# NORMATIVA DE USUARIOS

## 1. INTRODUCCIÓN

El artículo 5.1.f del Reglamento General de Protección de Datos (RGPD) determina la necesidad de establecer garantías de seguridad adecuadas contra el tratamiento no autorizado o ilícito, contra la pérdida de los datos personales, la destrucción o el daño accidental. Esto implica el establecimiento de medidas técnicas y organizativas encaminadas a asegurar la integridad y confidencialidad de los datos personales y la posibilidad (artículo 5.2) de demostrar que estas medidas se han llevado a la práctica (responsabilidad proactiva).

El RGPD señala unos principios básicos que todo tratamiento de datos debe cumplir entre los que se encuentra la exigencia de que éstos sean tratados garantizándose una seguridad apropiada de dichos datos, "incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas". (artículo 5.1 f)

A tenor del tipo de tratamiento, a continuación se detallan las medidas mínimas de seguridad mínimas que debería tener conocer y respetar.

## 2. GLOSARIO DE TÉRMINOS DE PROTECCIÓN DE DATOS

**Dato de carácter personal:** Toda información sobre una persona física identificada o identificable ("el interesado"); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular, mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona (Definición del Reglamento Europeo de Protección de Datos). Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables (Definición de la Ley Orgánica de Protección de Datos).

**Datos genéticos:** Datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de una persona, obtenidos en particular del análisis de una muestra biológica de tal persona (Definición del Reglamento Europeo de Protección de Datos).

**Datos biométricos:** Datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos (Definición del Reglamento Europeo de Protección de Datos).

**Datos relativos a la salud:** Datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud (Definición del Reglamento Europeo de Protección de Datos).

Informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo. En particular, se consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad y su información genética (Definición del Reglamento de desarrollo de la Ley Orgánica de Protección de Datos).

**Tratamiento de datos:** Cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción (Definición del Reglamento Europeo de Protección de Datos).

**Responsable del tratamiento o responsable:** La persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros (Definición del Reglamento Europeo de Protección de Datos).

Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento (Definición de la Ley Orgánica de Protección de Datos).

**Encargado del tratamiento:** La persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable (Definición del Reglamento Europeo de Protección de Datos).

**Consentimiento:** Toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen (Definición del Reglamento Europeo de Protección de Datos). Toda manifestación de voluntad, libre inequívoca, específica e informada mediante la que el interesado consiente el tratamiento de sus datos personales que le conciernen (Definición de la Ley Orgánica de Protección de Datos).

**Afectado o interesado:** Persona física titular de los datos que sean objeto del tratamiento (Definición de la Ley Orgánica de Protección de Datos).

**Cesión o comunicación de datos:** Toda revelación de datos realizada a una persona distinta del interesado (Definición de la Ley Orgánica de Protección de Datos).

**Violación de seguridad de datos personales:** Toda violación de seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizado a dichos datos (Definición del Reglamento Europeo de Protección de Datos).

**Privacidad por diseño:** Adopción de medidas técnicas y organizativas cuya finalidad es aplicar de forma efectiva los principios de protección de datos e integrar las garantías necesarias en el tratamiento de los datos (Reglamento Europeo de Protección de Datos).

**Privacidad por defecto:** Adopción de medidas técnicas y organizativas cuya finalidad es garantizar que por defecto sólo se traten aquellos datos que sean necesarios para los fines del tratamiento (Reglamento Europeo de Protección de Datos).

**Evaluación de impacto relativa a la protección de datos:** Análisis de carácter previo de aquellos tratamientos de datos que puedan suponer un alto riesgo para los derechos y libertades de las personas (Reglamento Europeo de Protección de Datos).

**Elaboración de perfiles:** Toda forma de tratamiento automatizado de datos personales consistente en utilizar los datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona (Definición del Reglamento Europeo de Protección de Datos).

**Seudonimización:** El tratamiento de datos personales de tal manera que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable.

## 3. MEDIDAS ORGANIZATIVAS Y TÉCNICAS

El personal que, para el correcto desarrollo de su labor, tiene autorizado acceso a datos personales, tiene el deber de tener conocimiento de las medidas implantadas por la empresa para el correcto tratamiento de los datos.

### MEDIDAS ORGANIZATIVAS

Todo el personal con acceso a los datos personales deberá tener conocimiento de sus obligaciones con relación a los tratamientos de datos personales y serán informados acerca de dichas obligaciones. La información mínima que será conocida por todo el personal será la siguiente:

**DEBER DE CONFIDENCIALIDAD Y SECRETO**

- Se deberá evitar el acceso de personas no autorizadas a los datos personales, a tal fin se evitará: dejar los

datos personales expuestos a terceros (pantallas electrónicas desatendidas, documentos en papel en zonas de acceso público, soportes con datos personales, etc.), esta consideración incluye las pantallas que se utili-cen para la visualización de imágenes del sistema de videovigilancia. Cuando se ausente del puesto de traba-jo, se procederá al bloqueo de la pantalla o al cierre de la sesión.
- Los documentos en papel y soportes electrónicos se almacenarán en lugar seguro (armarios o estancias de acceso restringido) durante las 24 horas del día.
- No se desecharán documentos o soportes electrónicos (cd, pen drives, discos duros, etc.) con datos persona-les sin garantizar su destrucción.
- No se comunicarán datos personales o cualquier información personal a terceros, se prestará atención espe-cial en no divulgar datos personales protegidos durante las consultas telefónicas, correos electrónicos, etc.
- El deber de secreto y confidencialidad persiste incluso cuando finalice la relación laboral del trabajador con la empresa.
- Se deberá guardar el necesario secreto respecto a cualquier tipo de información de carácter personal conoci-da en función del trabajo desarrollado, incluso una vez concluida la relación laboral con la organización.

**DERECHOS DE LOS TITULARES DE LOS DATOS**

- Siempre se debe **solicitar la firma del interesado**, afirmando que ha sido informado y que autoriza de for-ma expresa el tratamiento de datos. Deberá especificar qué datos se recogen, para qué fin y si se comparte con algún encargado de tratamiento.
- La información a los interesados, tanto respecto a las condiciones de los tratamientos que les afecten como en las respuestas a los ejercicios de derechos, deberá proporcionarse de forma concisa, transparente, inteli-gible y de fácil acceso, con un lenguaje claro y sencillo.
- En el caso de que los datos hayan sido facilitados por el propio interesado, mediante una llamada de teléfono, la entrega de una tarjeta o cualquier otro medio similar, sin que se le haya podido informar correctamente, se deberá preceder a informarle con posterioridad, dándole opción a negarse a la incorporación de los mismos al fichero o al tratamiento de los mismos. En estos casos, cuando la persona se persone en la Empresa, se le deberá solicitar la firma. Otra forma, sería el envío de una carta o correo electrónico, donde se incluirá dicha información, las finalidades para las que supuestamente ha dado su aprobación (incluido el envío de comuni-caciones comerciales) y especificando el modo en el que puede acceder a sus derechos sobre los datos faci-litados.
- Ante la recepción por carta, email, telefónicamente o de cualquier otra forma habilitada por la empresa de una solicitud de un cliente, empleado o proveedor del ejercicio de su derecho de acceso, rectificación, cance-lación, oposición, portabilidad u olvido a sus datos personales, deberá informarse inmediatamente al Respon-sable de Tratamiento o Delegado de Protección de Datos (si lo hubiera), quien se ocupará de dar trámite a di-cha solicitud conforme a las normas que rigen el ejercicio de los derechos de los afectados.
- Si solo se recibe una consulta sobre el ejercicio de alguno de estos derechos, el trabajador debe informar del procedimiento para ejercerlo, que es el siguiente:
    - Previa presentación de su documento nacional de identidad o pasaporte, los titulares de los datos personales (interesados) podrán ejercer sus derechos de acceso, rectificación, supresión, oposición y portabilidad. El responsable del tratamiento deberá dar respuesta a los interesados sin dilación indebida.

Para el **derecho de acceso** se facilitará a los interesados la lista de los datos personales de que disponga junto con la finalidad para la que han sido recogidos, la identidad de los destinatarios de los datos, los plazos de conservación, y la identidad del responsable ante el que pueden solicitar la rectificación supresión y oposición al tratamiento de los datos.
Para el **derecho de rectificación** se procederá a modificar los datos de los interesados que fueran inexactos o incompletos atendiendo a los fines del tratamiento.
Para el **derecho de supresión** se suprimirán los datos de los interesados cuando los interesados manifiesten su negativa u oposición al consentimiento para el tratamiento de sus datos y no exista deber legal que lo impida.
Para el **derecho de portabilidad** los interesados deberán comunicar su decisión e informar al responsable, en su caso, sobre la identidad del nuevo responsable al que facilitar sus datos personales.

El responsable del tratamiento deberá informar a todas las personas con acceso a los datos personales acerca de los términos de cumplimiento para atender los derechos de los interesados, la forma y el procedimiento en que se atenderán dichos derechos.

- No dar información a nadie que no sea el interesado o su representante legal
- La ley prohíbe comunicar datos de carácter personal de una persona a otra que no sea él mismo o su representante legal (debidamente acreditado).

Por lo tanto, salvo que previamente haya sido autorizado por el interesado, no se podrá entregar documentación o informar a personas no autorizadas, aunque sean familiares. En el caso de que alguien, en su nombre, solicite alguna información, se deberá poner en conocimiento del interesado y solicitar su autorización. Otra forma podrá ser la del envío de la información solicitada al propio interesado, para que sea él, bajo su propia responsabilidad, la que se la entregue a quien considere.

- Menores de edad.

En el caso de menores de edad (14 años) la información solo se entregará a su(s) representante(s) legal(es). A este respecto, queremos comentar que en el caso de los menores de edad, cualquier dato que se maneje se debe tomar especial precaución, siendo necesario siempre recabar el consentimiento de representantes legales para el tratamiento de cualquier dato personal.

**VIOLACIONES DE SEGURIDAD DE DATOS DE CARÁCTER PERSONAL**

- Cuando se produzcan violaciones de seguridad DE DATOS DE CARÁCTER PERSONAL, como por ejemplo, el ro-bo o acceso indebido a los datos personales se notificará a la Agencia Española de Protección de Datos en término de 72 horas acerca de dichas violaciones de seguridad, incluyendo toda la información necesaria para el esclarecimiento de los hechos que hubieran dado lugar al acceso indebido a los datos personales. La notifi-cación se realizará por medios electrónicos a través de la sede electrónica de la Agencia Española de Protec-ción de Datos en la dirección: https://sedeagpd.gob.es

**CAPTACIÓN DE IMÁGENES CON CÁMARAS Y FINALIDAD DE SEGURIDAD (VIDEOVIGILANCIA)**

- **UBICACIÓN DE LAS CÁMARAS:** Se evitará la captación de imágenes en zonas destinadas al descanso de los trabajadores.
- **UBICACIÓN DE MONITORES:** Los monitores donde se visualicen las imágenes de las cámaras se ubicarán en un espacio de acceso restringido de forma que no sean accesibles a terceros.
- **CONSERVACIÓN DE IMÁGENES:** Las imágenes se almacenarán durante el plazo máximo de un mes, con excepción de las imágenes que sean aportadas a los tribunales y las fuerzas y cuerpos de seguridad.
- **DEBER DE INFORMACIÓN:** Se informará acerca de la existencia de las cámaras y grabación de imágenes mediante un distintivo informativo donde mediante un pictograma y un texto se detalle el responsable ante el cual los interesados podrán ejercer su derecho de acceso. En el propio pictograma se podrá incluir el texto in-formativo.
- **CONTROL LABORAL:** Cuando las cámaras vayan a ser utilizadas con la finalidad de control laboral según lo previsto en el artículo 20.3 del Estatuto de los Trabajadores, se informará al trabajador o a sus representan-tes acerca de las medidas de control establecidas por el empresario con indicación expresa de la finalidad de control laboral de las imágenes captadas por las cámaras.
- **DERECHO DE ACCESO A LAS IMÁGENES:** Para dar cumplimiento al derecho de acceso de los interesados se solicitará una fotografía reciente y el Documento Nacional de Identidad del interesado, así como el detalle de la fecha y hora a la que se refiere el derecho de acceso.
    - No se facilitará al interesado acceso directo a las imágenes de las cámaras en las que se muestren imágenes de terceros. En caso de no ser posible la visualización de las imágenes por el interesado sin mos-trar imágenes de terceros, se facilitará un documento al interesado en el que se confirme o niegue la exis-tencia de imágenes del interesado.

**MEDIDAS TÉCNICAS**

**IDENTIFICACIÓN**

- Cuando el mismo ordenador o dispositivo se utilice para el tratamiento de datos personales y fines de uso personal se recomienda disponer de varios perfiles o usuarios distintos para cada una de las finalidades. De-ben mantenerse separados los usos profesional y personal del ordenador.

No está permitido emplear identificadores y contraseñas de otros usuarios para acceder al sistema.

- Se recomienda disponer de perfiles con derechos de administración para la instalación y configuración del sis-tema y usuarios sin privilegios o derechos de administración para el acceso a los datos personales. Esta me-dida evitará que en caso de ataque de ciberseguridad puedan obtenerse privilegios de acceso o modificar el sistema operativo.
- Se garantizará la existencia de contraseñas para el acceso a los datos personales almacenados en sistemas electrónicos. La contraseña tendrá al menos 8 caracteres, mezcla de números ,letras, mayúsculas, minúscu-las y caracteres especiales.
- Cuando a los datos personales accedan distintas personas, para cada persona con acceso a los datos perso-nales, se dispondrá de un usuario y contraseña específicos (identificación inequívoca).
- Se debe garantizar la confidencialidad de las contraseñas, evitando que queden expuestas a terceros. En nin-gún caso se compartirán las contraseñas ni se dejarán anotadas en lugar común y el acceso de personas dis-tintas del usuario.

**DEBER DE SALVAGUARDA**

A continuación se exponen las medidas técnicas mínimas para garantizar la salvaguarda de los datos personales:

**DATOS EN MEDIOS ELECTRÓNICOS**

- **ACTUALIZACIÓN DE ORDENADORES Y DISPOSITIVOS:** Los dispositivos y ordenadores utilizados para el almacenamiento y el tratamiento de los datos personales deberán mantenerse actualizados en la media posi-ble.
- **MALWARE:** En los ordenadores y dispositivos donde se realice el tratamiento automatizado de los datos personales se dispondrá de un sistema de antivirus que garantice en la medida posible el robo y destrucción de la información y datos personales. El sistema de antivirus deberá ser actualizado de forma periódica.
- **CORTAFUEGOS O FIREWALL:** Para evitar accesos remotos indebidos a los datos personales se velará pa-ra garantizar la existencia de un firewall activado en aquellos ordenadores y dispositivos en los que se realice el almacenamiento y/o tratamiento de datos personales.
- **CIFRADO DE DATOS:** Cuando se precise realizar la extracción de datos personales fuera del recinto donde se realiza su tratamiento, ya sea por medios físicos o por medios electrónicos, se deberá valorar la posibili-dad de utilizar un método de encriptación para garantizar la confidencialidad de los datos personales en caso de acceso indebido a la información.
- **COPIA DE SEGURIDAD:** Periódicamente se realizará una copia de seguridad en un segundo soporte distinto del que se utiliza para el trabajo diario. La copia se almacenará en lugar seguro, distinto de aquél en que esté ubicado el ordenador con los ficheros originales, con el fin de permitir la recuperación de los datos personales en caso de pérdida de la información.
- **DISPOSITIVOS MÓVILES:** Todo aquel dispositivo móvil (Tablet, ordenador portátil o smartphone) que se ponga en disposición de los empleados para realizar su trabajo, deberá ser custodiado por cada uno, guardan-do las mismas medidas de seguridad y acceso que en el resto de equipos, teniendo que contar con la debida autorización de la empresa para utilizarlos fuera de sus instalaciones y notificando cualquier incidencia de seguridad que se produzca.

No se podrán disponer fuera de la empresa de cualquier soporte con datos de carácter personal relativos a clientes, salvo autorización expresa de los responsables.

- Los **aparatos y líneas telefónicas contratadas**, la red informática, los terminales fijos y móviles, las apli-caciones, redes, conexiones y demás elementos de hardware y software utilizados por cada empleado, no de-berán usarse para fines ajenos a los relacionados con la actividad que el usuario deba desempeñar para tu empresa. No se usarán para fines personales.
- El titular de la cuenta de **correo electrónico** asignado por la empresa será responsable del uso de la misma. Debe tener en cuenta que se trata de un correo electrónico profesional, por lo que se deberá usar sólo para este fin y no para fines personales. Es importante que el trabajador observe las pautas de buena conducta en la gestión de las contraseñas asignadas para acceder a su equipo. La empresa podrá monitorizar el uso del correo electrónico por parte del empleado como medida de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales .

Queda prohibido el envío de correo electrónico con datos personales y, si se hace, la información deberá cifrarse. En el supuesto de envío de un correo electrónico a varias personas, se debe utilizar la casilla CCO (con copia oculta) ya que, si no, se entiende como una vulneración del deber de secreto. Por este motivo, queda también

prohibido el envío o reenvío mensajes en cadena o con fines comerciales o publicitarios sin el consentimiento del destinatario.

- No conectar memorias USB  o discos externos desconocidos en nuestro ordenador.
- **USO DE INTERNET:** Deberá el empleado realizar un uso seguro de Internet y e informar al Responsable de Tratamiento de cualquier incidencia que pueda comprometer la seguridad del sistema y de los datos de ca-rácter personal. Quedando prohibido el acceso a páginas que supongan una actividad ilegal, o de contenido no relacionado con el trabajo, también el acceso a páginas de dudosa procedencia.
- **INSTALACIÓN DE PROGRAMAS POR CUENTA PROPIA:** Instalar aplicativos por cuenta propia y sin auto-rización y/o conocimiento de la empresa puede generar riesgos innecesarios para la empresa y para nosotros mismos, por esto, la instalación de programas por cuenta del empleado debe estar expresamente autorizada por la empresa.
- **WHATSAPP:** En el caso específico de la aplicación Whatsapp no se deberá instalar en dispositivos empresariales ni se utilizará en cualquier dispositivo para comunicación empresarial, salvo expresa autorización por parte de la empresa. En todo caso, se evitará el envío de cualquier dato personal por medio de esta aplicación ya que puede generar riesgos innecesarios, dado que para el envío de datos personales existen medios más seguros como por ejemplo email cifrados.

**DATOS EN MEDIOS FÍSICOS (PAPEL)**

El personal que, para el correcto desarrollo de su labor, tiene autorizado acceso a datos personales, tiene las siguientes obligaciones:

- Mantener debidamente custodiadas las llaves de acceso a las dependencias de la empresa, a sus despachos y a los armarios, archivadores u otros elementos que contenga ficheros no automatizados con datos de carácter personal, debiendo poner en conocimiento del Responsable de Tratamiento cualquier hecho que pueda haber comprometido esa custodia.
- Cerrar con llave las puertas de los despachos al término de la jornada laboral o cuando deba ausentarse temporalmente de esta ubicación, a fin de evitar accesos no autorizados.
- Queda prohibido el traslado de cualquier listado o documento análogo con datos de carácter personal en los que se almacene información titularidad de la entidad fuera de los locales de la misma.
- Guardar todos los soportes físicos o documentos que contengan información con datos de carácter personal en un lugar seguro, cuando estos no sean usados, particularmente fuera de la jornada laboral.
- Asegurarse de que no quedan documentos impresos que contengan datos protegidos impresos en la bandeja de salida de la impresora.
- Únicamente las personas autorizadas para ello en el listado de accesos podrán introducir, modificar o anular los datos contenidos en los ficheros objeto de protección. Los permisos de acceso de los usuarios a los diferentes ficheros son concedidos por el Responsable de Tratamiento. En el caso de que cualquier usuario requiera, para el desarrollo de su trabajo, acceder a ficheros a cuyo acceso no está autorizado, deberá ponerlo en conocimiento del Responsable.
- No enviar documentación por fax: Al no existir modo de garantizar que la persona que recibe el fax, conteniendo datos de carácter personal, es realmente el interesado, este medio de comunicación no es el adecuando. Por lo tanto, se deberá evitar su utilización en la medida de lo posible.

## Acuse de recibo de la Normativa de Usuarios

Yo _____ _____, con DNI _____ declaro haber recibido de la entidad Asociación de discapacitados físicos de la isla de La Palma ADFILPA , con NIF G38772117 el documento denominado NORMATIVA PARA USUARIOS, explicativo de las funciones y obligaciones en materia de Protección de Datos Personales.

En _____ a ___ de _____ de 20___

**Firma:**