Consejo General
de Colegios Oficiales
de Farmacéuticos

GUÍA PRÁCTICA DE APLICACIÓN DEL REGLAMENTO EUROPEO DE PROTECCIÓN DE DATOS

Dirigida a la Organización Farmacéutica Colegial, oficinas de farmacia y otros establecimientos o centros sanitarios

Edita:
Consejo General de Colegios Oficiales de Farmacéuticos
C/ Villanueva, 11, 7ª planta. 28001 Madrid
congral@redfarma.org
www.portalfarma.com

Con la colaboración de: Previsión Sanitaria Servicios y Consultoría S.L.U.

Maquetación y Producción Gráfica: Comuniland S.L.

DICIEMBRE 2017

ÍNDICE

RESUMEN EJECUTIVO

Aspectos más destacados de la aplicación de la nueva regulación sobre protección de datos, aplicable en España a partir del 25 de mayo de 2018

¿Qué es el RGPD?

El Reglamento General de Protección de Datos (RGPD) es un nuevo marco normativo que tiene como objetivo fortalecer y unificar la protección de datos en todos los países de la Unión Europea

El RGPD será de obligado cumplimiento a partir del 25 de mayo de 2018

DPO ¿Necesito designar un DPO?

El RGPD introduce la figura del Delegado de Protección de Datos (DPO en sus siglas en inglés).

COLEGIOS PROFESIONALES
OBLIGATORIO

OFICINAS DE FARMACIA, ORTOPEDIA, LABORATORIO DE ANÁLISIS CLÍNICOS
CONVENIENTE

¿CUÁNDO ES NECESARIO UN DPO?
Cuando se requiera el tratamiento de categorías especiales de datos a gran escala

¿QUÉ SE CONSIDERA "GRAN ESCALA?
Este concepto está sujeto a varias interpretaciones ya que el término "gran escala" no está cuantificado (concepto jurídico indeterminado)

En definitiva, habría que hacer un análisis del volumen de datos tratados, número de afectados y ámbito geográfico, aunque sería recomendable la designación de un DPO en aras del cumplimiento de la nueva regulación. Existe también la posibilidad de que este DPO pueda ser compartido.

¿Qué es un DPO compartido?

El RGPD dice que: "El delegado de protección de datos podrá actuar por cuenta de (...) asociaciones y otros organismos que representen a responsables o encargados". Por ejemplo, el DPO que haya designado Colegio Oficial de Farmacéuticos podría desempeñar el mismo papel para los colegiados siempre que estos se adscriban de forma voluntaria a dicho DPO.

Consentimiento

Antes de la introducción del RGPD, el consentimiento "tácito" (por omisión/inacción) estaba permitido.

Ahora, a partir del comienzo de la aplicación (25 de mayo de 2018) el consentimiento tiene que proceder de una manifestación de voluntad "libre, específica, informada e inequívoca", aunque esto no significa que sea necesario el consentimiento por escrito (consentimientos aceptados por medios electrónicos). El consentimiento en menores de edad se fija para mayores de 13 años (según el Proyecto de LOPD).

Principio de proactividad

Antes de la introducción del RGPD, las medidas que se articulaban eran principalmente reactivas. Ahora, a partir del momento en el que sea de obligado cumplimiento (25 de mayo de 2018) serán principalmente preventivas (principio de proactividad). Esto se manifiesta en el análisis de riesgo, evaluaciones de impacto, privacidad desde el diseño y por defecto.

Registro de actividad

ADIÓS A LA INSCRIPCIÓN DE FICHEROS

Con el RGPD, se establece la obligatoriedad de elaborar un registro de actividad del tratamiento de datos que deberá facilitarse a la AEPD en caso de solicitud y publicarlo en nuestra página web para cumplir con el principio de transparencia.

Derecho a la portabilidad, a la limitación y notificaciones

El RGPD dota a los ciudadanos de nuevos derechos y herramientas con las que proteger y facilitar la gestión de sus datos.

- **PORTABILIDAD:** Los ciudadanos podrán obtener una copia de sus datos en un formato estructurado y legible mecánicamente.
- **LIMITACIÓN:** Los ciudadanos pueden solicitar a que no se realice tratamiento con respecto a una parte de su datos personales si se dan las circunstancias para ello.
- **NOTIFICACIONES:** Los responsables de tratamiento deberán notificar violaciones de seguridad de datos antes de 72 horas a la AEPD.

Encargado de tratamiento

- Antes del RGPD, las relaciones del encargado y el responsable del tratamiento se regulaban mediante un compromiso de confidencialidad.
- Ahora, se debe plasmar en un nuevo modelo de contrato que especifique en que consiste el tratamiento.
- Con ello se pretende dar garantías a la hora de elegir prestadores de servicios y saber si estos cumplen con las nuevas exigencias del RGPD y garantizar su cumplimento.

Categorías especiales de datos

Además de los datos de salud, con el RGPD se extienden las categorías especiales de datos a los datos genéticos y biométricos.

Mayores sanciones

Antes las multas iban desde los 900 hasta los 600,000 €, ahora pueden llegar hasta los 20 millones de euros como máximo o, tratándose de una empresa, el 4% de la facturación anual global.

| 1. INTRODUCCIÓN |

El **Reglamento Europeo 2016/679** de 27 de abril de 2016, Reglamento General de Protección de Datos (en adelante **RGPD**) entró en vigor el 25 de mayo de 2016 y será de obligado cumplimiento y de aplicación directa en España a partir del **25 de Mayo de 2018.**

En la actualidad, tenemos las siguientes normativas en materia de Protección de Datos de carácter personal en vigor:

– Ley Orgánica 15/1999, de Protección de Datos de carácter personal (en adelante **LOPD**)
– Real Decreto 1720/2007, Reglamento de desarrollo de la Ley Orgánica 15/1999 (en adelante **RLOPD**)

Las citadas normativas van a ser sustituidas y derogadas por **la nueva Ley Orgánica de Protección de Datos de Carácter Personal** (en adelante **Nueva LOPD**)

Dicha ley se encuentra en **fase de proyecto en las Cortes para su tramitación y aprobación.**

Son sujetos obligados por dicha normativa:

– La Organización Farmacéutica Colegial (Consejo, Colegios)
– Las oficinas de farmacia
– Otros establecimientos o centros sanitarios (óptica, ortopedia, laboratorios de análisis clínicos etc...)

El **objeto de la presente guía** es hacer **una comparativa entre las obligaciones actuales** que establece la Ley Orgánica de Protección de Datos en vigor (LOPD) **y las novedades y cambios que van a introducir el Reglamento General de Protección de Datos (RGPD) y la nueva Ley Orgánica de Protección de Datos (Nueva LOPD).**

| 2. DEFINICIONES |

Entre las definiciones que se introducen en el Reglamento, se destacan a continuación algunas de ellas:

- **Datos personales:** 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.
- **Tratamiento**: 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);
- **Responsable del tratamiento**: persona física o jurídica, autoridad pública, que solo o junto con otros, determine los fines y medios de tratamiento de datos
- **Encargado del tratamiento**: persona física o jurídica, autoridad pública que trate datos personales por cuenta del responsable del tratamiento.
- **Limitación del tratamiento:** Derecho del interesado de marcar sus datos para limitar su tratamiento en el futuro.
- **Elaboración de perfiles**: toda forma de tratamiento automatizado de datos personales consistente en utilizar 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 física;
- **Seudonimización**: el tratamiento de datos personales de manera tal 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;
- **Consentimiento del interesado:** 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;
- **Violación de la seguridad de los datos personales**: toda violación de la 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 autorizados a dichos 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 esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona;
- **Datos biométricos**: datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos;
- **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;

| 3. DPO (DATA PROTECTION OFFICER) |

DATA PROTECTION OFFICER (DPO) / DELEGADO DE PROTECCIÓN DE DATOS (DPD)

Normativa actual (LOPD y RLOPD)

La Ley Orgánica de Protección de Datos de carácter personal (LOPD) y su Reglamento de Desarrollo (RLOPD) establecían la figura del Responsable de Seguridad.

El Responsable de Seguridad era la persona que se encargaba de implementar las medidas de seguridad en materia de Protección de Datos y dicha figura era obligatoria designarla siempre que se realizaran tratamientos de datos en ficheros de nivel medio/alto (Datos de salud por ejemplo).

Normativa de aplicación a partir del 25 de Mayo de 2018 (Reglamento General de Protección de Datos (RGPD) y Nueva Ley Orgánica de Protección de Datos de Carácter Personal)

La nueva normativa introduce la figura del **Data Protection Officer o Delegado de Protección de Datos** que será la persona física o jurídica encargada de

velar por el cumplimiento de la normativa de Protección de Datos de carácter personal.

Esta figura se regula en el artículo 37 y siguientes del RGPD y en el artículo 34 de la Nueva LOPD.

Las funciones a desarrollar el DPO son las siguientes:

- Informar y asesorar al responsable del tratamiento de datos de las nuevas obligaciones y ayudar a la implementación del Reglamento General y la Nueva Ley Orgánica de Protección de Datos de Carácter Personal.
- Supervisar los nuevos contratos que se firmen con los encargados de tratamiento, así como la verificación de que un encargado de tratamiento ofrece las garantías adecuadas a nivel de protección de datos para el cumplimiento de lo establecido en la normativa.
- Supervisar la documentación, notificación y comunicación de las violaciones de seguridad de datos personales, así como la supervisión de las normativas de confidencialidad relativas a empleados, formación interna y realización de auditorías.
- Cooperar con la autoridad de control y establecer un punto de contacto entre el Responsable del tratamiento y la Agencia Española de Protección de Datos (AEPD).

Será obligatorio el nombramiento o designación del DPO en los siguientes supuestos:

- Autoridades y organismos públicos, **así como las organizaciones colegiales profesionales en cuanto al tratamiento de datos correspondiente a los ficheros que actualmente se encuentran inscritos en la AEPD, como ficheros de titularidad pública, tales como ficheros de colegiación en el ejercicio de potestades públicas, de sanciones.**
- Responsables o encargados de tratamiento que tengan entre sus actividades principales operaciones de tratamiento que requieran una observación habitual y sistemática de interesados a gran escala o que traten a gran escala categorías especiales de datos (entre otros, salud, biométricos, genéticos).

El DPO nombrado tiene:

- Total autonomía en el ejercicio de sus funciones: garantía de no recibir instrucción en el desempeño de sus funciones;
- Rinde cuentas directamente al más alto nivel jerárquico de la dirección;
- Se le tienen que facilitar todos los recursos necesarios para el desarrollo de su actividad y para el mantenimiento de sus conocimientos;
- No puede ser destituido ni sancionado por desempeñar sus funciones;
- Puede ejercer otras funciones que no den lugar a conflictos de intereses.

El DPO puede ser de carácter interno (personal laboral del Responsable) o ser de carácter externo (contratar a un prestador de servicios) y tiene que ser un profesional especializado en Derecho y Protección de Datos y con experiencia práctica en la materia.

Un mismo DPO puede atender a distintos Responsables siempre que sea accesible a cada establecimiento.

Por ejemplo, un COF podría nombrar un DPO colegial y, este mismo DPO puede ofertar sus servicios a oficinas de farmacias u otros establecimientos que así lo decidan.

Los datos de contacto del DPO deben hacerse público por los Responsables y Encargados del tratamiento y, además, ser comunicados a las autoridades de supervisión (AEPD). Son puntos de contacto para los interesados en todo lo relacionado con el tratamiento de sus datos personales.

4. INFORMACIÓN Y OBTENCIÓN DEL CONSENTIMIENTO

INFORMACIÓN Y OBTENCIÓN DEL CONSENTIMIENTO PARA EL TRATAMIENTO DE DATOS

Normativa actual (LOPD y RLOPD)

Deber de información

La LOPD establecía que el responsable del fichero estaba obligado a informar sobre la existencia de un fichero o tratamiento de datos de carácter personal, la identidad del responsable del tratamiento, la finalidad de la recogida de los datos y de los destinatarios de la información, así como de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición en todos los procesos en los que hubiera recogida de datos.

Consentimiento
La LOPD requería el consentimiento inequívoco del afectado, pero admitía el consentimiento tácito en determinados supuestos. Respecto a los datos de menores de edad, se establecía que los mayores de 14 años de edad podían otorgar su consentimiento sin necesidad de recabar el de sus progenitores.

Normativa de aplicación a partir del 25 de Mayo de 2018

(Reglamento General de Protección de Datos (RGPD) y Nueva Ley Orgánica de Protección de Datos de Carácter Personal)

Transparencia, Información y acceso a los datos personales
El artículo 13 y 14 del RGPD y el artículo 11 de la Nueva LOPD establecen que el Responsable del tratamiento deberá **facilitar la información a los interesados de forma concisa, transparente, inteligible y de fácil acceso y con lenguaje claro y sencillo.** Dicha información contemplará la identidad y datos de contacto del Responsable, los fines del tratamiento especificando la base jurídica del tratamiento, los destinatarios o categoría de destinarios de datos, el período de conservación de los datos, si se van o no a realizar transferencias internacionales, los datos de contacto del DPO, si se va a realizar elaboración de perfiles, así como los derechos que asisten a los interesados y a que autoridad de control (AEPD) podrán dirigir sus reclamaciones.

Consentimiento
El artículo 4.11 del RGPD y el artículo 6 de la Nueva LOPD establecen que el consentimiento del interesado es 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.

Con el RGPD, no se admiten los consentimientos tácitos o por omisión, ya que se basan en la inacción y así se recoge en el Considerando 32 del RGPD que expone que el silencio, las casillas premarcadas o la inacción no constituirán prueba de consentimiento.

Respecto a los datos de menores de edad, el RGPD establece que el consentimiento de los menores de edad será válido cuando tengan como mínimo 16 años (artículo 8 del RGPD).

Actualmente, la edad mínima para prestar el consentimiento esta fijada en los 14 años. El proyecto de ley de la Nueva LOPD, pendiente de aprobación, propone rebajar la edad a los 13 años.

| 5. PRINCIPIO DE PROACTIVIDAD |

PRINCIPIO DE RESPONSABILIDAD PROACTIVA

Normativa actual (LOPD y RLOPD)

En el RLOPD se recogía un catálogo de medidas en función del nivel de datos (básico, medio o alto) que manejaba el Responsable de Fichero (contraseñas individualizadas, registros de accesos, normativas de confidencialidad, Contratos de Encargados de Tratamiento, Realización de Copias de Seguridad semanales...)

Normativa de aplicación a partir del 25 de Mayo de 2018

(Reglamento General de Protección de Datos (RGPD) y Nueva Ley Orgánica de Protección de Datos de Carácter Personal)

La distinción de niveles de ficheros básicos, medios y alto desaparece con el RGPD y en el artículo 24 del RGPD se especifica que las medidas de seguridad se aplicarán teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los riesgos para los derechos y libertades de las personas físicas.

No se establece como tal un catálogo cerrado de medidas, sino que el Responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas para cumplir con lo establecido en el RGPD y la Nueva LOPD.

No obstante, el principio de responsabilidad proactiva conlleva que se apliquen determinadas medidas y procedimientos que conlleven a verificar e implementar mejoras dentro del cumplimiento de la normativa en materia de protección de datos.

Las medidas y procedimiento a destacar son:

- **PROTECCIÓN DE DATOS DESDE EL DISEÑO Y POR DEFECTO:**
  Los Responsables de tratamiento tienen que enfocar el tratamiento de datos con Responsabilidad proactiva, es decir, desde el momento en que se empiece a diseñar el servicio o producto que pueda implicar tratamiento de datos de carácter personal y con anterioridad al inicio del tratamiento deben tomar las medidas organizativas y técnicas necesarias para aplicar de forma efectiva los principios establecidos en el RGPD.

Se tendrá en cuenta: la cantidad de datos a tratar, la extensión del tratamiento, periodos de conservación de los datos y su accesibilidad.

- **ANÁLISIS DE RIESGOS DEL TRATAMIENTO DE DATOS:**
  El artículo 32.2 del RGPD establece que al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los costes de aplicación, la naturaleza, alcance, contexto y fines del tratamiento y los riesgos que conlleva para los derechos y libertades de los interesados.

  Los Colegios, farmacias y otros establecimientos sanitarios como Responsables del tratamiento de datos deben realizar una valoración y análisis del riesgo de dicho tratamiento en función de:

  – tipo de tratamiento se va a realizar;
  – naturaleza de los datos;
  – número de interesados afectado y
  – cantidad y variedad de datos

En función del resultado de este análisis de riesgo, se establecerán las medidas de seguridad que se deben aplicar para cumplir con lo establecido en el RGPD y la Nueva LOPD.

Al inicio del análisis de riesgo, habrá que:

  – Ver si tratamos datos sensibles, como entre otros, los datos genéticos, biométricos o relativos a la salud;
  – Ver si con el tratamiento se elaboran perfiles;
  – Ver si se tratan datos de muchas personas y gran cantidad o variedad de datos;
  – Ver si hay cruce de datos de los interesados con los obtenidos de otras fuentes;
  – Ver si se van a utilizar para una finalidad o para varias finalidades;
  – Ver si se usan tecnologías invasivas de la privacidad (geolocalización, videovigilancia...).

- **EVALUACIÓN DE IMPACTO SOBRE LA PROTECCIÓN DE DATOS:**
  La evaluación de impacto sobre la protección de datos se debe realizar con carácter previo a la puesta en marcha de los tratamientos que sea probable que conlleven un alto riesgo para los interesados en los que se evalúe el origen, la naturaleza, la particularidad y la gravedad de dicho riesgo. Como lista indicativa, entre otros, de los supuestos en los que se considera que hay alto riesgo:

  – Elaboración de perfiles en base a los cuales se toman decisiones que produzcan efectos jurídicos sobre los interesados o que les afecten significativamente.
  – Tratamiento de categorías de datos especiales (de salud, genéticos y biométricos entre otros) a gran escala. Para valorar si el tratamiento se realiza a gran escala se tendrá en cuenta el número de interesados afectados en términos absolutos o en proporción a una población; volumen y variedad de datos tratados, duración de la actividad del tratamiento y extensión geográfica.

Si se ha realizado el análisis de riesgo sobre los tratamientos de datos que se están llevando a cabo antes de la aplicación del Reglamento y el resultado es que presentan alto riesgo para los derechos y libertades de los interesados, los Responsables de tratamiento deben realizar una Evaluación de Impacto sobre la protección de datos. La AEPD elaborará una lista de tratamientos que requieren impacto de protección, así como en su caso también una que no lo requiera. Con independencia de las listas, los Responsables tienen que realizar el análisis de riesgos.

- **CONSULTA Y AUTORIZACIONES PREVIAS:**
  El Responsable del tratamiento consultará a la AEPD cuando una evaluación de impacto muestre que el tratamiento entrañaría un alto riesgo si el Responsable no toma medidas para mitigarlo y el Responsable considera que no puede mitigarse por medios razonables en cuanto a tecnología y costes de aplicación.

  La AEPD:
  – Asesorará por escrito al Responsable o, en su caso, al encargado.
  – Puede llegar a prohibir el tratamiento.

  El Reglamento prevé que la normativa nacional pueda establecer consulta y autorización en tratamientos derivados del ejercicio de una misión realizada en interés público por el Responsable.

- **NOTIFICACIÓN DE VIOLACIÓN DE SEGURIDAD:**
  Se define violación como *"incidente que ocasiona destrucción, pérdida, alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma o la comunicación o acceso no autorizado a los mismos"*. (EJEMPLO: pérdida portátil, acceso no autorizado a bases de datos por personal propio o terceros, borrado accidental de algunos registros.)

Salvo que se estime que resulte improbable que exista riesgo para los derechos y libertades de los interesados, ante cualquier violación o quiebra de seguridad, deberá el Responsable:

- Notificar a la autoridad de protección de datos competente el fallo de seguridad, en el plazo de 72 horas o justificar, informando de la naturaleza de la violación; categorías de datos y de interesados afectados; medidas adoptadas para solventar la quiebra y medidas para paliar los posibles efectos negativos sobre los interesados.
- Si la violación entraña alto riesgo hay que notificar también a los afectados. Por ejemplo, cuando se desvele información confidencial, contraseñas, difusión de datos sensibles o que produzcan perjuicios económicos.
- Valoración del riesgo: Hay alto riesgo: (i) Cuando el tratamiento permita elaborar perfiles sobre cuya base se tomen decisiones con efectos jurídicos sobre los interesados o que les afecten significativamente,; (ii) Cuando se realice el tratamiento a gran escala de datos sensibles y hay gran escala en función del número de interesados afectados en términos absolutos o en proporción a una determinada población; volumen y variedad de datos tratados; duración o permanencia de la actividad de tratamiento y extensión geográfica de la actividad de tratamiento.

| 6. REGISTRO DE ACTIVIDAD DEL TRATAMIENTO |

REGISTRO DE ACTIVIDADES DE TRATAMIENTO:

Normativa actual (LOPD Y RLOPD)

El CAPÍTULO I Y II de la LOPD establecía la obligación de creación e inscripción de ficheros en el Registro General de la Agencia Española de Protección de Datos.

Normativa de aplicación a partir del 25 de Mayo de 2018 (Reglamento General de Protección de Datos (RGPD) y Nueva Ley Orgánica de Protección de Datos de Carácter Personal)

Desaparece la obligación de inscripción de ficheros ante el Registro de la Agencia Española de Protección de Datos y se sustituye por la elaboración de un Registro de Actividades de tratamiento.

El artículo 30 del RGPD expone que las organizaciones que habitualmente realicen tratamiento de datos de riesgo para la privacidad de los interesados o traten datos sensibles, deberán elaborar con un registro de las actividades de tratamiento efectuadas bajo su responsabilidad. El Registro de las actividades del tratamiento es de aplicación a los Responsables y Encargados de tratamiento con más de 250 empleados, salvo si se tratan categorías especiales de datos como los de salud, entre otros, o datos con riesgo para los derechos y libertades de los interesados.

Los Responsables de tratamiento vienen obligados a mantener un Registro de actividades conteniendo: nombre y datos de contacto del Responsable y del DPO; los datos personales que se traten, los destinatarios de los datos, los plazos previstos para la supresión, la finalidad de dicho tratamiento y las medidas técnicas y de seguridad adoptadas por la empresa para realizar dicho tratamiento.

Dicho registro deberá ser publicado en nuestra página web y deberá facilitarse a la AEPD en caso de solicitud.

| 7. NUEVOS DERECHOS ARCO |

EJERCICIO DE LOS DERECHOS POR PARTE DE LOS INTERESADOS:

Normativa actual (LOPD Y RLOPD)

Los derechos reconocidos en la LOPD son los siguientes:

- Derecho de acceso
- Derecho de rectificación
- Derecho de oposición
- Derecho de cancelación

Normativa de aplicación a partir del 25 de Mayo de 2018 (Reglamento General de Protección de Datos (RGPD) y Nueva Ley Orgánica de Protección de Datos de Carácter Personal)

Con el RGPD y la Nueva LOPD, se amplía el catálogo de derechos que poseen los interesados respecto al tratamiento de sus datos personales. Para poder ejercitarlos, se deberá implementar un procedimiento fácil, ágil y gratuito para gestionar las solicitudes en el plazo de un mes. Si se entiende que no procede a admitir la solicitud, se deberá motivar dentro del plazo de un mes.

Así mismo, los usuarios deberán verificar su identidad ante el Responsable y este podrá contar con la colaboración de los encargados del tratamiento para la correcta gestión del ejercicio de los Derechos ARCO.
A continuación, se expone el catálogo completo de derechos que se recogen en los artículos 15 a 22 del RGPD y en los artículo 12 a 18 de la Nueva LOPD:

Derechos

- **Acceso**: El interesado tiene derecho a obtener copia de los datos personales objeto de tratamiento, incluyendo la posibilidad de dar acceso remoto directo a través de un sistema seguro.

- **Rectificación**: El interesado tiene derecho de rectificación de sus datos inexactos, así como de que se completen los que estuvieren incompletos. El responsable comunicará al interesado la rectificación.

- **Supresión**: El interesado tiene derecho de supresión de sus datos cuando ya no sean necesarios en relación con los fines para los que se recabaron; se retire el consentimiento; se oponga el interesado al tratamiento (oposición).

- **Oposición**: El interesado tendrá derecho a oponerse en todo momento al tratamiento de los datos personales que le conciernan, incluida la elaboración de perfiles, cuando el tratamiento de datos personales tenga por objeto la mercadotecnia directa.

  El interesado tendrá derecho, por motivos relacionados con su situación particular, a oponerse al tratamiento de datos personales que le conciernan cuando los datos personales se traten con fines de investigación científica o histórica o fines estadísticos, salvo que sea necesario para el cumplimiento de una misión realizada por razones de interés público.

- **Limitación del tratamiento**: Es un derecho nuevo en el que por parte del interesado se puede solicitar que no se apliquen a sus datos personales las operaciones de tratamiento, mientras se están ejerciendo los derechos de rectificación u oposición y el Responsable está en proceso de determinar si procede o no. También cuando el tratamiento es ilícito, lo que determinaría el borrado de datos pero el interesado se opone o cuando los datos ya no son necesarios (se borrarían) pero el interesado solicita limitación.

  Durante el período de duración de la limitación, el Responsable del tratamiento sólo puede tratar los datos de éstos para su conservación, salvo con el consentimiento del interesado para formular la defensa de reclamaciones.

  La limitación impide el borrado de datos cuando se ejercitan otros derechos como el de acceso, ya que se impediría -si se borraran- el ejercicio del derecho a la limitación del tratamiento.

- **Portabilidad:** Es un derecho de acceso avanzado por el cual se facilita a un interesado la copia de sus datos en un formato estructurado, de uso común y lectura mecánica cuando el tratamiento se efectúa por medios automatizados.

  Es un derecho que implica que a solicitud de un interesado sus propios datos se puedan enviar de un Responsable a otro, si técnicamente es posible.

  No cabe portabilidad cuando los datos han sido facilitados por terceros.

| 8. RELACIÓN ENTRE LOS RESPONSABLES Y ENCARGADOS DE TRATAMIENTO |

RELACIONES ENTRE LOS RESPONSABLES DE TRATAMIENTO Y LOS ENCARGADOS DE TRATAMIENTO:

Normativa actual (LOPD y RLOPD)

La LOPD establecía que la relación entre el Responsable del Fichero y el Encargado de Tratamiento se regulaba a través de un contrato de prestación de servicios con acceso a datos (Contrato de Encargado de Tratamiento en base al artículo 12 de la LOPD).

Normativa de aplicación a partir del 25 de Mayo de 2018 (Reglamento General de Protección de Datos (RGPD) y Nueva Ley Orgánica de Protección de Datos de Carácter Personal)

El RGPD introduce nuevas obligaciones para los encargados de tratamiento en determinados supuestos.
A modo de ejemplo, los Encargados de tratamiento:

- Deben mantener un registro de actividades de tratamiento.
- Determinar las medidas de seguridad aplicables a los tratamientos que realizan.
- Designar un Delegado de Protección de Datos en los casos previstos.

Un ejemplo de Encargado de tratamiento es la asesoría fiscal, una empresa de mantenimiento informático o empresa de mantenimiento de página web.

La elección del Encargado del tratamiento por parte del Responsable del tratamiento debe garantizar que el Encargado está en condiciones de cumplir con la aplicación de las medidas técnicas y organizativas apropiadas y deberemos asegurarnos que este Encargado de tratamiento cumple con lo establecido con el RGPD y la Nueva LOPD. Las obligaciones entre Responsable del tratamiento y el Encargado deben figurar en un nuevo modelo de contrato donde se deben definir el tipo de datos a los que va a acceder.

El contenido mínimo del contrato debe prever los siguientes aspectos:

- Objeto, duración, naturaleza y la finalidad del tratamiento;
- Tipo de datos personales y categorías de interesados;
- Obligación del encargado de tratar los datos personales únicamente siguiendo; instrucciones documentadas del Responsable;
- Condiciones para que el Responsable pueda dar su autorización previa, específica o general, a las subcontrataciones;
- Asistencia al Responsable, siempre que sea posible, en la atención al ejercicio de derechos de los interesados...

| 9. CATEGORÍAS ESPECIALES DE DATOS |

Normativa actual (LOPD y RLOPD)

El artículo 7 de la LOPD establecía como datos especialmente protegidos:

– Origen étnico o racial.
– Opiniones políticas.
– Convicciones religiosas o filosóficas.
– Datos relativos a la salud (Recogido específicamente en el artículo 8 de la LOPD)
– Datos relativos a la vida y orientación sexuales.

Normativa de aplicación a partir del 25 de Mayo de 2018 (Reglamento General de Protección de Datos (RGPD) y Nueva Ley Orgánica de Protección de Datos de Carácter Personal)

Con el RGPD y la Nueva LOPD, cambia la denominación y pasan a llamarse "Categorías especiales de datos" donde se incorporan dos nuevas tipologías de datos:

a) Datos genéticos.
b) Datos biométricos que permitan la identificación unívoca de una persona.
c) Por tanto, el catálogo completo de Categorías especiales de datos se recoge en el artículo 9 del RGPD y en el artículo 9 de la Nueva LOPD:

– Origen étnico o racial.
– Opiniones políticas.
– Convicciones religiosas o filosóficas.
– Datos relativos a la salud
– Datos relativos a la vida y orientación sexuales.
– Datos genéticos.
– Datos biométricos que permitan la identificación unívoca de una persona.

| 10. SANCIONES |

Normativa actual (LOPD y RLOPD)

La LOPD establecía una serie de sanciones económicas para los titulares de los ficheros para los casos en que los responsables de los mismos y los encargados de su tratamiento incurran en infracciones.

En el **cuadro 1**, se recoge la clasificación de infracciones y la cuantía de las sanciones actuales:

CUADRO 1	
Infracción	Sanción
Leve	900 € a 40.000 €
Grave	de 40.001 € a 300.000 €
Muy grave	de 300.001 € a 600.000 €

CUADRO 2	
Infracción	Sanción
Leve	No se establece un rango mínimo de cuantía
Grave	Multas administrativas de 10 000 000 € como máximo o, si es una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, eligiendo la de mayor cuantía.
Muy grave	Multas administrativas de 20 000 000 € como máximo o, si es una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, eligiendo la de mayor cuantía.

Normativa de aplicación a partir del 25 de Mayo de 2018 (Reglamento General de Protección de Datos (RGPD) y Nueva Ley Orgánica de Protección de Datos de Carácter Personal)

En los artículos 83 y 84 del RGPD y los artículos 70 y siguientes de la Nueva LOPD se establece el nuevo régi men de sanciones e infracciones en materia de Protección de Datos de carácter personal. Se exponen los cambios más significativos en el **cuadro 2**. El régimen sancionador incorpora una mecanismo de advertencias y apercibimientos en casos de denuncias.

11. RESUMEN DE PAUTAS ORIENTATIVAS DE ACTUACIONES A REALIZAR PARA LA ADECUACIÓN AL REGLAMENTO/LEY ORGÁNICA ANTES DEL 25 DE MAYO DE 2018

1. NOMBRAMIENTO DEL DPO: Obligatorio para Consejo/ Colegios, así como para las farmacias y establecimientos sanitarios, laboratorios, en los supuestos específicos en los que entre sus actividades principales traten categorías especiales de datos a gran escala. Sería conveniente nombrar un DPO en el resto de supuestos y se podría utilizar la fórmula del DPO compartido ya analizada en la presente guía.
   Una vez nombrado el DPO, tendremos que:
   – Hacer pública su designación y sus datos de contacto.
   – Comunicación a la AEPD.
   – Establecimiento del procedimiento para que los interesados puedan contactar con el Delegado de Protección de Datos.

2. ELABORACIÓN DEL REGISTRO DE ACTIVIDADES: afecta al Consejo, COFs y a las farmacias y otros centros y establecimientos sanitarios (laboratorios, ortopedias, ópticas...) que realicen tratamiento de datos que puedan entrañar un riesgo para los derechos y libertades de los interesados o de categorías especiales de datos (de salud, biométricos o genéticos....). Dicho registro deberá conservarse a disposición de la AEPD y publicarse en nuestra página web para cumplir con el principio de transparencia. Puede obtener un modelo de registro de actividad consultando la guía de Análisis de Riesgos publicada en la web de la Agencia Española de Protección de Datos.

3. REALIZAR UN ANÁLISIS DE RIESGOS Y UNA EVALUACIÓN DE IMPACTO SOBRE LA PROTECCIÓN DE DATOS DE LOS FICHEROS QUE TRATAMOS PARA: Revisar y valorar si los tratamientos presentan alto riesgo para los derechos y libertades de los interesados y comprobar, si tenemos las medidas adecuadas a las exigencias del Reglamento o deben implementarse medidas adicionales como auditorías de protección de datos periódicas en función del resultado del análisis de riesgos y si debemos realizar una evaluación de impacto. Si desea más información sobre análisis de riesgos y evaluaciones de impacto, puede consultar las guías de Análisis de Riesgos y Evaluación de Impacto en la Protección de Datos Personales publicadas en la web de la Agencia Española de Protección de Datos.

4. REVISAR LOS DATOS DE CARÁCTER PERSONAL QUE SE TRATAN PARA COMPROBAR: La Legitimación del tratamiento: si se tiene base legal para el tratamiento sin consentimiento o si ha existido consentimiento previo recabado de forma acorde al RGPD.
   – Si es obtenido el consentimiento para el tratamiento de los datos, comprobar: Si para recabar el consentimiento, se ha facilitado la debida y necesaria información mediante la colocación de un cartel informativo (cartel de aviso legal, cartel de videovigilancia etc...). Verificar que hemos obtenido el consentimiento expreso para tratar datos relativos a fidelización de clientes, datos a través de página web....
   – Si el consentimiento otorgado se ajusta o no al tipo de datos que se recaban y comprobar: que no se ha facilitado por silencio, casillas ya marcadas o por inacción; los formularios donde se ha otorgado para ver si está ajustado a su finalidad; Si se ha solicitado para varias finalidades y se ha otorgado para cada una de ellas; que se ha dado de forma inequívoca, mediante acto afirmativo claro que refleje manifestación libre e informada del interesado; de manera lícita, leal y transparente; si se están tratando durante el tiempo necesario y si se tienen que seguir o no conservando así como si hay datos excesivos o no ajustados a la finalidad.

5. REALIZAR UNA VALORACIÓN DE LA RELACIÓN CON LOS ENCARGADOS DE TRATAMIENTO QUE TENEMOS PARA COMPROBAR: Si ofrecen garantías de cumplimiento del RGPD y la Nueva LOPD.
   – Revisión de los contratos para poder adecuarlos al cambio normativo.

6. ESTABLECIMIENTO DE MECANISMOS PARA LA IDENTIFICACIÓN CON RAPIDEZ DE VIOLACIONES DE SEGURIDAD: Establecimiento de medidas de reacción frentes a los diferentes tipos de quiebras de seguridad.
   – Establecimiento de procedimientos de notificación de violaciones de seguridad a la AEPD y, si fuera necesario, a los afectados.
   – Establecimiento de un registro o herramienta de documentación de los incidentes de seguridad.

Consejo General
de Colegios Oficiales
de Farmacéuticos