulado en el inciso anterior, las partes pueden usar cualquier forma de firma electrónica para celebrar contratos y documentos de cualquier tipo, siempre y cuando no exista un requisito legal o una formalidad que estipule lo contrario.

Los artículos 1258 y 1262 del Código Civil, y el artículo 23.1 de la LSSI, no exigen que los contratos se celebren por medios manuscritos, aceptando que estos se encuentren en formato electrónico, y que su ratificación también se pueda realizar mediando un instrumento electrónico.

No obstante, para que un contrato electrónico, firmado mediante firma electrónica pueda surtir efectos, y se asegure el respeto a la voluntad contractual y el consentimiento de las partes será necesario:

- Que exista la voluntad o consentimiento de las partes (arts. 1262-1270, CC).
- Que exista un objeto o que exista un fin contractual (arts. 1271-1273, CC).
- Que dicho objeto esté fundamentado en una causa lícita (arts. 1274-1277, CC).

02.1.4. Conclusión

[1] La Ley 59/2003 fue derogada por la Ley 6/2020 y sustituida por el Reglamento eIDAS y la Ley 6/2020.

En base a lo expuesto con anterioridad, en España los documentos firmados electrónicamente causan plenos efectos jurídicos y tienen validez legal como prueba documental en los procedimientos judiciales.

Por lo tanto, la firma electrónica de Signaturit (o el servicio de entrega electrónica certificada) podrá utilizarse para la firma (o el envío) de todo tipo de documentos que no estén sujetos a exigencias de forma específicas. En particular, se podrá utilizar la firma electrónica en documentos en el ámbito de las relaciones de los ciudadanos con la Administración y, especialmente, en las relaciones entre empresas o entre empresas y clientes (todo tipo de contratos que no requieran de exigencia de formalismo específico o que requieren establecerse "por escrito", a saber, contrato de prestación de servicios, de arras, mandatos de venta, etc.), y entre éstas y los consumidores (es decir, en el ámbito del denominado comercio electrónico).

03. Signaturit como Prestador de Servicio de Confianza.

03.1. Definición y supervisión

El Reglamento (UE) 910/2014 recoge como definición de Prestador de Servicios Electrónicos de Confianza: "*una persona física o jurídica que presta uno o más servicios electrónicos de confianza, bien como prestador cualificado o como prestador no cualificado de servicios electrónicos de confianza*".

Los servicios de confianza a los que hace alusión son los siguientes:
"la creación, verificación y validación de firmas electrónicas, sellos electrónicos o sellos de tiempo electrónicos; servicios de entrega electrónica certificada y certificados relativos a estos servicios; o la creación, verificación y validación de certificados para la autenticación de sitios web; o la preservación de firmas, sellos o certificados electrónicos relativos a estos servicios."

Los Prestadores de Servicios de Confianza podrán ser no cualificados o cualificados, siendo éstos últimos aquellos prestadores que han recibido la cualificación del organismo de supervisión en base a lo establecido en el Reglamento eIDAS. A tal efecto, entre las funciones de los organismos de supervisión se encuentra la de supervisar a los Prestadores Cualificados de Servicios de Confianza establecidos en el Estado miembro, a fin de garantizar, mediante actividades de supervisión previas y posteriores, que dichos prestadores cualificados y los servicios de confianza cualificados prestados por ellos, cumplen los requisitos establecidos en el Reglamento. En España, el organismo de supervisión es el Ministerio de Asuntos Económicos y Transformación Digital.

El Reglamento eIDAS establece una serie de requisitos de seguridad de aplicación a los Prestadores de Servicios de Confianza, sean éstos cualificados o no. Así deberán adoptar las medidas técnicas y organizativas adecuadas para gestionar los riesgos para la seguridad de los servicios de confianza

que prestan. Dichas medidas **garantizarán un nivel de seguridad** proporcionado al grado del riesgo, y en particular se adoptarán medidas para evitar y reducir al mínimo el impacto de los incidentes de seguridad e informar a los interesados de los efectos negativos de dichos incidentes.
El Ministerio de Asuntos Económicos y Transformación Digital, en su página web, lleva a cabo un registro y publicación tanto de los Prestadores de Servicios de Confianza Cualificados como de los no cualificados. En este sentido, Signaturit consta registrada como Prestador Cualificado de Servicios de Confianza, para las siguientes categorías de servicios, habiendo, por tanto, dado cumplimiento al deber de comunicación previsto en la normativa:

"Servicio de expedición de certificados electrónicos cualificados de firma electrónica"

Por otro lado, Signaturit consta registrada como Prestador de Servicio de Confianza, para varios servicios No cualificados:

- En la categoría de "Otros servicios en relación con la firma electrónica de documentos": Servicio consistente en la puesta a disposición de los medios telemáticos necesarios (integración web, firma móvil) para que los clientes de Signaturit y sus terceros de interés realicen la firma y gestión de documentos electrónicos (p.ej.: contratos) con plena validez legal.
- En la categoría de "Servicio de entrega electrónica certificada". Servicio consistente en el envío de comunicaciones certificadas (ej.: Email y SMS) para enviar contratos y notificaciones con acuse de recibo.
- En la categoría de "Servicio de entrega electrónica certificada": Servicio consistente en la puesta a disposición (notificación) de los medios telemáticos necesarios (integración web, firma móvil) para que los clientes de Signaturit y sus terceros de interés realicen la firma y gestión de notificaciones electrónicas.

La condición de Signaturit como Prestador de Servicios de Confianza puede comprobarse ante:
A) La Secretaria de Estado de Digitalización e Inteligencia Artificial integrada en el Ministerio Para la Transformación Digital y de la Función Pública, a través del siguiente enlace: https://avancedigital.mineco.gob.es/es-es/servicios/firmaelectronica/paginas/prestadores.aspx

B) La lista de Prestadores de Servicios de Confianza de la Unión Europea por países publicada por la Comisión de la Unión Europea a través del siguiente enlace:
https://eidas.ec.europa.eu/efda/tl-browser/#/screen/home

03.2. Garantías que ofrece un Prestador de Servicios de Confianza

Enmarcado dentro de una regulación específica y controlado por un organismo estatal, un Prestador de Servicios de Confianza permite ofrecer las garantías de seguridad requeridas a todo proceso

informático y de cumplimiento normativo en cuanto a los requisitos legales y técnicos necesarios para otorgar validez jurídica al acto o documento que se procesa electrónicamente.

Así, como veremos a continuación, en un proceso de firma electrónica entran en juego varios factores que permitirán consolidar la autenticidad del documento, la identidad del o los firmantes y en general, de cada paso del proceso de envío y recepción del documento electrónico.

Es importante señalar que un Prestador de Servicios de Confianza es un tercero ajeno a la relación jurídica que puedan establecer las partes que usan sus servicios, por lo que ofrece las garantías de neutralidad frente a las pretensiones de una u otra en caso de conflicto, pudiendo certificar la integridad y autenticidad de los eventos electrónicos producidos y registrados en sus sistemas con imparcialidad y aportando por tanto la seguridad jurídica y validez probatoria ante un procedimiento judicial.

Ese rol del Prestador de Servicios de Confianza (antiguamente también llamado "Tercero de confianza" según la LSSI) es precisamente lo que permite crear un clima de confianza que haga posible y refuerce el comercio electrónico y las transacciones digitales en la UE, tal como lo ha fomentado el Reglamento eIDAS.

04. Funcionamiento de la Plataforma de firma electrónica Signaturit

04.1. Descripción general de un proceso de firma electrónica con Signaturit

La Plataforma Signaturit funciona de la siguiente forma: desde su cuenta de usuario, el cliente (remitente) genera un proceso o circuito de firma escogiendo el nivel de firma deseado (firma simple, firma avanzada con biometría, con firma OTP o firma con certificado digital) y sube uno (o varios) documento previamente elaborado por él que dese enviar a firmar a las personas interesadas (destinatarios o firmantes).

A continuación, el remitente puede configurar el lugar donde desea que aparezca la firma del firmante en el documento y añadir acciones adicionales (widgets) que deberá efectuar el destinatario como poner la fecha, el lugar, rellenar un checkbox a modo de aceptación de un texto especifico o bien incluso incluir un texto.

Finalmente, el remitente debe informar de la identidad del destinatario con su nombre y apellidos así como su dirección de correo electrónico personal. Adicionalmente puede añadir su número de

teléfono para el envío de un código OTP y así reforzar la eficacia de la firma electrónica mediante un factor de autenticación adicional.

Una vez lanzado el proceso, desencadena el envío de un correo electrónico al destinatario que deberá abrir un enlace que le permitirá entrar en el entorno controlado del Prestador Signaturit y deberá seguir los pasos indicados hasta completar el proceso de firma. Cada acción realizada por el destinatario quedará registrada en los sistemas de Signaturit generando tantas evidencias como eventos producidos.

Todas las evidencias de la transacción generadas durante el proceso de firma son recogidas en el documento probatorio (**Audit Trail**) generado por el Prestador para cada proceso, a través del cual las partes van a poder hacer valer las evidencias generadas de forma fácilmente comprehensible.

Dicho documento probatorio que contiene las evidencias generadas durante todo el proceso de firma queda firmado electrónicamente y que, junto a la posterior aplicación del algoritmo de encriptación, asegura la integridad de los datos y su validez legal como prueba de a quién se ha enviado un documento, cuándo y dónde se ha recibido, etc...

Los algoritmos de cifrado utilizados son altamente seguros y se basan en claves criptográficas que garantizan la confidencialidad de los datos. Esto significa que sólo los destinatarios autorizados pueden acceder a la información contenida en el documento enviado.

Utilizamos, por tanto, técnicas de encriptación y autenticación para garantizar la integridad del documento y evitar así posteriores modificaciones de las que no quedaría evidencia sin el uso de estas técnicas. Esta integridad implica que las evidencias electrónicas generadas durante el proceso de envío de email certificado a través de Signaturit existieron y no pueden ser alteradas desde un instante específico en el tiempo.

04.2. El proceso de Firma avanzada de Signaturit

El artículo 26 del eIDAS establece los requisitos que debe cumplir una firma electrónica avanzada para ser válida. Signaturit cumple con los requisitos del mencionado artículo 26 de la siguiente manera:

1. A los efectos de garantizar que la firma se asocia a un único firmante, se envía el documento a la dirección de correo electrónico del firmante en cuestión;
2. Para poder identificar al firmante, obtenemos la geolocalización al momento de la firma, las direcciones IP de origen y destino de la solicitud, la fecha/hora de la firma y los datos biométricos del grafo del firmante (presión, velocidad y aceleración); adicionalmente se refuerza dicha identificación del firmante mediante el segundo factor de autenticación que constituye el Código OTP enviado a su teléfono móvil.
3. El pleno control de la firma se garantiza mediante la posibilidad que otorgamos al firmante de firmar el documento en cuestión mediante cualquier dispositivo con acceso a internet (ordenador, tablet, móvil); y

4. Impedimos cualquier cambio ulterior en la firma garantizando la integridad del documento. Para garantizar la absoluta integridad, ciframos el documento e incluimos un sellado de tiempo cualificado que asegura que los datos del documento no han sido alterados desde el momento de su firma.

Todas las evidencias electrónicas generadas por Signaturit en el proceso de firma se reflejarán en un documento probatorio o audit trail. El audit trail recoge toda la información relevante recabada en el proceso de firma, pudiendo ser presentado como prueba judicial ante cualquier Tribunal.

El documento probatorio contiene la siguiente información:

- **Identificador único de la transacción**

Queda registrado e indicado tanto en el Audit Trail, como en el mismo documento firmado a fin de correlacionar los documentos. A parte de ello, cabe recordar que ambos documentos (documento firmado y Audit Trail) se reciben automática y simultáneamente al correo del emisor por lo que existe un doble factor de correlación entre documentos.

Se vincula al firmante mediante la generación de hashes que identifican el documento, el identificador privado, el proceso de identificación de la firma y las referencias biométricas de la firma por cada uno de los firmantes.

- **Nombre del firmante y su dirección de correo electrónico**

Existe una vinculación precisa y única en tanto que el firmante recibe un correo electrónico a su dirección de correo electrónico de la cual es titular.

Existen otras medidas para reforzar dicha vinculación que incluirían como añadido en este correo electrónico la aplicación de medidas OTP (One Time Password) a fin de poder proceder a la firma del documento en cuestión o la validación de IDs, pasaportes, entre otros, mediante nuestra tecnología OCR.

- **Evidencias del proceso**

Se permite identificar al firmante mediante el registro de todas las evidencias relativas a la dirección IP, hora, geolocalización y el tipo de dispositivo. Asimismo, también se permite trazar el documento recabando el momento del envío, las veces que este ha sido abierto, el momento de la aceptación de los términos y condiciones, así como cuando ha sido firmado.

  - Dirección IP
  - Geolocalización
  - Historial de autenticación
  - Cadena de custodia (ej. enviado, visto, firmado, etc.)
  - Estado completado

- **Sellado de tiempo oficial**

Mediante la utilización del sellado de tiempo se garantiza la integridad del conjunto de datos electrónicos que conforman la firma electrónica. Es decir, el sello de tiempo garantiza que una firma se realizó en un momento determinado imposibilitando su modificación posterior, puesto que se encripta y se sella el documento una vez se ha finalizado el proceso de firma.

- **Datos biométricos**

La información biométrica que capturamos proviene de la información sobre el grafo, consistente en los puntos que lo integran y su posición, la velocidad, la aceleración y finalmente, en los dispositivos que lo permiten, la presión con que se realiza.

Cabe destacar que la presión es un dato adicional de la biometría de la firma, la cual se define como rasgos únicos de cada persona. En los casos en que el dispositivo no permita recabar datos de presión, mediante algoritmos informáticos se recaba la pseudo presión que permite adaptar el grueso del trazo a la velocidad de la firma. En consecuencia, se requiere un dispositivo homologado para cubrir los requisitos definidos en la ISO/IEC 19795-7 para que resulte plenamente válida.

Destacar que la actividad de Signaturit se encuentra amparada por el artículo 9.2 del RGPD ya que, para poder recoger los datos biométricos, solicita el consentimiento previo y expreso a los titulares de dichos datos, para poder tratarlos con el único objeto de poder identificar a quienes firman documentos a través de su plataforma, dentro de un proceso general de firma electrónica.

04.3. El proceso de entrega electrónica certificada

El proceso de entrega electrónica certificada que ofrece la Plataforma de Signaturit tiene dos modalidades de envío:

- Por sms
- Por correo electrónico

Cada una de dichas modalidades permiten a su vez realizar dos tipos de entregas electrónicas:

- Comunicación electrónica certificada: se certifica el contenido de un mensaje enviado por sms o por email
- Notificación electrónica certificada: se certifica el contenido de un mensaje enviado por sms o por email pero sobre todo la entrega y apertura de documentos adjuntos.

En cada envío se deja constancia de las siguientes evidencias:

- Entrega del mensaje a su destinatario con constancia de fecha y hora
- Apertura y lectura de documentos adjuntos
- Contenido de los documentos

Todas las evidencias se recogen en el documento probatoria similar al que se genera en procesos de firma electrónica (ver punto anterior)).

05. Validez legal de las firmas y entregas electrónicas realizadas con Signaturit

05.1. Validez de la firma electrónica con trazo digital y recogida de datos biométricos

Tal como se indicó anteriormente, para cumplir con los requisitos necesarios para brindar un servicio de firma electrónica avanzada en cumplimiento del artículo 26 del eIDAS, Signaturit debe poder identificar al firmante. La información de datos biométricos de la firma realizada por el firmante que recoge Signaturit permite brindar seguridad a nuestros clientes, ya que, llegado el caso que cualquiera de los firmantes negase su autoría, podremos recurrir a la información recabada para probar la identidad del firmante en cuestión.

A todo evento, resulta importante aclarar que los datos biométricos que obtiene Signaturit permanecen encriptados: como regla general, nadie podrá tener acceso a los datos y éstos permanecerán bloqueados hasta que por alguna circunstancia excepcional deban ser presentados para su análisis, en especial, ante sede judicial por el acaecimiento de algún conflicto que se hubiese originado alrededor de la firma del documento en cuestión.

A nivel de privacidad, de acuerdo con el RGPD se entenderán como datos biométricos aquellos datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como por ejemplo imágenes faciales o datos dactiloscópicos.

En consecuencia, serán considerados datos biométricos aquellos datos que permitan identificar a una persona y/o confirmar quién es mediante la realización de tratamientos técnicos que recojan datos relativos al aspecto físico, corporales o conductuales.
Asimismo, el RGPD cataloga a los datos biométricos como una categoría especial de datos personales. El artículo 9.2 del RGPD permite el tratamiento de los datos biométricos toda vez que haya mediado el consentimiento por parte del interesado. En concreto, el apartado a) del mencionado artículo 9.2 establece que: [la prohibición no resultará aplicable cuando ocurra lo siguiente] "*que el interesado por dicho tratamiento hubiera otorgado su consentimiento explícito para dicho tratamiento con uno o más de los fines especificados, excepto que existiera una prohibición legal a nivel europeo o estatal sobre ello*".

En tal sentido, la actividad de Signaturit se encuentra amparada en dicho artículo: Signaturit se encuentra autorizada a recoger datos biométricos ya que, para poder hacerlo, solicita el consentimiento previo y expreso a los titulares de dichos datos. En concreto, Signaturit pide consentimiento a los titulares de los datos biométricos para poder tratarlos con el único objeto de poder identificar a quienes firman documentos a través de su plataforma, dentro de un proceso general de firma electrónica.

05.2. Validez de la firma electrónica con clave OTP

En la actualidad gran cantidad de países requieren normativamente que para obtener un número de teléfono móvil sea necesario un proceso de verificación de la identidad del usuario. En España la emisión de una SIM móvil requiere esta identificación por parte de, así como la firma de un contrato. Por ello, una línea móvil está necesariamente vinculada a una persona física o jurídica.

Por ello, se cumplen los requisitos establecidos para que una firma electrónica sea considerada de tipo avanzada según el artículo 26 del Reglamento eIDAS antes comentados. A continuación, se analizan con la solución de firma con OTP SMS:

1. Estar vinculada al firmante de manera única. El firmante posee un teléfono móvil con un número de teléfono
2. Permite identificar al firmante. El número de teléfono es personal y le pertenece, exclusivamente.
3. La firma debe haber sido creada utilizando medios de creación de la firma que el firmante pueda utilizar con alto nivel de confianza y bajo su control exclusivo. Tanto el acceso a la petición de firma, como el código SMS, quedan bajo el control exclusivo de la persona que firma (enviados al email y al teléfono móvil de la persona firmante, respectivamente).
4. Está vinculada con los datos firmados de forma que cualquier alteración posterior pueda ser detectada. El documento queda vinculado al Audit Trail y asimismo, se le estampa un sello cualificado de tiempo que permite detectar cualquier modificación en el documento.

Por otra parte, hay que tener presente que esta correspondencia no ocurriría en aquellos países donde se puedan obtener tarjetas SIM de forma anónima. En el proceso de firma OTP el número de teléfono queda vinculado a la operación de firma con la persona firmante y el contenido se vincula además con el OTP creado y además se obtienen evidencias adicionales y la trazabilidad del mensaje en el documento Audit Trail.

05.3. Validez de la entrega electrónica certificada

Tal como hemos indicado en el apartado 2.1.1, el servicio de entrega electrónica certificada es un servicio reconocido por el Reglamento eIDAS por lo que goza de validez jurídica, incluso si no es cualificado, en base a lo dispuesto en el artículo 43:

Para obtener este reconocimiento, es necesario que el proceso de entrega bien sea por sms bien sea por email, cumpla una serie de requisitos:

- Transmisión de datos entre terceras partes por medios electrónicos
    - Identificación del emisor
    - Identificación del receptor (email o teléfono móvil)
- Generación de pruebas:
    - Del envío de los datos transmitidos

    - De la recepción
    - Del contenido del mensaje
    - De los documentos adjuntos
- Protege los datos del riesgo de pérdida, robo, deterioro o alteración no autorizada.
    - Sello electrónico del Prestador
    - Sellado de tiempo

Al ser un servicio de confianza eIDAS prestado por un Prestador de Servicios de Confianza, las normas nacionales sobre la prueba -como el art. 326.3 de la LEC en España-, reconocen su eficacia jurídica al igual que las pruebas aportadas en formato papel, según la naturaleza pública o privada del documento.

En definitiva, con los servicios de Signaturit podrás aportar seguridad a tus procesos de digitalización contando con todas las evidencias que permitan convencer a cualquier parte, juez o tribunal sobre la autenticidad de la prueba electrónica aportada, y protegerse así ante la hipotética impugnación de la contraparte. Y si aun así, necesitas nuestra intervención en caso de litigio o impugnación, podrás contar con la ayuda de nuestros equipos para asesorarte y de nuestro equipo legal en caso de necesitar la elaboración de informes o intervención en juicio*.

(*consultar tarifica aplicable)

Departamento Legal Grupo Signaturit.