# PLAN DE INSPECCIÓN DE OFICIO SOBRE CONTRATACIÓN A DISTANCIA EN OPERADORES DE TELECOMUNICACIONES Y COMERCIALIZADORES DE ENERGÍA

# Contenido

# RESUMEN EJECUTIVO

La utilización de nuevas tecnologías se ha aplicado en todos los sectores permitiendo que se realicen contrataciones de servicios fundamentales para los ciudadanos. Estamos hablando de sectores como operadores de telecomunicaciones, comercializadores de energía, entidades financieras, seguros, etc., que realizan parte de sus contratos utilizando la red y sin presencia física simultánea de los implicados en la contratación.

La Agencia Española de Protección de Datos como Autoridad de Control tiene entre sus funciones promover la sensibilización del público y su comprensión de los riesgos, normas y garantías y derechos en relación con los tratamientos de datos personales, así como concienciar a los responsables y encargados del tratamiento acerca de sus obligaciones. Por otra parte, siempre ha sido consciente de que el mayor problema que se plantea en la utilización de medios digitales es la posible suplantación de identidad y las consecuencias negativas para los ciudadanos, así como la necesidad de que las empresas estén en condiciones de acreditar los servicios contratados cuando estos se realizan a distancia y por tanto sin presencia de los contratantes.

Es sabido que existen otros riesgos asociados a la contratación electrónica como el robo de credenciales, por ejemplo mediante phishing y la suplantación de identidad del proveedor de servicio, No obstante, dentro del Plan Estratégico de la Agencia se ha acometido este Plan de inspección de Oficio con el objetivo de analizar los tratamientos de datos en los sectores de operadores de telecomunicaciones y comercializadores de energía, su adecuación a la normativa de protección de datos siempre visto desde la perspectiva de acreditar la identidad del contratante y de los servicios contratados.

En todo momento se ha hecho hincapié en verificar los procedimientos que se utilizan en estos sectores para identificar a los interesados y con ello evitar, en lo posible, la suplantación de identidad y el consiguiente fraude. También se ha prestado especial atención a la manera en que las empresas acreditaban la contratación de sus servicios. Por ello, se han realizado actuaciones en entidades que están implantando proyectos innovadores para salvar estos escollos. Los procedimientos analizados han sido: firma manuscrita electrónica, reconocimiento facial, productos de análisis de riesgos on-line, notificación electrónica certificada y prueba acreditativa de los sucesos digitales.

Es reseñable indicar que durante el transcurso del presente Plan, la aplicación de la normativa de protección de datos ha evolucionado positivamente en muchos aspectos y ha significado un cambio sustancial en la forma de acometer los tratamientos de datos en ambos sectores ya que debido al volumen de datos que gestionan se han visto en la necesidad de realizar evaluaciones de impacto de procedimientos ya implantados e impulsar mecanismos para garantizar la privacidad y la seguridad de la información con la nueva visión adoptada a raíz del Reglamento UE 2016/679, Reglamento General de Protección de Datos (RGPD) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD).

# INTRODUCCIÓN

La transformación digital es el resultado de un proceso continuo de cambio y adaptación a las nuevas tecnologías que avanzan muy rápidamente y alcanza a todos los sectores empresariales y sociales. Este avance tiene que ir acompañado de modelos jurídicos que le permitan desarrollarse y al mismo tiempo ser respetuosos con el derecho fundamental a la protección de datos de los usuarios.

La Agenda Digital para Europa, principal instrumento para el cumplimiento de los objetivos de la Estrategia Europa 2020, persigue que para 2020 todos los europeos tengan la posibilidad de acceder a conexiones de banda ancha a una velocidad como mínimo de 30 Mbps, y que, al menos, un 50 % de los hogares europeos estén abonados a conexiones de banda ancha superiores a 100 Mbps. Estos objetivos han quedado incorporados a la agenda digital española, aprobada por el Gobierno en febrero de 2013.

Por otra parte, y con motivo de la liberalización de los sectores de suministro de gas y electricidad, las compañías comercializadoras pueden contratar directamente con los clientes (persona física o jurídica), realizando todas las gestiones asociadas a los suministros.

En su momento, el desarrollo normativo asociado a esta liberalización introdujo dos novedades relevantes. Por un lado, se configura la Base de Datos de Puntos de Suministro (SIPS) que las distribuidoras han de poner a disposición de las empresas comercializadoras y que deberán mantener de forma permanente para garantizar el contenido actualizado de cada uno de los datos que componen dichas bases. Por otra parte, se crea la "Oficina de Cambios de suministrador", que realiza sus funciones en los sectores de gas natural y de la electricidad y cuyo objeto social exclusivo es la supervisión de los cambios de suministrador, y tal y como se especifica en la normativa tendrán "*la responsabilidad de la supervisión de los cambios de suministradores conforme a los principios de transparencia, objetividad e independencia…*"

La Agencia Española de Protección de Datos siempre ha destacado la importancia de la tecnología para el progreso y pone de manifiesto la relevancia de la norma jurídica que se dispone actualmente con el Reglamento Europeo de Protección de Datos que permite a las Autoridades de Control un modelo de supervisión para acompañar este proceso. Asimismo, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y Garantía de los Derechos Digitales que adapta el derecho español al modelo establecido en el Reglamento, exige a las Autoridades de Control la supervisión de la aplicación de dicho marco jurídico con el fin de proteger los derechos y las libertades fundamentales de la personas físicas en lo que respecta al tratamiento de datos personales y acompañar este proceso continuo de cambio y adaptación a las nuevas tecnologías.

Entre las funciones encomendadas a la Agencia Española de Protección de Datos como Autoridad de Control se encuentra la de promover la sensibilización del público y su comprensión de los riesgos, normas y garantías y derechos en relación con los tratamientos de datos personales, así como concienciar a los responsables del tratamiento acerca de sus obligaciones.

La adaptación de las nuevas tecnologías ha extendido, entre la población, otras formas

de contratación en las que ya no se requiere la presencia física simultánea de los contratantes. Esta situación conlleva la necesidad de garantizar la identificación de los titulares y de los contratos formalizados a través de los medios telemáticos puestos a disposición de los consumidores.

El principal problema que se plantea en la utilización de medios digitales en la contratación es la posible suplantación de identidad y las consecuencias negativas para los ciudadanos. Por otra parte, los responsables deben estar en condiciones de acreditar los servicios contratados cuando estos se realizan a distancia y, por tanto, sin presencia de los contratantes. Todo ello pone de manifiesto la necesidad de establecer sistemas que minimicen el riesgo que supone la suplantación de identidad y la contratación fraudulenta

# OBJETIVOS

La Agencia Española de Protección de Datos, conocedora de la dificultad que entraña la identificación de los consumidores que utilizan medios telemáticos en la contratación de servicios ofertados a través de la red, ha incluido en su *Plan Estratégico* la realización de actuaciones de oficio que tienen como objetivo verificar, dentro de las competencias que legalmente tiene atribuidas, el grado de cumplimiento de la normativa de protección de datos en la contratación de estos servicios, con el fin de facilitar el cambio hacia el entorno digital y contribuir al desarrollo de estos nuevos modelos en un marco respetuoso con los derechos de los afectados.

En su función preventiva y de sensibilización de los responsables se afronta este Plan de Auditoría Preventiva cuya finalidad es obtener una imagen de los procesos involucrados en los sectores de operadores de telecomunicación y comercializadores de energía que permita elaborar unas recomendaciones haciendo hincapié en la identidad del contratante y la acreditación de la contratación efectuada.

# METODOLOGÍA Y ACTUACIONES REALIZADAS

El Plan de Auditoría se ha estructurado en fases en base a los dos sectores estudiados: Se han analizado algunos de los proyectos que se están implantando con objeto de hacer más segura la contratación a distancia que, como se estipula en la Ley General para la Defensa de los Consumidores y Usuarios, abarca todos los casos en los cuales los contratos se celebran entre el empresario y el consumidor-usuario en el marco de un sistema organizado de venta o prestación de servicios a distancia, exclusivamente mediante el uso de una o varias técnicas de comunicación.

Las empresas que se dedican al sector de las telecomunicaciones disponen de millones de datos de ciudadanos, por ello, el Plan se ha dirigido básicamente a grandes compañías que tienen autorización para la distribución, están implantadas en todo el territorio nacional y ofrecen todos los servicios generales de telecomunicación: telefonía fija, telefonía móvil (también denominado OMR –operador móvil con red-), televisión e Internet, y, además, comercializan diferentes marcas. No obstante, se han realizado también investigaciones en empresas más pequeñas que ofertan servicios de operador de telefonía móvil virtual (también denominado OMV –operador móvil virtual-) que utilizan las redes de comunicación de aquellas operadoras que tienen red de

telecomunicaciones.

Con la liberalización del mercado de gas, en el año 2008, aumentaron las empresas comercializadoras de gas y tras las últimas reformas energéticas que tuvieron lugar en el año 2009 y 2013, han surgido nuevas compañías comercializadoras de electricidad con un alto volumen de datos de los consumidores. El estudio se ha dirigido a seis de las comercializadoras de energía con un gran volumen de contrataciones.

Por último, se han realizado actuaciones presenciales que han permitido el estudio de cinco de proyectos que comienzan a implantarse en los mercados: firma manuscrita electrónica, reconocimiento facial, productos de análisis de riesgos on-line, notificación electrónica certificada y prueba acreditativa de los sucesos digitales.

# ASPECTOS GENERALES

## *OPERADORES DE TELECOMUNICACIONES*

La mayor parte de las grandes operadoras de telefonía cuentan con diferentes marcas comerciales que ofrecen tipos diferentes de tarifa y están dirigidas a diferentes segmentos de clientes. En unos casos todas las marcas comerciales operan bajo el mismo NIF y en otros tienen diferentes, pero participadas por la operadora matriz. Por otro lado, cada una de las marcas comerciales tiene su propio sistema de información y estrategia comercial.

A la hora de la contratación son los propios interesados los que aportan sus datos personales y de facturación. En los casos de canal telefónico suelen ser grabados directamente como medida acreditativa de la contratación y, en los de portabilidad de la línea de otra compañía lo hacen a través de una tercera entidad (con la que tienen contrato de prestación de servicios como encargados del tratamiento) con objeto de verificar los datos aportados, tal como está estipulado en la normativa vigente (Circulares 1/2008 y 1/2009 de la CMT, actualmente CNMC). El teleoperador informa de la Política de Privacidad utilizando argumentarios, solicita consentimiento para el envío de comunicaciones comerciales y se suele remitir a la web para la ampliación de la política de privacidad.

En los contratos realizados telemáticamente, los interesados aportan sus datos utilizando las webs del operador con el que desean contratar. En los casos de portabilidad esta información se registra en un sistema informático a la espera de la conformidad del operador propietario de la línea (operador donante), momento en el cual el interesado pasa a ser cliente del nuevo operador.

En las webs se informa de la Política de privacidad y se solicita consentimiento sobre diversos aspectos: recibir comunicaciones comerciales, recibir comunicaciones comerciales de terceros, comunicación a empresas del Grupo o utilización para adoptar decisiones automatizadas, entre otros.

Todos los operadores disponen de aplicaciones para móviles que permiten realizar diferentes tipos de acciones, desde contrataciones de productos de valor añadido, nuevos terminales móviles, nuevas líneas telefónicas, cambios de tarifa… a aplicaciones meramente informativas. Con carácter general, no se permite una contratación nueva por esta vía sin ser anteriormente cliente.

En caso de contratación de nuevas líneas o clientes se realizan estudios de solvencia con los datos recabados en el momento de la contratación o los ya existentes en caso de un cliente, que incluyen la consulta a los sistemas comunes de información crediticia.

### *Acreditación de la identidad del contratante*

En las tiendas de algunas operadoras de telefonía se puede entregar el terminal móvil adquirido a los clientes que hayan contratado por medios telefónicos o telemáticos, en cuyo caso se solicita la presentación de un documento oficial de identidad (DNI, NIE, pasaporte) y un documento bancario que acredite que la cuenta sobre la que se van a realizar cargos es titularidad del contratante.

También se realizan entregas utilizando el servicio de Correos que comprueba el DNI del cliente utilizando un sistema de escaneo para recabar la copia.

Las contrataciones telefónicas suelen ser grabadas y en los casos de portabilidad, una tercera entidad realiza la verificación por terceros.

Las empresas de telecomunicaciones están embarcadas en nuevos proyectos que permiten acreditar la identidad del potencial cliente con anterioridad a la formalización de la contratación por Internet. Hablamos de proyectos novedosos como el reconocimiento facial mediante el envío de un mensaje SMS con un enlace a una aplicación que le permitirá al cliente remitir una imagen del DNI y una prueba de imagen de su rostro consistente en una fotografía en tiempo real de la cara del cliente, de tal forma que se analizará biométricamente la fotografía y la comparará con la del DNI para garantizar que es el titular de este documento el que está solicitando la contratación.

Otro proyecto, ya implantándose en muchos operadores, está dirigido a verificar la identidad del cliente y la titularidad de la cuenta corriente en el proceso de contratación por Internet y previa autorización del titular de la cuenta (avalado por la normativa PSD2 Europea de Regulación de Pagos, *Payment Service Providers Directive)* que permitirá el acceso de terceros a las cuentas de los clientes de un banco y el inicio de pagos en su nombre.

### *Acreditación de la contratación a distancia*

Las empresas de telecomunicaciones también están implantando proyectos que permitan acreditar la contratación de los servicios y los consentimientos otorgados por el cliente en el momento de la contratación.

Uno de los servicios que se empiezan a implantar corresponde a la utilización de un tercero de confianza el cual que permite certificar que el cliente, a través de la web, ha contratado y aceptado los tratamientos de datos, generando un fichero con los datos recabados y firmados digitalmente, cifrando además todo el contenido, de tal manera que cualquier modificación supondría un nuevo fichero.

En los casos de portabilidad se suelen remitir mensajes SMS al teléfono que se desea portar antes de activar el pedido que, como medida de control adicional, debe ser contestado aceptando el encargo. En caso de utilizar notificación electrónica certificada, un tercero de confianza certifica la entrega del mensaje.

Con carácter general, se almacena la dirección IP y la fecha y hora en que se produjo

la contratación, asociados a los datos del cliente en su ficha o en el Registro de accesos (LOG).

### *Verificación de la identidad del cliente en procesos posteriores*

En el Área de Clientes de la web, lo clientes se identifican y autentican a través de código de usuario y contraseña. Debido a que un cliente puede tener contratadas más de una línea, el código de usuario puede ser número de línea (acceso solo a los datos asociados a la línea consultada) o DNI (accesos a todos los datos asociados a las líneas contratadas por el usuario)

En los departamentos de Atención al Cliente (canal telefónico) de las diferentes compañías se suele identificar al cliente por nombre completo, DNI y un tercer dato aleatorio como domicilio al que se envían las facturas o número de la cuenta bancaria, aunque muchas compañías proporcionan una contraseña (a solicitud del cliente) que debe ser indicada para proceder al acceso a los datos.

### *Alertas*

Algunas empresas del sector han identificado diferentes circunstancias que pueden ser susceptibles de fraude en la contratación (alta concentración de pedidos en determinadas zonas, mismas direcciones IP…) y han implantado procedimientos que permitan alertar de estas anomalías y determinen la probabilidad de fraude, en cuyo caso, se suelen verificar las contrataciones por especialistas y se puede requerir documentación complementaria al cliente.

También en caso de impagos se hacen pruebas aleatorias de fraude. Ante la sospecha fundada de un fraude o una suplantación de identidad, se cancela la deuda que hubiera podido contraerse y se buscan casos que pudieran estar relacionados.

## *COMERCIALIZADORES DE ENERGÍA*

Existen múltiples servicios ofertados por las empresas comercializadoras de energía. No obstante, los más relevantes respecto de la normativa de protección de datos corresponden a:

- nuevas contrataciones en las cuales el cliente no tiene servicio con ninguna otra compañía comercializadora,
- cambio de comercializadora en el cual el cliente tiene un contrato activo con otra empresa,
- cambio de titular en el caso de un contrato activo en el que se modifica el titular manteniendo el contrato con la misma compañía comercializadora.

Además de estos servicios, todas las comercializadoras ofertan modificaciones sobre el contrato activo: cambio de tarifa, modificaciones de potencia… y también ofrecen al cliente la posibilidad de contratar servicios de mantenimiento asociados a la energía.

Las compañías disponen de distintos canales para realizar contrataciones. Las más habituales corresponden con: contratación presencial, solicitudes de contratación a través de webs y app para móvil y solicitudes telefónicas, ya sean iniciadas por el interesado o por el call center de la entidad o de terceras empresas con contratos de prestación de

servicios. Asimismo, se suele ofertar un sistema combinado entre las solicitudes vía web y la contratación telefónica (venta asistida -*click to call-).*

Sea cual sea el canal elegido por el cliente para realizar la contratación, en el caso de cambio de comercializadora se envía una solicitud de cambio del nuevo comercializador al distribuidor de energía, el cual acepta o rechaza su tramitación. Si la solicitud es aceptada, el distribuidor realiza el cambio y lo comunica a ambas comercializadoras.

Los clientes acceden a través de webs o de las App en ambos casos con una aplicación similar y cumplimentan los datos en el formulario de registro (solicitud o pedido) con los datos personales del titular, datos bancarios, punto de suministro y datos de la anterior comercializadora, en su caso, incluyendo una contraseña para procesos posteriores y la aceptación de la política de privacidad (en algunas compañías se deben aceptar diferentes cláusulas de consentimiento individualmente que corresponden a finalidades distintas al servicio contratado y que cumplen las condiciones del consentimiento). Una vez finalizado, se le asigna un número de pedido y generalmente se envía un correo electrónico al interesado indicando la documentación que debe aportar para activar el servicio. El formulario es revisado por personal de la compañía encargado de la tramitación de las contrataciones hasta la activación del servicio.

En los casos en los que el interesado ya es cliente de la compañía y solicita una nueva contratación, el proceso es similar permitiendo incluir datos del nuevo contrato y de las formas de pago.

Además de los datos personales y del servicio se solicita al cliente la aportación de una copia del DNI o documento acreditativo de identidad y, en algunas empresas, una copia de una factura bancaria del solicitante. En las solicitudes a través de App suelen pedir una foto de la factura.

La mayor parte de las compañías ponen a disposición del cliente, en el Área de Clientes de la web, un documento “pdf” con el contrato y las condiciones suscritas. Algunas utilizan terceras empresas con objeto de acreditar la contratación on-line.

Todas las compañías remiten el contrato en soporte papel al domicilio indicado por el cliente.

Las comercializadoras de energía también proporcionan un canal telefónico para contratar con los interesados. En este caso, proporcionan sus datos registrándose directamente en la empresa y, posteriormente, son revisados por el departamento encargado de las tramitaciones y activación del servicio. Se solicita la misma documentación para finalizar el contrato (copia del DNI, factura bancaria).

Las llamadas son grabadas como medida de acreditación de la contratación y de los consentimientos otorgados.

Un caso especial y muy frecuente tiene que ver con la solicitud de cambio de titular sobre un contrato ya activo. El nuevo titular realiza la solicitud por la web o contacta telefónicamente con la compañía. Las empresas han establecido un procedimiento en el cual se solicitan los datos personales del titular, datos de suministro y datos personales del nuevo titular con objeto de cotejar la información con la existente en sus los sistemas informáticos antes de continuar con la contratación y solicitar el resto de los

datos, ya que este contrato nuevo necesita autorización del anterior titular. Además de la documentación del nuevo titular, hay que aportar una copia del DNI del anterior titular y un documento de autorización firmado por ambos.

### *Acreditación de la identidad del contratante*

En los canales telemáticos y, con carácter general, los clientes ya registrados en una compañía de energía y que solicitan nuevos contratos se identifican con código de usuario y contraseña a través del área de Clientes de la web o, si no disponen de identificación, se les solicita el DNI y otro dato identificativo (normalmente el número de contrato o el número de cuenta bancaria). A los interesados en la contratación y no clientes de la compañía se les solicitan los datos personales, de contacto, bancarios y de punto de suministro (CUP –que identifica unívocamente un punto de suministro-) y la dirección del mismo.

A través de los Departamentos de Atención al Cliente (canal telefónico) para realizar la contratación de servicios se identifica al contratante ya cliente utilizando generalmente datos de nombre, DNI y dirección de punto de suministro y en el caso de no clientes se solicitan igualmente los datos personales, de contacto, bancarios y de punto y dirección de suministro.

Todas las compañías requieren documentos para formalizar la contratación, básicamente copia del DNI y copia de un recibo bancario (o fotografía en caso de pedidos realizados con aplicaciones móviles). En los cambios de titular, además, hay que aportar la copia del DNI del anterior titular y el documento de autorización. En aquellos casos en los que la situación del punto de suministro lo requiera, se solicita el boletín eléctrico o de gas correspondiente. Todos estos documentos se cotejan por personal de la compañía.

Las compañías remiten al interesado el documento de domiciliación bancaria (formulario SEPA) por el sistema que haya elegido (correo electrónico, postal…) que debe ser devuelto firmado.

Las compañías auditadas no permiten la contratación a interesados que no vayan a ser titulares del contrato, salvo autorizados.

Se utiliza el DNI del posible cliente en las consultas a los sistemas comunes de información crediticia.

### *Acreditación de la contratación a distancia*

Las compañías acreditan la contratación con la documentación aportada (copia del DNI, recibo bancario, formulario SEPA firmado, y en su caso, boletín energético y documentos de cambio de titular). Alguna entidad indica que en caso de que se sospeche que la documentación pueda haber sido manipulada, se solicita al cliente su presentación compulsada.

En los pedidos por canal telemático se registra la dirección IP.

Generalmente las solicitudes de contratación realizadas por canal telefónico nuevas o por cambio de comercializadora, se acreditan mediante la grabación de la conversación en el proceso de contratación, ya sea por la propia compañía o por terceros con contrato

de prestación de servicio, registrándose la fecha y hora de la grabación con fines de trazabilidad de la operación. La custodia de las grabaciones la realiza la entidad contratante. Alguna entidad no graba esta conversación, ya que considera que la contratación no es efectiva hasta que el cliente acepte el documento de contrato generado en la web.

En los casos de nuevos contratos con cambio de comercializadora, las compañías intercambian ficheros con la información de los clientes a portar con las empresas distribuidoras y deben cumplir lo estipulado en la normativa sectorial al respecto (Resolución de 20 de diciembre de 2016, de la Comisión Nacional de los Mercados de la Competencia por la que se aprueban los formatos de los ficheros de intercambio de información entre distribuidores y comercializadores de energía).

Algunas compañías utilizan un sistema de acreditación a través de un tercero de confianza que verifica y acredita que todos los contratos que se celebran son debidamente firmados por la persona que se identifica como titular.

También se emplean otros sistemas de acreditación consistentes en el envío de un correo electrónico al interesado con el contrato y las condiciones, que debe ser leído y contestado. Una vez recibida la contestación, se envía un SMS al móvil con información para poder proseguir la contratación a través de la web.

En casos de contratación telefónica algunas compañías disponen de un proceso en el cual se remite un mensaje por SMS con notificación certificada al teléfono móvil aportado por el interesado con datos de la contratación. Dicho mensaje debe ser aceptado y contestado por el futuro cliente para finalizar la contratación.

Todas las compañías remiten copia del contrato y las condiciones por correo postal.

### *Verificación de la identidad del cliente en procesos posteriores*

En el Área de Clientes de la web se identifican y autentican a través de código de usuario (en muchos casos el código de usuario es la dirección de correo electrónico) y contraseña.

En los Departamentos de Atención al Cliente (canal telefónico) de las diferentes compañías se suele identificar al cliente por nombre completo, DNI y un tercer dato (dirección del punto de suministro, fecha de nacimiento, últimos dígitos de la cuenta) según la operativa a realizar, aunque algunas entidades se realizan preguntas sobre datos del contrato (potencia contratada) con objeto de añadir seguridad en la identificación del cliente.

Algunas compañías disponen de otros canales para la atención al cliente. En los casos de redes sociales (Facebook, Twitter y WhatsApp) se les identifica con los datos de nombre completo, DNI y dirección del punto de suministro. También utilizan el correo electrónico para el Servicio de Atención al cliente y para ello en el primer contacto se suele pedir copia del DNI.

## *PROYECTOS INNOVADORES*

### *Firma manuscrita biométrica*

El producto de firma manuscrita biométrica permite capturar la firma manuscrita utili-

zando dispositivos especiales para ello (tabletas digitalizadoras) que capturan datos biométricos del firmante durante el proceso de la firma asociándolos al documento electrónico firmado.

Está implantado en prácticamente todas las entidades bancarias y en otros entornos donde los documentos en soporte electrónico tengan que garantizar la autenticidad, la integridad y no repudio. Tiene validez jurídica.

Los datos biométricos capturados durante el proceso de firma tienen que ver con la presión del lápiz, la velocidad y aceleración de la escritura, el grafo, el vuelo del lápiz y la grabación del proceso de firma. Tiene prácticamente un cien por cien de validez en la identificación única e inequívoca del firmante ante una verificación de la identidad por un calígrafo. Este tipo de firma no se puede reproducir ya que los datos biométricos son muy complejos e intrínsecos a cada persona y difícilmente controlables.

Como requisitos básicos para tener plena garantía legal hay que tener en cuenta además de la confirmación de autoría a través de los datos biométricos mencionados, el no repudio a través del almacenamiento de sello de tiempo, tipo de dispositivo, etc.

### *Reconocimiento facial biométrico*

El Reconocimiento facial biométrico es un procedimiento informático para identificar a una persona en una imagen digital (reconocimiento facial) analizando las características faciales extraídas de una imagen o un fotograma de un video generando un *patrón* o *huella facial* de tal manera que sirve para comparar. La información biométrica almacenada (*patrón)* permite reconstruir parcialmente la información biométrica original. Dicha reconstrucción puede tener, en ocasiones, la fidelidad suficiente para que otro sistema biométrico lo reconozca ya que es posible conseguir un retrato robot, por ejemplo. La fidelidad de la reconstrucción depende de la cantidad de información biométrica recogida.

Generalmente, las entidades que utilizan este procedimiento suelen incluir en sus propios sistemas de información el algoritmo que permite generar el *patrón,* siendo por tanto responsables de realizar el registro inicial de los datos de las personas**.**

En el proceso de registro, se solicita una fotografía o un video junto con una fotocopia del DNI para una verificación humana posterior. Con los datos biométricos extraídos de la imagen se genera el *patrón* que se almacena junto con la documentación anterior.

A través de la web o de la app de la entidad se captura el anverso y el reverso del DNI y un video con la imagen de la persona o una autofoto con una cámara digital o un teléfono móvil (*selfi*). Se compara ambas imágenes y se genera el *patrón* con un índice de fiabilidad que define la empresa, relacionados con el riesgo que asume la propia empresa. El patrón se almacena junto con el resto de los datos aportados por el interesado cifrados en los sistemas informáticos de la entidad (propios o contratados).

En caso de que se necesite verificar la identidad de la persona, se procede a realizar un nuevo procedimiento completo incluyendo copia del DNI e imagen del interesado generándose un nuevo *patrón* que se compara con el existente obteniendo un porcentaje de similitud.

### *Identificación de titulares y Análisis de riesgos on-line*

Con la entrada en vigor de la segunda directiva de pagos europea (*Payment Service Providers Directive* -PSD2-) en enero de 2018, que obliga a las entidades financieras a permitir el acceso de terceras empresas a sus plataformas digitales siempre y cuando cuenten con el consentimiento del cliente, han aparecido en el mercado diferentes soluciones que permiten la identificación de los titulares de la cuentas bancarias y la realización de análisis de riesgos en el mismo momento en el que se produce un contrato o una solicitud de financiación por medios telemáticos.

El acceso a los datos del cliente lo realiza el propio interesado introduciendo sus credenciales (código de usuario y contraseña) sin que las entidades implicadas conozcan esta información. Una vez se haya accedido, la entidad bancaria proporciona los datos establecidos (desde la identificación del titular -nombre, DNI, domicilio…- a movimientos de las cuentas, calificaciones de riesgo, saldos medios… incluyendo datos de sistemas comunes de información crediticia, en muchos casos) que permitirán a la compañía identificar al titular y realizar un *scoring* en su caso.

Como se ha visto en el funcionamiento del sector que utiliza este tipo de procedimientos se proporciona una gran cantidad de información a las entidades implicadas en el proceso, alguna de ellas ubicadas en la Unión Europea. *Al ser un tema muy específico y con un periodo corto de implantación, la Agencia Española de Protección de Datos no realiza ninguna valoración en este informe*.

### *Notificación electrónica certificada*

La notificación electrónica es una comunicación electrónica que acredita el contenido del texto, el emisor, el destinatario, la fecha y hora del envío y de la entrega. La comunicación se puede enviar utilizando el correo electrónico o bien como un mensaje SMS. Con la información de la notificación se genera un certificado que se asocia a los datos del destinatario.

Los documentos o textos de mensajes que se envían junto con el certificado obtenido se custodian en la entidad que proporciona el servicio de notificación electrónica y en muchos casos se utiliza un depósito notarial como medida adicional de seguridad.

Para la remisión de documentación se utiliza el correo electrónico y los documentos en formato “pdf”, generando un *hash* (resultado de aplicar un algoritmo criptográfico a una serie de datos que representa de forma univoca un concreto texto sin cifrar – documento original- y que no tiene función inversa) y se consigna la fecha y la hora custodiando el resultado (hash junto con fecha y hora). En muchos casos, es un proveedor externo (entidad de certificación) la encargada de certificar y custodiar la prueba electrónica (documento y su hash) de este modo el documento es inalterable.

El destinatario recibe un mail con un enlace para acceder a la documentación, en la que se ha incluido un identificador de la transacción que identifica unívocamente al documento y el receptor debe aceptar la notificación y acceder a los documentos para su descarga en cuyo caso se genera un *hash* con la información de la notificación volviéndose a consignar fecha y hora.

Tanto el emisor como los destinatarios reciben el certificado de la notificación efectuada.

### *Prueba acreditativa de los sucesos digitales*

Hay en el mercado entidades que ponen a disposición de las empresas prestaciones de servicios encaminadas a la obtención de prueba acreditativa de los sucesos digitales utilizados, entre otros, para acreditar contratos realizados por medios telemáticos sin presencia de ninguno de los actores.

El procedimiento es similar a los servicios de notificación electrónica certificada, aunque el proceso comienza con el envío de las condiciones del contrato al destinatario, el cual, si está de acuerdo, debe firmar, ya que, tal y como se le informa, tendrá carácter contractual. Con toda la documentación remitida, la firma del interesado y el proceso de intercambio con el destinatario se genera un *hash* que identifica unívocamente a este proceso y no permite su alteración. La entidad custodia toda la documentación junto con el *hash* y el certificado, el cual es además remitido al emisor y al receptor. Generalmente se custodia también en depósitos notariales constando una referencia del mismo.

# CONCLUSIONES Y RECOMENDACIONES

Hay que tener en cuenta que, entre los objetivos perseguidos en el Plan de Auditoría se encontraba el estudio de los procedimientos que las empresas auditadas han implantado, y en algunos casos estaban inmersos en la implantación, de los mecanismos para mecanismos para garantizar la nueva visión adoptada a raíz del Reglamento General de Protección de Datos. Por ello algunas de las deficiencias detectadas han sido ya subsanadas, no obstante, se detallan para conocimiento del sector implicado.

## *TRANSPARENCIA E INFORMACIÓN*

Todas las empresas investigadas disponen en sus portales webs de información al usuario adaptadas a lo estipulado en los artículos 13 y 14 del Reglamento y al artículo 11 de la LOPDPGDD en su Política de Privacidad.

- En los Grupos empresariales hay compañías que incluyen información sobre todas las entidades del grupo con los datos del responsable y de contacto de cada una de ellas, sin embargo, algunas de las empresas solo incluyen información de un responsable.
- Las entidades incluyen los datos de contacto del Delegado de Protección de Datos. No obstante, se ha detectado en uno de los operadores de telecomunicaciones no se aporta la dirección de contacto del DPD, sino que únicamente se informa del domicilio social de la compañía. También se ha detectado en algún caso que al acceder por el nombre comercial no figura información sobre el DPD de la compañía, siendo necesario dirigirse a la página del responsable de la marca comercial para encontrar dicha información.
- En las compañías que realizan contratación electrónica se informa sobre:
    - Tipo de datos objeto de tratamiento: datos sobre el contrato, datos de tráfico, datos de visitas web (direcciones IP, páginas consultadas, dominios accedidos…), datos de localización, datos de acceso público, datos de sistemas comunes de información crediticia. En algunos casos se incluye datos aportados en las redes sociales en su parte pública, habilitada para poder recibir comentarios de los clientes.
    - Base Jurídica para los tratamientos:
        - Basadas en el cumplimiento de una relación contractual (básicamente de los datos relativos al contrato establecido entre las partes para la utilización de los servicios)
        - Basadas en el interés legítimo: Comprobar la solvencia del cliente mediante el acceso a sistemas de información crediticia. Remisión de comunicaciones comerciales teniendo en cuenta los productos contratados. En algunas compañías la elaboración de perfiles comerciales se ha definido como tratamientos de interés legítimo.
        - Basadas en el consentimiento: campañas comerciales que requieren

elaboración de perfiles, datos de tráfico y geolocalización, comunicación de datos a empresas participadas.

  - Acciones comerciales en base al interés legítimo una vez finalizada la relación contractual.

- Las entidades proporcionan información de las posibles comunicaciones de datos a otras entidades (empresas del Grupo, filiales, proveedores de servicios…) y generalmente informan en la propia web de la relación de empresas a las que se comunican los datos o incluyen el canal para poder acceder a esta información.
- Respecto de la conservación de datos se informa de que los plazos de conservación se mantendrán mientras dure la relación comercial (prestación de los servicios contratados) y serán bloqueados conforme a lo dispuesto en la normativa de protección de datos. No obstante, con carácter general las empresas investigadas no proceden a bloquear o suprimir los datos, salvo solicitud expresa del usuario y solo algunas compañías informan de diferentes plazos de conservación, según la tipología de los datos: datos de tráfico, datos de cliente y productos, datos de consumo, facturación, datos de web y localización.
- Muchas compañías no informan del periodo de conservación de los datos facilitados por el interesado para una contratación que finalmente no se ha hecho efectiva.
- En las políticas de privacidad se informa de la existencia de transferencias internacionales de datos a empresas que participan en el marco del Escudo de Privacidad entre la Unión Europea-Estados Unidos y Suiza. En la propia web o en un enlace se muestra un listado de las empresas encargadas del tratamiento situadas fuera de la Unión Europea indicando en qué país se encuentra. No obstante, algunas compañías solo informan de la posible transferencia y de la autorización de la Agencia para habilitarla.
- Se informa sobre el acceso a datos de geolocalización para las aplicaciones de móviles y solo en algunos casos se indica al usuario el procedimiento para eliminar esta opción en su terminal móvil.
- También se informa de los datos que se recogen de forma automática, direcciones IP, fecha y hora, historial de visitas a la web y algunas compañías informan sobre el acceso a datos recabados de otras fuentes, incluido historial de crédito para prevenir el fraude.
- Se informa sobre la anonimización y agregación de datos para su utilización posterior con diversos fines: identificar comportamientos, patrones y tendencias, siempre con carácter general y no individual con objeto de tratamientos automatizados que utilizan tecnologías de procesamiento y almacenamiento de datos, conocidas como Big Data.
- Los canales telefónicos utilizan un argumentario para informar de la política de privacidad en modo reducido, que suele contener los aspectos básicos de responsable, finalidad, destinatarios y procedimiento para ejercitar los derechos previstos en la normativa. No en todos los casos se indica cómo acceder a más información que la proporcionada.

- En todos los casos figuran las referencias al ejercicio de los derechos que asisten al interesado (acceso, rectificación, cancelación, oposición, limitación del tratamiento y portabilidad) indicando el procedimiento para ejercerlos y la dirección postal. En muchos casos se incluye también una dirección de correo electrónico. Y se suele informar del derecho a presentar reclamaciones ante la Agencia Española de Protección de Datos.

***Recomendaciones***

- En los medios telemáticos donde no es posible facilitar una información completa al usuario se recomienda adoptar un modelo de información por capas o niveles de tal manera que se presente al interesado una información básica reducida y una referencia al procedimiento sencillo para obtener información adicional.
- Es obligatorio incluir los datos de contacto del Delegado de Protección de Datos en los casos en que se exige su designación.
- Los datos personales se recopilarán para fines específicos, explícitos y legítimos y no se procesarán de manera incompatible con aquellos fines distintos de los establecidos originalmente.
- Es de obligado cumplimiento informar de la base jurídica de cada uno de los tratamientos y de su finalidad. Se considera una buena práctica informar sobre las categorías de datos que se someten a cada tratamiento.
- Las compañías pueden basar la remisión de publicidad por correo electrónico o similar a sus clientes en la regla de ponderación de intereses, recogida en el artículo 6.1.f) del Reglamento Europeo, siempre que haya una relación comercial o contractual previa, el cliente no se haya opuesto y los productos o servicios ofertados sean similares a los contratados. En cualquier caso, están obligadas a ofrecer a los destinatarios la posibilidad de oponerse al tratamiento de sus datos con fines promocionales mediante un procedimiento sencillo y gratuito.
- Es de carácter obligatorio informar sobre las decisiones automatizadas incluida la elaboración de perfiles y en aquellos casos en que las decisiones produzcan efectos jurídicos o afecten significativamente al interesado habrá que solicitar su consentimiento, salvo que haya otra base jurídica que lo ampare.
- El scoring es un perfilado del individuo orientado a tomar una decisión sobre cómo se le va a ofrecer el servicio. Es de carácter obligatorio informar. Las empresas deben analizar las bases jurídicas para la realización del scoring y estudiar la proporcionalidad y la necesidad de este tratamiento.
- Es necesario informar sobre la posible utilización de datos obtenidos de otras fuentes distintas del interesado, aunque el tratamiento sea necesario para la satisfacción de los intereses legítimos del responsable.
- Hay que informar al interesado de los destinatarios de los datos incluyendo las empresas que forman parte de un Grupo empresarial.
- Se debe informar de la posible transferencia de datos personales a un tercer país

indicando una referencia a las garantías establecidas para su realización.

Se considera una buena práctica que las empresas dispongan de un lugar donde el interesado pueda consultar las empresas a las que pueden ser cedidos sus datos.

- El Reglamento utiliza el principio de "minimización de datos" por el cual los datos deben ser adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados. En el mismo sentido el artículo 25 del RGPD insta a los responsables que implantar estrategias que incluyan los mecanismos de minimización por defecto desde el inicio del diseño de los tratamientos.
- El Reglamento obliga a informar sobre el periodo de conservación de los datos recabados o en su defecto, de los criterios utilizados para determinar el plazo. En este sentido también es obligatorio suprimir los datos recabados cuando finalmente no se haya establecido una relación contractual.
- Se debe de informar correctamente de los medios de ejercitar los derechos y la dirección habilitada para ello.

## *TRATAMIENTOS BASADOS EN EL CONSENTIMIENTO*

- Los operadores de telecomunicaciones suelen realizar campañas publicitarias para captar clientes y, en muchos casos utilizan diversas fuentes y distintos medios, aunque el más frecuente son las campañas telefónicas utilizando bases de datos adquiridas a proveedores externos, el cual garantiza contractualmente que se cuenta con el consentimiento del interesado. No obstante, se ha detectado que las empresas contratantes, ante una reclamación, desconocen si se puede probar que el afectado ha dado su consentimiento
- Los comercializadores de energía también realizan campañas de captación de clientes y, en algunos casos, enriquecen los datos extraídos de sus sistemas con otras fuentes de información, entre ellas, la información que figura en la Base de Datos de Consumidores y Puntos de Suministro (Base de Datos creada de acuerdo con lo establecido en el artículo 7 del Real Decreto 1435/2002, de 27 de diciembre) y proveedores externos de repertorios telefónicos.

### *Recomendaciones*

- El responsable del tratamiento se asegurará de que el consentimiento se haya obtenido: libremente, especifico, informado e inequívoco.

  Se debe conservar cuándo y cómo se obtuvo el consentimiento y se garantizará que el interesado pueda retirar su consentimiento en cualquier momento con un procedimiento sencillo.
- En las acciones comerciales a través de comunicaciones electrónicas que basan la licitud de los tratamientos en el consentimiento del usuario, las compañías responsables de los datos deben asegurarse de tener el consentimiento expreso para el tratamiento con las finalidades que constan en la información al interesado y están obligadas a ofrecer a los destinatarios un sistema para la revocación del consentimiento prestado.

No obstante, para clientes y antiguos clientes a los que se remite comunicaciones electrónicas con información comercial de productos similares a los contratados es obligatorio que figure el procedimiento para oponerse al tratamiento de sus datos con fines comerciales en cada comunicación.

- En caso de obtener datos de potenciales clientes de bases de datos elaboradas por terceros cuya base es el consentimiento, la empresa debe ser diligente para asegurarse el consentimiento prestado por el destinatario de la comunicación comercial. Por ello, se aconseja a las empresas que adquieren estas bases de datos la realización de comprobaciones aleatorias para acreditar que se cuenta con el efectivo consentimiento expreso del destinatario de la publicidad.
- Para la personalización de publicidad basada en decisiones automatizadas incluida la elaboración de perfiles cuando tengan consecuencias jurídicas o efectos equivalentes, es necesario que el interesado preste su consentimiento explícito y la empresa debe proporcionar un mecanismo sencillo para retirarlo.
- En la utilización de cookies o tecnología para poder obtener información de los terminales de los usuarios debe obtenerse su consentimiento informado. La información debe ser clara y precisa y el consentimiento debe ser fácilmente revocable. La Agencia Española de Protección de Datos tiene publicada en su web www.aepd.es una Guía sobre el uso de las cookies https://www.aepd.es/sites/default/files/2019-12/guia-cookies.pdf).

## *ACREDITACIÓN DE LA IDENTIDAD DEL INTERESADO*

- La identificación del contratante se realiza, en todos los casos, con posterioridad a la contratación de un servicio.

  Los contratos telemáticos requieren firma de contrato y copia de documentación (DNI y bancaria generalmente) aunque se ha detectado que no siempre esta documentación consta en las compañías.
- Se ha detectado por parte de todas las compañías una creciente inquietud por garantizar la identidad del contratante y por ello se están estudiando e implantando diferentes soluciones con objeto de evitar en lo posible la suplantación de identidad, entre ellas, reconocimiento facial y la firma manuscrita electrónica.

### *Recomendaciones*

- Es necesario extremar las garantías de identificación del contratante con anterioridad a la ejecución del contrato.
- Es importante que se utilicen sistemas con garantías adicionales del estilo de lo definido en el en la normativa del PSD2: autenticación reforzada del cliente (basada en la utilización de dos o más elementos categorizados como conocimiento -algo que solo conoce el usuario-, posesión -algo que solo posee el usuario– e inherencia -algo que es el usuario- que son independientes de tal forma que la vulneración de uno no compromete la fiabilidad de los demás y concebidos de manera que proteja la confidencialidad de los datos de autenticación.

- Puede interpretarse que de acuerdo con el art. 4 del RGPD el concepto de dato biométrico incluiría la identificación y la verificación/autenticación (verificación uno contra uno, verificación uno contra varios). Sin embargo y, con carácter general, los datos biométricos únicamente tendrán la consideración de categoría especial de datos en los supuestos en que se sometan a tratamiento técnico dirigido a la identificación biometría (uno a varios) y no en el caso de verificación/autenticación biométrica (uno a uno).

  No obstante, esta Agencia considera que se trata de una cuestión compleja, sometida a interpretación, respecto de la cual no se pueden extraer conclusiones generales, debiendo atenderse al caso concreto según los datos tratados, las técnicas empleadas para su tratamiento y la consiguiente injerencia en el derecho a la protección de datos, debiendo, en tanto en cuanto no se pronuncia al respecto el Comité Europeo de Protección de Datos o los órganos jurisdiccionales, adoptarse, en caso de duda, la interpretación más favorable para la protección de los derechos de los afectados.

  En cualquier caso, es necesario hacer un análisis de la proporcionalidad y necesidad del tratamiento, en particular, una evaluación del riesgo. En la lista de tipos de tratamiento de datos que requieren evaluación de impacto relativa a la protección de datos (art.35.4) publicada en la Agencia (https://www.aepd.es/sites/default/files/2019-09/listas-dpia-es-35-4.pdf), se ha establecido como uno de los criterios para que, en conjunto con otros, se determine la obligación a la evaluación de impacto l*os tratamientos que impliquen el uso de datos biométricos con el propósito de identificar de manera única a una persona física*. También se incluyen como criterios el que los *tratamientos que impliquen el uso de datos a gran escala y los tratamientos que impliquen la utilización de nuevas tecnologías o un uso innovador de tecnologías consolidadas, incluyendo la utilización de tecnologías a una nueva escala, con un nuevo objetivo o combinadas con otras, de forma que suponga nuevas formas de recogida y utilización de datos con riesgo para los derechos y libertades de las personas.*

## *ACREDITACIÓN DE LA CONTRATACIÓN A DISTANCIA*

- Las compañías acreditan la contratación de un servicio por medios telemáticos con el propio procedimiento de registro de la cuenta de cliente o solicitud del contrato y asociado al mismo, la fecha, hora y la dirección IP.
- Adicionalmente se custodia la documentación aportada en su caso (albarán de entrega de productos, contratos firmados, copia de recibos bancarios…) así como los correos o mensajes SMS intercambiados entre los contratantes.

### *Recomendaciones*

- Es recomendable que las empresas utilicen sistemas que permitan la acreditación de los contratos efectuados telemáticamente con obtención de prueba de los sucesos digitales, de tal manera que la documentación contractual se almacene aplicando una función criptográfica que detecte la posible modificación posterior, asegurando con ello la integridad de los documentos.

- En los contratos remitidos a través de correos electrónicos o los textos de los mensajes SMS es necesario poder acreditar su recepción por parte del interesado. Por ello es recomendable la utilización de técnicas de notificación automatizada certificada.
- La Ley 59/2003, de 19 de diciembre, de firma electrónica establece que "*la firma electrónica avanzada es la firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede utilizar, con un alto nivel de confianza, bajo su exclusivo control*" y por ello le atribuye el mismo valor jurídico que la firma manuscrita. Sería recomendable la potenciación del uso de certificados electrónicos como medida de identificación de las personas.
- Otros sistemas de acreditación menos robustos, que utilizan el correo electrónico para la remisión de documentación y mensajes SMS para continuar el proceso de contratación o adquisición, deben de asegurarse que estos datos han sido aportados por el propio interesado y utilizar otras medidas adicionales para garantizar su identidad y deseo de contratar.

## *ACREDITACIÓN DE LA IDENTIDAD DEL INTERESADO EN PROCESOS POSTERIORES*

- Para la identificación y autenticación de los usuarios se utiliza un sistema basado en código de usuario y contraseña. Generalmente este código de usuario es la dirección de correo electrónico, el DNI o el número de línea telefónica en el caso de los operadores de telecomunicación.

  Se ha detectado que las empresas no obligan al cambio de contraseña a sus usuarios periódicamente.
- En los Servicios de Atención al Cliente en canal telefónico generalmente la identificación del cliente se realiza verificando los datos de DNI, Nombre y Apellidos y un tercer dato (dirección postal, datos bancarios…).

  Alguna entidad proporciona una contraseña adicional a solicitud del usuario para el contacto telefónico.

### *Recomendaciones*

- Es recomendable que las empresas utilicen sistemas de autenticación de doble factor dependiendo de la operación que vaya a realizar.

  Sería recomendable que en el acceso de los clientes a las webs para realizar nuevas compras o contrataciones se incluya un tercer dato agregando con ello una mayor capa de seguridad.
- En el canal telefónico también añade una capa de seguridad la aportación de una contraseña además de los datos identificativos y adicionales solicitados al cliente.
- Las contraseñas deben ser robustas para asegurar la autenticación del cliente.

- Se considera una buena práctica que las empresas recuerden a sus clientes la necesidad de cambiar regularmente las contraseñas.

## *CONSERVACIÓN DE DATOS*

- En el sector de comercializadoras de energía se informa de que los datos se mantienen mientras dure la relación contractual y exista una obligación legal, en cuyo caso se mantendrán bloqueados y quedaran a disposición exclusiva de los Organismos competentes.

  No obstante, se ha detectado que algunas entidades, una vez finalizada la relación contractual, conservan los datos durante 5 años una vez vencidas las deudas existentes y las obligaciones de pago. Solo una entidad utiliza un periodo de conservación entre 5 y 15 años dependiendo de la fecha de comienzo de la relación contractual.

  Respecto a la información relativa al envío de comunicaciones comerciales, algunas empresas mantienen indefinidamente los datos de sus exclientes con esta finalidad siempre y cuando no hayan ejercido su derecho de supresión.

  Las empresas que utilizan grabación con proveedores externos suelen tener por contrato una periodicidad programada para la cancelación de las grabaciones por parte del prestador del servicio.

  En los casos de solicitudes de nuevos clientes que por cualquier causa no finalicen con un contrato, las entidades suelen anular la solicitud/pedido y borrar los datos aportados. Si una grabación se interrumpe y no se puede contactar con el cliente para proseguir el proceso, los datos aportados hasta el momento son eliminados.

- En el sector de operadores de telecomunicaciones, los datos de los potenciales clientes que han otorgado su consentimiento para ser contactados no se suprimen. Sólo algunas compañías tienen implantados procedimientos para que periódicamente esta información se borre (en una de las entidades investigadas el periodo es de tres meses) siempre que no ejerciten antes el derecho de supresión u oposición.

  Con carácter general, los datos de los clientes no se cancelan, salvo petición de los mismos, quedando en los ficheros en situación de baja.

  Cuando un cliente solicita la cancelación de sus datos se bloquean si no hay incidencias en la facturación.

  Los datos de tráfico y localización se conservan durante un año.

  Las empresas que utilizan grabación con proveedores externos suelen tener por contrato una periodicidad programada para la cancelación de las grabaciones.

  Algunas compañías tienen procedimientos para borrar definitivamente los datos de los clientes que han solicitado la supresión después de transcurrir un periodo razonable para poder solventar las incidencias que se puedan producir (una de las entidades investigadas procede al borrado a los 90 días de la solicitud si no se ha producido ninguna incidencia).

***Recomendaciones***

- Todo tratamiento de datos personales debe limitarse a un mínimo estricto su plazo de conservación. Para garantizar que los datos personales no se conservan más tiempo del necesario se deben establecer plazos para su supresión o revisión periódica.
- Los datos recabados con objeto de realizar una contratación y que finalmente no se ha establecido una relación comercial deben ser suprimidos salvo que se basen en otro fundamento jurídico.
- Los datos de los clientes deberán ser suprimidos cuando haya finalizado los servicios para los que fueron recabados y haya transcurrido el tiempo necesario para cumplir con las responsabilidades derivadas del tratamiento.
- Es recomendable que los datos de los potenciales clientes que han otorgado su consentimiento para ser contactados se supriman pasado un periodo de tiempo razonable, o en su defecto, se implanten procedimientos de revisión periódica.

## *EJERCICIO DE LOS DERECHOS*

- Las compañías aportan una dirección postal y una dirección de correo electrónico para ejercer los derechos previstos en la normativa y también de forma presencial en sus tiendas u oficinas comerciales. En las grandes compañías hay establecido además procedimientos para el ejercicio de los derechos por el canal telefónico directamente en el Departamento de Atención al Cliente o a través de las redes sociales.
- En los casos de venta telefónica se informa del procedimiento para ejercer los derechos previstos cuando se está contactando con el cliente para la venta, y se indica la dirección de correo postal o el número del servicio telefónico al que debe dirigirse el usuario.
- En algunos Grupos empresariales el procedimiento para ejercitar los derechos de los interesados se dirige al Grupo y por tanto es el propio consumidor quién debe especificar si lo solicita para una de las empresas o para todas ellas. El derecho se realiza sobre la información de la solicitud y por desconocimiento se puede dar casos que no correspondan con los deseos del ciudadano.
- El ejercicio del derecho de supresión se realiza bloqueando los datos. Con carácter general, cuando un cliente solicita la supresión de sus datos las compañías adoptan inicialmente medidas para evitar que reciba comunicaciones comerciales y posteriormente proceden a bloquear los datos manteniendo información sobre facturación para posibles incidencias.
- La identificación del solicitante se acredita con la copia del DNI. No obstante, algunas entidades han implantado otras formas de acreditación: solicitud vía web utilizando código de usuario y contraseña para clientes ya registrados, nombre y apellidos junto con el número de DNI y otro dato adicional en caso de solicitud telefónica.
- En los casos de negativa a recibir comunicaciones comerciales algunas compañías han habilitado procedimientos que permiten revocar el consentimiento para tres tipos de comunicaciones comerciales: promociones y servicios de la propia compañía,

ofertas de empresas del Grupo y servicios de terceras empresas en los sectores informados en la contratación.

- Algunas empresas van a centralizar las respuestas a las solicitudes de los derechos a través de la oficina del Delegado de Protección de Datos.
- La normativa de protección de datos ha incluido el derecho de portabilidad. En los operadores de telecomunicaciones la portabilidad de la línea telefónica estaba ya establecida en la legislación propia de las telecomunicaciones de tal manera que se permite al cliente mantener la línea telefónica cambiando de operador. El derecho de portabilidad amplia los datos a portar, ya que establece que un responsable del tratamiento transmitirá a otro responsable la información que disponga en un formato estructurado. A este respecto, algunos de los operadores de telecomunicaciones están diseñando conjuntamente un procedimiento para atender el derecho de portabilidad de sus clientes permitiendo el intercambio de información entre ellos y otros sectores de forma rápida y efectiva.
- Los clientes tienen que aceptar expresamente su inclusión en Guías y generalmente en las propias webs de las operadoras de telecomunicaciones se puede gestionar los consentimientos al respecto. También las empresas han habilitado otros sistemas (correo electrónico) para solicitar o denegar la inclusión en repertorios telefónicos.

***Recomendaciones***

- El Reglamento Europeo y la LOPDGDD introducen nuevos derechos para los interesados, entre ellos el derecho a la limitación del tratamiento, por lo que el responsable tendrá que mantener un procedimiento que permita el ejercicio de este derecho, limitando los tratamientos a lo estipulado en la normativa sin borrar los datos, aunque se ejerciten otros derechos.
- En los procedimientos establecidos para el ejercicio de los derechos es necesario garantizar la comprobación de la identificación inequívoca del interesado.
- Los Grupos empresariales deben tener un procedimiento de fácil entendimiento para el usuario que le permita ejercer sus derechos ante una de las empresas o para todo el Grupo.

## *ENCARGADO DE TRATAMIENTO*

- Las compañías tienen suscrito contratos de prestación de servicios con empresas externas para la realización de algunas actividades como encargados del tratamiento. En los casos de grupos de empresas suelen tener también suscrito un contrato de encargado del tratamiento con aquellas empresas del Grupo que realizan funciones para diversas empresas del Grupo.

***Recomendaciones***

- La LOPDGDD establece que los contratos de encargado del tratamiento suscritos con anterioridad al 25 de mayo de 2018, al amparo de lo dispuesto en el artículo 12 de la antigua LOPD, mantendrán su vigencia hasta la fecha de vencimiento señalada

en los mismos y en caso de haberse pactado de forma indefinida, hasta el 25 de mayo de 2022. No obstante, y para estos contratos, se considera una buena práctica incluir un anexo en el que se especifique los nuevos aspectos incorporados en la normativa.

- La normativa también establece que tanto los responsables como los encargados del tratamiento determinaran las medidas técnicas organizativas apropiadas que deben aplicar teniendo en cuenta, entre otros aspectos, la posible usurpación de identidad en los tratamientos y cuando los tratamientos impliquen un gran números de afectados o conlleve a la recogida de una gran cantidad de datos personales: Es una exigencia legal que en los contratos se especifiquen las medidas de seguridad que debe de disponer el encargado según el nivel de riesgo del tratamiento objeto del contrato y del procedimiento para la notificación de brechas de seguridad.

# ANEXO I: Marco jurídico de los tratamientos de datos

## NORMATIVA GENERAL

- Reglamento UE 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento Europeo de Protección de Datos).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales.
- Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y Comercio Electrónico.
- Ley 7/1998, de 13 de abril, sobre condiciones generales de la contratación.
- Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias.
- Ley 3/2014, de 27 de marzo, por la que se modifica el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias, aprobado por el Real Decreto Legislativo 1/2007.

## NORMATIVA ESPECIFICA

### Operadores de telecomunicación

- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.
- Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.
- Real Decreto 424/2005, de 15 de abril, por el que se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios.
- Real Decreto 899/2009, de 22 de mayo, por el que se aprueba la carta de derechos del usuario de los servicios de comunicaciones electrónicas.
- Circular 1/2008, de 19 de junio, de la Comisión del Mercado de las Telecomunicaciones, sobre conservación y migración de numeración telefónica.
- Circular 1/2009 de la Comisión del Mercado de las Telecomunicaciones, por la que se introduce el consentimiento verbal con verificación por tercero en la contratación de servicios mayoristas regulados de comunicaciones fijas, así como las solicitudes de conservación de numeración (publicada el 25 de julio de 2017 y consolida las modificaciones de la circular 1/2012).

### Comercializadores de energía

- Ley 24/2013, de 26 de diciembre, del Sector Eléctrico.
- La Ley 34/1998, de 7 de octubre, del Sector de Hidrocarburos Real Decreto 1434/2002, de 27 de diciembre, por el que se regulan las actividades de transporte, distribución, comercialización, suministro y procedimientos de autorización de instalaciones de gas natural.
- Real Decreto 1011/2009, de 19 de junio, por el que se regula la Oficina de Cambio de Suministrador.
- Real Decreto 984/2015, de 30 de octubre, por el que se regula el mercado organizado de gas y el acceso de terceros a las instalaciones del sistema de gas natural.
- Real Decreto 335/2018 de 25 de mayo, por lo que se modifican diversos reales decretos que regulan el sector del gas natural modifica, entre otros, el Real Decreto 1434/2002, de 27 de diciembre y el Real Decreto 984/2015, de 30 de octubre.

Otras referencias

Informes del Gabinete jurídico de la Agencia publicados en la web:

https://www.aepd.es/es/documento/2020-0036.pdf

https://www.aepd.es/es/documento/2019-0031.pdf

Dictámenes del Grupo de trabajo del articulo 29 sobre evolución de las tecnologías:

https://www.aepd.es/sites/default/files/2019-12/wp193_es.pdf

# RECOMENDACIONES EN LA CONTRATACIÓN A DISTANCIA DE SERVICIOS DE TELECOMUNICACIONES Y ENERGÍA

agencia española protección datos

**Asegúrate de acceder a la página web de la empresa con la que deseas contratar el servicio.**

Para ello, comprueba que está identificada con los datos del responsable, su domicilio social y un procedimiento sencillo y rápido para contactar. Esta información debe estar disponible en la propia web (aviso legal/ política de privacidad) en un lenguaje claro y conciso.

**Infórmate sobre los criterios que tiene la compañía para la conservación de tus datos una vez finalizada la relación contractual.**

**Presta atención a la política de privacidad.**

Si utilizas el canal telefónico asegúrate de que te facilitan la información básica y una referencia a la forma de obtener información adicional.

**Infórmate sobre el procedimiento para ejercer tus derechos.**

La nueva normativa ha incluido el **derecho de limitación del tratamiento** que te permite oponerte a la supresión de los datos aportados, pero inhabilita a la empresa su utilización. Y el **derecho de portabilidad,** que obliga a que los datos recabados sean remitidos a una tercera empresa cuando sea técnicamente posible.

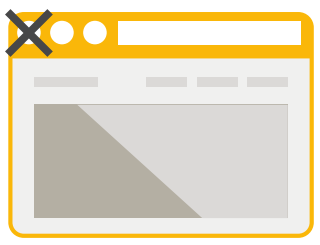
**Infórmate sobre si tus datos van a ser comunicados a terceras empresas.**

**Utiliza contraseñas seguras**

basadas en combinaciones de números, letras y caracteres especiales. Es muy útil para recordar las contraseñas que se basen en información combinada que solo conoces tú, sin usar nombres, fechas de cumpleaños, ni otra información similar fácil de averiguar. Es muy importante cambiar las contraseñas cada cierto tiempo.

**Infórmate del uso que van a hacer de tus datos.**

Deben facilitarte información sobre la base legal que asiste a la compañía para utilizar tus datos personales.



**Cierra la sesión al finalizar el proceso que estás realizando tanto en la web como en las aplicaciones móviles.**

**Recuerda que para recibir comunicaciones comerciales debe existir una relación comercial vigente y que los productos ofertados sean similares a los contratados.**

Asegúrate de que existe un procedimiento sencillo y gratuito para que puedas oponerte a su recepción. En otros casos, tienen que solicitarte tu consentimiento mediante casillas sin premarcar. Ten presente que existen sistemas de exclusión publicitaria donde puedes manifestar tu deseo de que tus datos no sean tratados para enviarte comunicaciones comerciales.

**En dispositivos móviles utiliza medidas de seguridad adicionales.**

Puedes establecer un bloqueo de tiempo y una contraseña de acceso. Muchos terminales disponen de autenticación con huella o reconocimiento facial que puedes habilitar.

**Recuerda que la Agencia Española de Protección de Datos es el organismo competente para las reclamaciones en materia de protección de datos**

**#ProtegeTusDatos**