COLEGIO OFICIAL
DE VETERINARIOS
DE MADRID

MANUAL DE RECOMENDACIONES PARA LA ADECUACIÓN DE LOS CENTROS DE MEDICINA VETERINARIA A LA VIGENTE NORMATIVA DE PROTECCIÓN DE DATOS

ÍNDICE

1. PRESENTACIÓN

El objetivo del presente MANUAL es ofrecer una herramienta de ayuda a las clínicas y los profesionales veterinarios a cumplir con la legalidad vigente de protección de datos personales.

No ha sido nuestra pretensión abordar toda la problemática de la abundante materia en protección de datos, sino incidir en aspectos que pueden tener mayor relevancia y aplicación práctica en la actividad desempeñada por los profesionales veterinarios.

Nos parece de gran interés explicar a los colegiados, cómo afecta esta normativa a su actividad profesional, cual es su ámbito de aplicación así como cuales son las principales obligaciones dimanantes de esta normativa.

En este sentido, para elaborar este MANUAL se han utilizado informes de la Agencia Española de Protección de Datos, así como las consultas expuestas por los profesionales veterinarios al Colegio Oficial de Veterinarios de Madrid.

Para facilitar la compresión de los conceptos de la normativa de protección de datos y aclarar definiciones que en algunas ocasiones pueden resultar bastante complejas, después de cada apartado se han incluido preguntas frecuentes.

2. ACRÓNIMOS Y DEFINICIONES

2.1. ACRÓNIMOS

- AEPD: Agencia Española de Protección de Datos.
- LOPD: Ley Orgánica de Protección de Datos.
- RGPD: Registro General de Protección de Datos.
- RLOPD: Reglamento de Desarrollo de la LOPD.

2.2. DEFINICIONES

- ***Afectado o interesado:*** *Persona física titular de los datos que sean objeto del tratamiento.*
- ***Cancelación:*** *Procedimiento en virtud del cual el responsable cesa en el uso de los datos. La cancelación implicará el bloqueo de los datos, consistente en la identificación y reserva de los mismos con el fin de impedir su tratamiento excepto para su puesta a disposición de las Administraciones Pública, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento y sólo durante el plazo de prescripción de dichas responsabilidades. Transcurrido ese plazo deberá procederse a la supresión de los datos.*
- ***Cesión o comunicación de datos:*** *tratamiento de datos que supone su revelación a una persona distinta del interesado.*
- ***Consentimiento del interesado****: toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.*
- ***Dato disociado:*** *aquél que no permite la identificación de un afectado o interesado.*
- ***Datos de carácter personal:*** *cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables.*

- ***Datos de carácter personal relacionados con la salud:*** *las 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 a su información genética.*

- ***Destinatario o cesionario:*** *la persona física o jurídica, pública o privada u órgano administrativo, al que se revelen los datos.*

  Podrán ser también destinatarios los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

- ***Encargado del tratamiento:*** *la persona física o jurídica, pública o privada, u órgano administrativo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento o del responsable del fichero, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio.*

  Podrán ser también encargados del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

- ***Exportador de datos personales:*** *la persona física o jurídica, pública o privada, u órgano administrativo situado en territorio español que realice una transferencia de datos de carácter personal a un país tercero.*

- ***Fichero:*** *todo conjunto organizado de datos de carácter personal, que permita el acceso a los datos con arreglo a criterios determinados, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.*

- ***Ficheros de titularidad privada:*** *los ficheros de los que sean responsables las personas, empresas o entidades de derecho privado, con independencia de quien ostente la titularidad de su capital o de la procedencia de sus recursos económicos, así como los ficheros de los que sean responsables las corporaciones de derecho público, en cuanto dichos ficheros no se encuentren estrictamente vinculados al ejercicio de potestades de derecho público que a las mismas atribuye su normativa específica.*

- ***Ficheros de titularidad pública:*** *los ficheros de los que sean responsables los órganos constitucionales o con relevancia constitucional del Estado o las*

instituciones autonómicas con funciones análogas a los mismos, las Administraciones públicas territoriales, así como las entidades u organismos vinculados o dependientes de las mismas y las corporaciones de derecho público siempre que su finalidad sea el ejercicio de potestades de derecho público.

- ***Fichero no automatizado**: todo conjunto de datos de carácter personal organizado de forma no automatizada y estructurado conforme a criterios específicos relativos a personas físicas, que permitan acceder sin esfuerzos desproporcionados a sus datos personales, ya sea aquél centralizado, descentralizado o repartido de forma funcional o geográfica.*
- ***Fuentes accesibles al público**: Exclusivamente tendrán esta consideración: el censo promocional; las guías de servicios de comunicaciones electrónicas; listas de personas pertenecientes a grupos de profesionales; los diarios y boletines oficiales; y los medios de comunicación social.*
- ***Importador de datos personales**: la persona física o jurídica, pública o privada, u órgano administrativo receptor de los datos en caso de transferencia internacional de los mismos a un tercer país, ya sea responsable del tratamiento, encargada del tratamiento o tercero.*
- ***Persona identificable:** toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social. Una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionados.*
- ***Procedimiento de disociación:** todo tratamiento de datos personales que permita la obtención de datos disociados.*
- ***Responsable del fichero o del tratamiento**: persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que sólo o conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente.*

  Podrán ser también responsables del fichero o del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

- ***Tercero:*** *la persona física o jurídica, pública o privada u órgano administrativo distinta del afectado o interesado, del responsable del tratamiento, del responsable del fichero, del encargado del tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable del tratamiento o del encargado del tratamiento.*

  Podrán ser también terceros lo entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

- ***Transferencia internacional de datos:*** *tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo, bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español.*

- ***Tratamiento de datos:*** *cualquier operación o procedimiento técnico, sea o no automatizado, que permita la recogida, grabación, conservación, elaboración, modificación, cancelación, bloqueo o supresión, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.*

3. NORMATIVA APLICABLE Y SU OBJETO.

El fundamento de la vigente normativa de protección de datos personales constituye:

- Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa al tratamiento de datos personales y a la libre circulación de estos datos.
- **Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal** (en adelante **LOPD**).
- **Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de Desarrollo de la LOPD** (en adelante **RLOPD**).

Asimismo son de destacar las dos Sentencias del Tribunal Constitucional 290/2000 y 292/2000, que han definido y delimitado el contenido esencial del derecho a la protección de datos como un derecho fundamental.

Para aquellas clínicas que disponen de sistemas de videovigilancia sería de aplicación también la Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras.

4. OBJETO Y ÁMBITO DE APLICACIÓN DE LA NORMATIVA DE PROTECCIÓN DE DATOS

El objeto principal de la LOPD es garantizar y proteger, en lo que concierne al tratamiento de los datos de carácter personal, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar.

Con el fin de determinar el ámbito de aplicación de la normativa de protección de datos, debemos aclarar algunos conceptos y explicar qué es un dato personal, cómo se define el fichero, qué se entiende por tratamiento de datos personales y quién es el Responsable del Fichero.

¿Por qué las clínicas veterinarias deben cumplir con la normativa de protección de datos?

Las clínicas veterinarias como cualquier otra empresa en su actividad recaban datos personales de clientes (propietarios de los animales), proveedores, personal etc. que son susceptibles del tratamiento y/o pueden formar parte los respectivos ficheros de su responsabilidad, por lo que le es de aplicación la normativa de protección de datos.

4.1. QUÉ SON LOS DATOS DE CARÁCTER PERSONAL

El dato de carácter personal constituye "**cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables**".

Como se ha dicho con anterioridad, las clínicas recogen diferentes datos personales relativos a sus clientes – propietarios de los animales, proveedores o empleados, por ejemplo: nombres y apellidos, dirección postal o electrónica, número de teléfono, firma, DNI o documento equivalente, número de cuenta corriente etc. Podrán recoger también otro tipo de datos como las imágenes captadas por las cámaras de videovigilancia o los datos de los internautas que se registren a través de las páginas Web. Todos estos datos por muy básicos que sean cuando permiten

identificar a la persona quedan protegidos por la LOPD y su normativa de desarrollo.

¿Los historiales clínicos de los animales recogen datos personales?

La normativa de protección de datos se aplica exclusivamente a las personas físicas por lo que los historiales clínicos por contener datos de los animales quedan fuera de su aplicación.

¿Si una clínica recoge solamente datos de nombre y apellidos de los propietarios de los animales, le son aplicables los protocolos a seguir por la LOPD?

Sí, puesto que nombre y apellidos son datos relativos a las personas físicas y suficientes para identificarlas.

4.2. QUÉ ES UN FICHERO

Coloquialmente se identifica el concepto de "fichero" con una base de datos alojada en un programa informático o un archivo documental, no obstante su definición legal es mucho más amplia y compleja. Conforme a la vigente normativa se considera un fichero "**todo conjunto organizado de datos de carácter personal, que permita el acceso a los datos con arreglo a criterios determinados, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso**".

En la práctica las clínicas pueden poseer diferentes ficheros en los que se recojan datos correspondientes a sus CLIENTES (propietarios de los animales), PROVEEDORES, PERSONAL (propio o ajeno), CANDIDATOS que participan en los procesos de selección (datos incluidos en curriculum vitae, etc), VIDEOVIGILANCIA (si se realizan las grabaciones de las cámaras de seguridad), o USUARIOS WEB (internautas que se registran en las páginas Web de las clínicas). Los ficheros dependiendo del soporte en que están almacenados los datos, pueden ser **automatizados** o **no automatizados**. Los datos alojados en los servidores, ordenadores personales o portátiles, discos duros externos, CD, DVD, pendrive, etc. constituyen ficheros automatizados y la documentación en papel como contratos o facturas formaría parte de los ficheros denominados no automatizados. No obstante también es posible que en un mismo fichero se pueda englobar ambos recursos tanto automatizados como no automatizados, por ejemplo en el caso del fichero

CLIENTES sus datos pueden ser recogidos en soporte de papel (facturas) e informático (una hoja Excel con el listado de clientes o facturas digitalizadas).

Por consiguiente, el fichero, tal y como lo define la LOPD, no tiene por qué tener una única ubicación física siendo posible su distribución en diferentes lugares, siempre y cuando la organización y sistematización de los datos responda a un conjunto organizado y uniformado de datos de acuerdo con un criterio lógico y gestionado de forma centralizada.

A diferencia de los ficheros **públicos** gestionados por las Administraciones o Entidades Públicas, los ficheros de las clínicas veterinarias son **privados** y la principal obligación dimanante de la existencia de estos ficheros es su inscripción en el Registro General de Protección de Datos (RGPD) dependiente de la Agencia Española de Protección de Datos (AEPD).

¿Deberían inscribir las clínicas el fichero de PACIENTES (relativo a los animales)?

Como ya se ha dicho con anterioridad, la LOPD garantiza y protege los derechos de las personas físicas y no de los animales por tanto a efectos de la normativa de protección de datos no sería necesario inscribir tal fichero. Sí que existe un fichero vinculado a éste, el de propietarios de los animales que serían CLIENTES de las clínicas veterinarias.

¿Si una clínica recoge datos personales de carácter público, por ejemplo apellidos, direcciones, teléfonos incluidos en las guías telefónicas, también debe declarar estos archivos?

Siempre que estos datos correspondan a las personas físicas (nunca jurídicas) y se recogiesen por las clínicas en el marco de sus actividades, formarían parte de un fichero y por tanto existiría la obligación de inscribirlo ante el RGPD.

4.3. EL TRATAMIENTO DE DATOS PERSONALES

Conforme la definición ofrecida por la LOPD "**cualquier operación o procedimiento técnico, sea o no automatizado, que permita la recogida, grabación, conservación, elaboración, modificación, cancelación, bloqueo o supresión, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias**" se considera un tratamiento de datos personales. En consecuencia la simple conservación de la documentación con

datos personales o información alojada en los discos duros de los equipos informáticos supone un tratamiento de datos personales.

¿Cuándo una clínica tenga instaladas las cámaras de videovigilancia pero no realiza las grabaciones, esto implica el tratamiento de datos personales?

Sí, puesto que la simple visualización de las imágenes supone un tratamiento de datos personales y por tanto la clínica tiene que cumplir con las obligaciones derivadas de la normativa de protección de datos.

¿Se debería registrar un fichero en estos casos?

Puesto que no se hacen las grabaciones, la información no queda almacenada en ningún soporte y por tanto no formaría ningún fichero. Hay que tener en cuenta que se registran los ficheros pero no los tratamientos.

No obstante, como se ha dicho con anterioridad, la visualización de las imágenes, sí que supone un tratamiento de datos, por lo que se debería que cumplir con otras normas de protección de datos como por ejemplo con el deber de informar a los interesados utilizando generalmente en estos casos, los carteles informativos.

4.4. LA CLÍNICA COMO RESPONSABLE DEL FICHERO O DEL TRATAMIENTO

La LOPD define como el Responsable del Fichero o Tratamiento a toda "**persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que sólo o conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente**".

Normalmente, estas funciones asume la propia clínica y ésta sería la Responsable del Fichero o Tratamiento respecto de los ficheros de su titularidad.

La designación de la clínica, y no una determinada persona o puesto dentro de la organización, como Responsable del Fichero o del Tratamiento tiene su especial importancia a efectos del ejercicio de los derechos de los afectados y de las funciones de inspección y sanción por el órgano de control.

¿Se podría designar como Responsable del Fichero por ejemplo al director de la clínica?

Sí, pero esto puede tener unas consecuencias bastante perjudiciales. Por ejemplo, si la clínica cometiera alguna infracción derivada de la normativa de protección de datos y la AEPD la sancionase, siendo el Responsables del Fichero una persona física respondería con todo su patrimonio.

4.5. ENCARGADO DE TRATAMIENTO

La normativa de protección de datos define al **Encargado de Tratamiento** como un tercero, que con ocasión de prestar determinados servicios al Responsable del Fichero tiene acceso a datos personales de su responsabilidad, como consecuencia de una relación jurídica.

Además, La LOPD y su reglamento de desarrollo obliga a que esta relación jurídica entre el Responsable y el Encargado de tratamiento sea regulada mediante un contrato por escrito con el fin de delimitar el ámbito de actuación para la prestación de un servicio.

El ejemplo más paradigmático de un Encargado de Tratamiento podría ser la gestoría laboral que confecciona las nóminas al personal de la clínica o una empresa de seguridad que supervisa las grabaciones de las imágenes captadas por las cámaras de videovigilancia.

¿Si una clínica contrata a una empresa informática que realiza el mantenimiento de su sistema operativo, tiene que firmar con esta empresa el contrato en los términos arriba expuestos?

Sí, este podría ser otro ejemplo de un Encargado de Tratamiento puesto que la empresa informática para hacer el mantenimiento del sistema operativo probablemente tendría que acceder a los ficheros con datos personales de la clínica.

5. LAS OBLIGACIONES DIMANANTES DE LA NORMATIVA Y PRINCIPIOS GENERALES DE LA PROTECCIÓN DE DATOS

5.1. DEBER DE INSCRIPCIÓN DE FICHEROS

Toda creación de un fichero de datos de carácter personal debe ser notificada previamente al Registro dependiente de la AEPD.

Además la normativa obliga a que la inscripción del fichero se encuentre actualizada en todo momento, por lo que cualquier modificación que afecte al contenido de la inscripción de un fichero habrá que notificar igualmente al RGPD.

Asimismo, cuando se decida suprimir el fichero, deberá notificarse al Registro su cancelación.

Para realizar la inscripción inicial del fichero así como su posterior modificación o supresión se debe utilizar un formulario denominado NOTA que proporciona la AEPD a través de su página Web. Las solicitudes deberían efectuarse en formulario electrónico NOTA (titularidad privada).

Este formulario permite la presentación de forma gratuita de las notificaciones a través de Internet con o sin el certificado de firma electrónica. En caso de no disponer de un certificado de firma electrónica se puede presentar la notificación a través de Internet, y después remitir a la AEPD la hoja de solicitud con su correspondiente código óptico de lectura debidamente firmada. Se puede optar por entregar dicha hoja de solicitud personalmente en los locales de la AEPD, enviándola por el correo ordinario a la dirección C/ Jorge Juan 6 en Madrid o por fax al número 914483680.

¿Quiénes o cuándo están obligadas las clínicas a dar de alta ficheros a la Agencia?

La LOPD indica que previamente a la creación de los ficheros con datos personales hay que inscribirlos en el RGPD. Las clínicas veterinarias como todas las empresas en su actividad recaban datos que forman los ficheros. Por tanto, en la práctica deberían tener inscritos los respectivos ficheros desde el mismo momento de su constitución como empresa.

¿Ante qué organismo se debe presentar la documentación, La Agencia autonómica o la estatal?

Las clínicas como empresas de derecho privado tienen que registrar los ficheros ante el Registro General de Protección de Datos dependiente de la Agencia estatal (AEPD). Las Agencias autonómicas registran solamente ficheros públicos.

5.2. PRINCIPIO DE CALIDAD

Este principio, fundamentalmente, implica que las clínicas:

- No deben recoger datos excesivos. Por ejemplo, recabar el dato de número de tarjeta de crédito de un cliente cuando no se van a realizar pagos con esta tarjeta.
- No deben tratar los datos para finalidades distintas de las que hayan informado a los afectados. Por ejemplo, utilizar la información relativa a sus clientes para hacer envíos comerciales cuando éstos no lo solicitasen.
- No deben mantener datos desactualizados ni incorrectos. Por ejemplo, no realizar las rectificaciones de datos, después de recibir la correspondiente comunicación por parte del cliente o mantener datos curriculares de forma indefinida, sin actualizar.
- No deben mantener datos por tiempo superior al mínimo indispensable para el cumplimiento de la finalidad. Por ejemplo, guardar datos de los ex empleados indefinidamente.
- Los datos se deben mantener debidamente organizados, de forma que el responsable pueda facilitar toda la información relativa a cada uno de sus clientes o trabajadores cuando lo solicitasen estas personas.

¿Cuánto tiempo han de guardar las historias clínicas de los animales?

En principio estaríamos fuera de la aplicación de la normativa de protección de datos, salvo que se incluyesen de forma accesoria en estas historias, los datos personales de los propietarios de los animales. En primer lugar habría que verificar la legislación específica que sería de aplicación en estos casos. En cuanto al tiempo de conservación de las historias clínicas, pueden establecerse los respectivos plazos en los códigos deontológicos. Por ejemplo en Titulo V del Código deontológico de COLVEMA se indica que “El veterinario debe conservar los protocolos clínicos y los

elementos materiales de diagnóstico, durante un plazo mínimo de un año desde la última anotación en la historia clínica del paciente". Igualmente pueden existir normas u órdenes emitidos por las Administraciones competentes de las Comunidades autónomas que regularicen estos aspectos.

¿Y las grabaciones captadas por las cámaras de videovigilancia, cuanto tiempo se pueden conservar?

Las grabaciones realizadas por las cámaras de seguridad pueden conservarse durante máximo un mes, conforme se establece en la Instrucción 1/2006 de la AEPD.

5.3. DEBER DE INFORMACIÓN

Este principio obliga a las clínicas como Responsables del Fichero, en el momento de la recogida de los datos, a informar a los afectados:

- De la inclusión de sus datos en un fichero titularidad del Responsable del Fichero.
- De los posibles destinatarios de los datos.
- De la finalidad del tratamiento.
- Del carácter obligatorio o facultativo de la información solicitada.
- De la posibilidad de ejercer sus derechos de acceso, rectificación, cancelación y oposición.
- De la identidad y dirección del Responsable del Fichero.

Para cumplir con el deber de información, las empresas incluyen en la documentación, formularios etc. cláusulas informativas de protección de datos. Por ejemplo, para con los clientes, las clínicas podrían insertar en los contratos y/o facturas la siguiente cláusula informativa:

"Sus datos están incluidos en un fichero responsabilidad de [INDICAR RAZÓN SOCIAL DE LA CLÍNICA], con domicilio en: [INDICAR EL DOMICILIO], con la finalidad de gestionar la relación comercial. Podrá ejercer sus derechos de acceso, rectificación, cancelación y oposición a través de comunicación escrita a la dirección indicada aportando fotocopia de su DNI o documento equivalente y concretando su solicitud".

Con carácter general, si las clínicas no obtuviesen los datos directamente de los afectados, deberían en un plazo de 3 meses informarles de los extremos antes expuestos.

En el caso de que las clínicas instalen las cámaras de videovigilancia deberían informar igualmente a los interesados de este tipo de tratamiento. En este sentido, se deberán ubicar en las entradas a las instalaciones, los cárteles informativos con el logotipo de la cámara de seguridad. Además, las clínicas deberán disponer de los impresos con toda la información necesaria.

A continuación se indica el modelo del cartel informativo de videovigilancia.

ZONA VIDEOVIGILADA

LEY ORGÁNICA 15/1999, DE PROTECCIÓN DE DATOS

PUEDE EJERCITAR SUS DERECHOS ANTE:

[INDICAR RAZÓN SOCIAL DE LA CLÍNICA]

[INDICAR EL DOMICILIO DE LA CLÍNICA],

¿Dónde deberían estar ubicadas las cámaras de videovigilancia?

Las cámaras no deberían captar las imágenes de vías públicas así como espacios protegidos por el derecho de la intimidad como baños o vestuarios.

5.4. OBTENCIÓN DEL CONSENTIMIENTO

Este principio va íntimamente ligado con el deber de información, pues una vez informado, el afectado deberá consentir de forma inequívoca al tratamiento de sus datos. Este consentimiento no será necesario cuando:

- Una Ley disponga lo contrario. Por ejemplo, la legislación laboral obliga a los empresarios a mantener la información relativa a sus empleados incluso una vez finalizada la relación laboral o tratándose de historias clínicas los profesionales están obligados legalmente a mantener entre otras, la información relativa a los titulares de los animales.
- Los datos se recojan para el ejercicio de las funciones propias de las Administraciones Públicas. Por ejemplo la información de los contribuyentes gestionada por AEAT o la relativa a los colegiados mantenida por los Colegios profesionales.
- Los datos se refieran a las partes de un contrato o precontrato de una relación civil, mercantil, laboral o administrativa y sean necesarios para el mantenimiento de dicha relación. Por ejemplo los datos de los clientes de las clínicas que sean necesarios para el mantenimiento de una relación comercial. No obstante aunque el consentimiento esté implícito en la relación contractual, sí que persiste el deber de información por eso incluso en los contratos se deberían incluir las cláusulas de protección de datos.
- Se trate datos de salud necesarios para proteger un interés vital del interesado.
- Los datos hayan sido obtenidos de fuentes accesibles al público[1].

En estos casos, el afectado podrá oponerse al tratamiento siempre que una Ley no diga lo contrario, y tenga motivos fundados para ello.

En los demás supuestos, el afectado podrá revocar el consentimiento prestado de forma justificada en cualquier momento, pero sin efectos retroactivos.

¿Para publicar las fotografías de las mascotas de mis clientes en un tablón de la clínica, necesito su autorización?

Tratándose de animales no se aplicaría la LOPD pero si en estas fotografías apareciesen sus dueños debería contarse con su consentimiento.

5.5. DATOS ESPECIALMENTE PROTEGIDOS

Este principio trata de garantizar un mayor control por parte de los afectados de sus datos más sensibles. A la gran mayoría de las clínicas no afectará este principio, pero en algunos casos puede que las clínicas gestionen alguno de los datos abajo tipificados como especialmente protegidos.

El Responsable del Fichero deberá recabar:

- Consentimiento expreso: para poder tratar los datos relacionados con:
    - origen racial;
    - salud;
    - vida sexual.
- Consentimiento expreso y por escrito: para poder tratar los datos relacionados con [1]:
    - ideología;
    - afiliación sindical;
    - religión y creencias.

Es posible que los profesionales veterinarios traten la información con datos de salud como consecuencia de los accidentes ocurridos en la clínica. En el caso de que toda la información la comunicasen a una mutua o compañía de seguros, sería ésta la responsable de aplicar las medidas de protección de nivel alto, pero si además esta información se recopilase por la propia clínica, también ésta tendría que implementar las correspondientes medidas de seguridad.

¿Han de ser considerados datos de salud los relativos a la enfermedad común y accidente profesional?

[1] Según el artículo 16.2 de la Constitución Española de 1978, "*nadie podrá ser obligado a declarar sobre su ideología, religión o creencias*".

Es criterio reiterado de la Agencia que en cuanto el fichero pueda contener datos relativos a las fechas de baja o alta de trabajadores, asociadas a un código que permita la identificación de la causa de la baja como motivada por enfermedad común, profesional o maternidad, estaremos en presencia de un dato de salud que implicará la necesidad de aplicar a dicho fichero medidas de seguridad de nivel alto.

No sería así, por ejemplo, si figuran únicamente las fechas y la indicación de "baja" u otros supuestos análogos de los que no pueda fácilmente deducirse que la baja se debe a algún tipo de enfermedad.

5.6. NIVELES DE SEGURIDAD Y MEDIDAS TÉCNICAS DE PROTECCIÓN DE LOS DATOS

Este principio obliga a la adopción de un catálogo de medidas técnicas y organizativas que garanticen la seguridad de los datos tal y como se indica en el Título VIII del RLOPD.

Las clínicas están obligadas a disponer de un **documento de seguridad** en que se recogiesen todos los procedimientos y medidas de índole técnica y organizativas necesarias para garantizar la seguridad de los datos de carácter personal y evitar su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que estén expuestos, ya provengan de la acción humana o del medio físico o natural.

Para cumplir con esta exigencia legal, la AEPD facilita el modelo del documento de seguridad a través de su la página Web que podrá adaptarse a las necesidades de cada una de las empresas o, en su caso, las clínicas podrán contratar servicios de las consultoras especializadas para su elaboración.

Dependiendo del carácter de los datos recogidos en los ficheros de las clínicas se aplicarían diferentes niveles de seguridad, BÁSICO, MEDIO O ALTO. La aplicación de estos niveles tiene forma escalonada y acumulativa en atención a la especial sensibilidad de algunos datos. Las medidas de seguridad calificadas de nivel básico deberán adoptarse a todos los ficheros o tratamientos de datos de carácter personal. A los datos de nivel medio deberán adoptarse además de las medidas de este nivel también las del nivel básico y a los datos especialmente protegidos se adoptarán las medidas de nivel alto, medio y básico.

En la siguiente tabla se indican diferentes tipos de datos y niveles de protección que les corresponden:

NIVEL BÁSICO	NIVEL MEDIO	NIVEL ALTO
• Nombre y apellidos • DNI/NIE • Firma • Dirección • Teléfono • Email • Foto • Cuenta bancaria • Número de tarjeta de crédito • Estado civil • Fecha de nacimiento • Lugar de nacimiento • Sexo • Nacionalidad • Lengua materna • Licencias, permisos, autorizaciones… • CV, formación, titulaciones, expediente… • Profesión, ocupación, experiencia… • Resto de datos personales a los que no les aplique el Nivel Medio ni el Nivel Alto.	• Multas, infracciones administrativas o penales • Conjuntos de datos que permitan definir la personalidad del individuo • Datos sobre impagos responsabilidad de empresas que prestan servicios de información sobre solvencia patrimonial y crédito • Datos fiscales responsabilidad de las administraciones tributarias • Datos económicos responsabilidad de las entidades financieras • Datos responsabilidad de la Seguridad Social	• Ideología ([2]) • Afiliación sindical ([2]) • Religión ([2]) • Creencias ([2]) • Origen racial ([2]) • Salud ([2]) ([3]) • Vida sexual ([2]) • Violencia de género

A continuación se indican las medidas de seguridad a implantar en diferentes procedimientos, dependiendo del nivel de seguridad aplicable.

MEDIDAS DE SEGURIDAD	NIVEL BÁSICO	NIVEL MEDIO	NIVEL ALTO

([2]) Bastará la implantación de las medidas de seguridad de nivel básico cuando:
a) Los datos se utilicen con la única finalidad de realizar una transferencia dineraria a las entidades de las que los afectados sean socios o miembros; o
b) Cuando sean ficheros no automatizados en los que se recojan estos datos de forma incidental o accesoria sin guardar relación con la finalidad del fichero.

([3]) Podrán implantarse las medidas de seguridad de nivel básico cuando los datos de salud únicamente expresen el grado de discapacidad, o la simple declaración de discapacidad o invalidez, con motivo del cumplimiento de deberes públicos.

MEDIDAS DE SEGURIDAD	NIVEL BÁSICO NIVEL MEDIO NIVEL ALTO		
FUNCIONES Y OBLIGACIONES DEL PERSONAL	• Funciones y obligaciones de los diferentes usuarios o de los perfiles de usuarios claramente definidas y documentadas. • Definición de las funciones de control y las autorizaciones delegadas por CLÍNICA VETERINARIA. • Difusión entre el personal, de las normas que les afecten y de las consecuencias por su incumplimiento.		
REGISTRO DE INCIDENCIAS	• Registro de incidencias: tipo, momento de su detección, persona que la notifica, efectos y medidas correctoras. • Procedimiento de notificación y gestión de las incidencias.	**SÓLO FICHEROS AUTOMATIZADOS** • Anotar los procedimientos de recuperación, persona que lo ejecuta, datos restaurados, y en su caso, datos grabados manualmente. • Autorización para la recuperación de datos.	
CONTROL DE ACCESO	• Relación actualizada de usuarios y accesos autorizados. • Control de accesos permitidos a cada usuario según las funciones asignadas. • Mecanismos que eviten el acceso a datos o recursos con derechos distintos de los autorizados. • Concesión de permisos de acceso sólo por personal autorizado. • Mismas condiciones para personal ajeno con acceso a los recursos de datos.	**SÓLO FICHEROS AUTOMATIZADOS** • Control de acceso físico a los locales donde se encuentren ubicados los sistemas de información.	**SÓLO FICHEROS AUTOMATIZADOS** • Registro de accesos: usuario, hora, fichero, tipo de acceso, autorizado o denegado. • Revisión mensual del registro por el Responsable de Seguridad. • Conservación 2 años. **SÓLO FICHEROS NO AUTOMATIZADOS** • Control de accesos autorizados. • Identificación accesos para documentos accesibles por múltiples usuarios.
IDENTIFICACIÓN Y AUTENTICACIÓN	**SÓLO FICHEROS AUTOMATIZADOS** • Identificación y autenticación personalizada. • Procedimiento de asignación y distribución de contraseñas. • Almacenamiento ininteligible de las contraseñas. • Periodicidad del cambio de contraseñas (<1 año).	**SÓLO FICHEROS AUTOMATIZADOS** • Limite de intentos reiterados de acceso no autorizado.	

MEDIDAS DE SEGURIDAD	NIVEL BÁSICO NIVEL MEDIO NIVEL ALTO		
GESTIÓN DE SOPORTES Y DOCUMENTOS	• Inventario de soportes. • Identificación del tipo de información que contienen, o sistema de etiquetado. • Acceso restringido al lugar de almacenamiento. • Autorización de las salidas de soportes (incluidas a través de email). • Medidas para el transporte y el desecho de soportes.	**SÓLO FICHEROS AUTOMATIZADOS** • Registro de entrada y salida de soportes: documento o soporte, fecha, emisor/destinatario, número, tipo de información, forma de envío, responsable autorizado para recepción/entrega.	**SÓLO FICHEROS AUTOMATIZADOS** • Sistema de etiquetado confidencial. • Cifrado de datos en la distribución de soportes. • Cifrado de información en dispositivos portátiles fuera de las instalaciones (evitar el uso de dispositivos que no permitan cifrado, o adoptar medidas alternativas). **SÓLO FICHEROS NO AUTOMATIZADOS** • Medidas que impidan el acceso o manipulación en su transporte o traslado.
COPIAS DE RESPALDO	**SÓLO FICHEROS AUTOMATIZADOS** • Copia de respaldo semanal. • Procedimientos de generación de copias de respaldo y recuperación de datos. • Verificación semestral de los procedimientos. • Reconstrucción de los datos a partir de la última copia. Grabación manual en su caso, si existe documentación que lo permita. • Pruebas con datos reales. Copia de seguridad y aplicación del nivel de seguridad correspondiente.		**SÓLO FICHEROS AUTOMATIZADOS** • Copia de respaldo y procedimientos de recuperación en lugar diferente del que se encuentren los equipos. **SÓLO FICHEROS NO AUTOMATIZADOS** • Sólo puede realizarse por los usuarios autorizados. • Destrucción de copias desechadas.
CRITERIOS DE ARCHIVO	**SÓLO FICHEROS NO AUTOMATIZADOS** • El archivo de los documentos debe realizarse según criterios que faciliten su consulta y localización para garantizar el ejercicio de los derechos de Acceso, Rectificación, Cancelación y Oposición (ARCO)		

MEDIDAS DE SEGURIDAD	NIVEL BÁSICO NIVEL MEDIO NIVEL ALTO		
ALMACENAMIENTO	**SÓLO FICHEROS NO AUTOMATIZADOS** • Dispositivos de almacenamiento dotados de mecanismos que obstaculicen su apertura.		**SÓLO FICHEROS NO AUTOMATIZADOS** • Armarios, archivadores de documentos en áreas con acceso protegido mediante puertas con llave.
CUSTODIA DE LA DOCUMENTACIÓN	**SÓLO FICHEROS NO AUTOMATIZADOS** • Durante la revisión o tramitación de los documentos, la persona a cargo de los mismos debe ser diligente y custodiarla para evitar accesos no autorizados.		
RESPONSABLE DE SEGURIDAD		• CLÍNICA VETERINARIA tiene que designar a uno o varios responsables de seguridad (no es una delegación de responsabilidad). • El responsable de seguridad es el encargado de coordinar y controlar las medidas del documento.	
AUDITORÍA		• Al menos cada dos años, interna o externa. • Debe realizarse ante modificaciones sustanciales en los sistemas de información con repercusiones en seguridad. • Verificación y control de la adecuación de las medidas. • Informe de detección de deficiencias y propuestas correctoras. • Análisis del responsable de seguridad y conclusiones elevadas al máximo responsable de CLÍNICA VETERINARIA.	
TELECOMUNICACIONES			**SÓLO FICHEROS AUTOMATIZADOS** • Transmisión de datos a través de redes públicas o inalámbricas, cifrando datos o cifrando la red.

¿Es necesario tener una empresa subcontratada para gestionar las tramitaciones derivadas de la LOPD, elaboración del documento de seguridad e implantación de los procedimientos?

No es necesario, pero en la práctica se contrata una consultora, por lo menos en el primer momento para la adecuación.

¿De qué datos y cuándo tienen que hacerse las copias de seguridad?

De todos los datos de carácter personal, independientemente del nivel de protección aplicable, se deberían hacer copias de seguridad por lo menos semanalmente.

¿Dónde deberían guardarse las copias de seguridad?

Deberían guardarse en un lugar con acceso restringido al personal autorizado. En el caso de que se hicieran copias de respaldo con datos especialmente protegidos deberían guardarse en un lugar diferente de aquel en que se encuentran los equipos informáticos que los tratan.

¿Qué personal de la clínica puede tener acceso a la base de datos? ¿Hasta que nivel de protección?

El acceso a los datos no depende solo de su sensibilidad sino de políticas internas de la clínica. Generalmente, las clínicas tratan datos personales de nivel básico de seguridad, pero incluso en estos debería distinguirse diferentes perfiles de usuarios con diferentes permisos de acceso a la información. Por ejemplo los usuarios del área de recursos humanos no tendrían por qué acceder a la información comercial y viceversa. En el caso de que hubiera datos de nivel medio o alto la política de permisos debería ser más estricta.

¿Qué formación y qué conocimientos debe tener el personal sobre la LOPD?

La formación en la LOPD no es obligatoria como por ejemplo, la de Prevención de Riesgos Laborales, pero es recomendable, puesto que es una norma de obligado cumplimiento. Las clínicas manejan diferentes tipos de datos personales y son responsables de las infracciones que cometa su personal.

5.7. DEBER DE SECRETO

El Responsable del Fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos. Por eso es muy importante que el personal de las clínicas tanto interno

como externo se comprometa a cumplir con el deber de confidencialidad que subsistirá aun después de finalizar sus relaciones con el Responsable del Fichero. La forma más adecuada de hacerlo sería que los empleados suscribiesen el correspondiente compromiso de confidencialidad y cumpliesen con las normas de seguridad existentes en la clínica.

¿Se debería firmar algún compromiso de confidencialidad con el personal propio de las clínicas?

El deber de secreto ya lo incluye de forma genérica el Estatuto de los Trabajadores. No obstante es muy recomendable firmar un compromiso de confidencialidad específico y no solamente con el personal propio sino con cualquier persona que podrá acceder a la información cualificada como confidencial.

5.8. COMUNICACIÓN DE DATOS

En la actividad de las clínicas veterinarias surgen situaciones en las cuales el tratamiento de los datos puede ser sometido a cesiones a los laboratorios, otras clínicas y/o particulares. En este sentido la normativa de protección de datos indica que los datos de carácter personal únicamente podrán ser cedidos a terceros con el consentimiento del interesado con indicación expresa de la finalidad de la cesión, salvo algunas excepciones:

- Cuando la cesión esté autorizada en una ley. Por ejemplo, cada Comunidad Autónoma tiene sus leyes de protección de animales que obligan a comunicar los datos de sus propietarios a las autoridades competentes.
- Cuando se trate de datos recogidos de fuentes accesibles al público.
- Cuando la cesión responda a la libre y legítima aceptación de una relación jurídica y sea necesaria para su mantenimiento.
- Cuando tenga por destinatario al Defensor del Pueblo, al Ministerio Fiscal, a Jueces o Tribunales, o al Tribunal de Cuentas en el ejercicio de sus funciones.
- Cuando la cesión se produzca entre Administraciones Públicas. Por ejemplo cesión de datos relativos a los colegiados veterinarios efectuada por los colegios autonómicos al Consejo General de Colegios Veterinarios.

- Cuando sean datos de salud y la cesión sea necesaria para solucionar una urgencia médica o para realizar estudios epidemiológicos.

¿Qué datos se pueden facilitar a terceros?

La norma general indica que para comunicar los datos a terceros hay que contar con su consentimiento, salvo algunas excepciones. Las más importantes serían:

Cuando la Ley obliga a comunicar estos datos a terceros o cuando las comunicaciones son necesarias para el adecuado cumplimiento de una relación contractual.

Las clínicas por ejemplo estarían obligadas por Ley a comunicar los datos identificativos de los propietarios de los animales a las administraciones públicas competentes o los datos de sus empleados a la Tesorería General de la Seguridad Social, Mutuas, AEAT.

Igualmente la relación con los clientes puede obligar a que comuniquen sus datos a los laboratorios o en caso de los empleados a comunicar sus datos a los bancos para pagar sus nóminas.

5.9. ACCESO A DATOS POR CUENTA DE TERCEROS

No se considera comunicación de datos el acceso de un tercero cuando sea necesario para la prestación de un servicio al Responsable del Fichero.

Conforme el artículo 12 de la LOPD, estas prestaciones de servicios deberán estar reguladas en un contrato por escrito, donde el prestador de servicios definido como Encargado de Tratamiento, se obligue de forma expresa a:

- Tratar los datos únicamente conforme a las instrucciones del Responsable del Fichero.
- No utilizarlos con fin distinto del que figure en dicho contrato.
- No comunicarlos, ni siquiera para su conservación, a otras personas.
- Aplicar las correspondientes medidas de seguridad.
- Devolver o destruir los datos cuando se cumpla el objeto del contrato.
- Asumir su responsabilidad por las infracciones en que hubiera incurrido.

- No subcontratar la prestación de los servicios contratados sin la autorización previa del Responsable del Fichero.
- Atender o remitir al Responsable del Fichero las solicitudes de ejercicio de derechos sobre el fichero accedido, que reciba por parte de los afectados.

¿Cuáles serían las consecuencias para la clínica si no se firmase el contrato de prestación de servicios con acceso a datos con un Encargado de Tratamiento?

La transmisión de los datos personales a un encargado del tratamiento sin dar cumplimiento a los deberes formales establecidos en el artículo 12 de la LOPD constituiría una infracción leve.

6. DERECHOS DE LOS AFECTADOS

La normativa vigente en materia de protección de datos, garantiza a los afectados los derechos de acceso, rectificación, cancelación y oposición (ARCO). Estos derechos son personalísimos, y sólo pueden ser ejercidos por sus legítimos titulares o sus representantes legales o voluntarios, aportando siempre documentación acreditativa de su condición. Por lo tanto, deberán ser denegados si no se aportase tal documentación.

- Acceso: Derecho del afectado a saber qué datos están siendo objeto de tratamiento, la finalidad del tratamiento, así como el origen de dichos datos y las comunicaciones realizadas o previstas de los mismos. Para atender este derecho, la clínica cuando recibida la solicitud, tiene la obligación legal de estimar su procedencia en el plazo de 10 días y en el plazo de un mes tendrá que contestar al interesado y hacer efectiva la entrega de la información solicitada. Se deberá siempre conservar una acreditación de haber realizado el envío de la información.
- Rectificación: Derecho del afectado a que se modifiquen los datos que resulten ser inexactos o incompletos.
- Cancelación: Derecho a que se supriman los datos que resulten ser inadecuados o excesivos, sin perjuicio del deber de bloqueo[4].
- Oposición: Derecho a que no se lleve a cabo un determinado tratamiento de los datos de carácter personal o se cese en el mismo.

En caso de derecho de rectificación, cancelación u oposición, la clínica tiene 10 días de plazo para informar al afectado, por cualquier medio que permita acreditar el envío de la comunicación, de que sus datos han sido rectificados/cancelados o de que se ha cesado en el tratamiento al que se hubo opuesto.

[4] Deber de bloqueo: Identificación y reserva de los mismos con el fin de impedir su tratamiento excepto para su puesta a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento y sólo durante el plazo de prescripción de dichas responsabilidades. Transcurrido ese plazo deberá procederse a la supresión de los datos.

¿Los plazos para atender los derechos ARCO se miden en días hábiles o naturales?

Todos los plazos empiezan a contar a partir del día en que se recibe la solicitud dentro de la clínica. Siempre que se hable de días, se entenderán días hábiles; y cuando se hable de meses, se contarán de fecha a fecha.

¿Si una clínica no responde a una solicitud, porque no dispone de ningún dato relativo al interesado supone esto una infracción?

Sí, en todo caso hay que responder al interesado dentro de los plazos estimados legalmente, incluso cuando una solicitud sea improcedente.

7. LAS INFRACCIONES Y EL RÉGIMEN SANCIONADOR

Las infracciones pueden ser las leves, graves y muy graves. La responsabilidad por las infracciones recae en el Responsable del Fichero o Encargado de Tratamiento.

Las infracciones leves:

- No atender la solicitud del interesado de rectificación o cancelación de los datos personales objeto de tratamiento cuando legalmente proceda.
- No proporcionar la información que solicite la AEPD en el ejercicio de sus competencias.
- No solicitar la inscripción del fichero de datos de carácter personal en el Registro General de Protección de Datos, cuando no sea grave.
- Proceder a la recogida de datos de carácter personal de los propios afectados sin cumplir con el deber de información.
- Incumplir el deber de secreto, salvo que constituya infracción grave.

Las infracciones graves:

- Crear ficheros públicos sin disposición publicada en Boletín Oficial.
- Recabar datos sin consentimiento expreso de las personas, en los casos en que éste sea exigible.
- El impedimento de los derechos de acceso y oposición y la negativa a facilitar la información solicitada.
- Mantener datos de carácter personal inexactos o no efectuar las rectificaciones o cancelaciones.
- La vulneración del deber de guardar secreto sobre datos de nivel medio.
- Incumplir las medidas de seguridad.
- No remitir a la AEPD las informaciones que sean requeridas.
- La obstrucción al ejercicio de la función inspectora.
- No inscribir el fichero, cuando haya sido requerido por el Director de la AEPD.

- Incumplir el deber de información cuando los datos hayan sido recabados de persona distinta del afectado.

Las infracciones muy graves:

- La recogida de datos en forma engañosa y fraudulenta.
- La comunicación o cesión de los datos de carácter personal sin habilitación legal o consentimiento.
- Recabar y tratar los datos especialmente protegidos sin el consentimiento debido o habilitación legal.
- No cesar en el uso ilegítimo de los tratamientos de datos cuando sea requerido por el Director de la AEPD o por las personas titulares del derecho de acceso.
- La transferencia internacional a países que no proporcionen un nivel de protección equiparable sin autorización del Director de la AEPD.
- La vulneración del deber de guardar secreto sobre los datos especialmente protegidos.
- No atender, u obstaculizar de forma sistemática el ejercicio de los derechos ARCO.
- No atender de forma sistemática el deber legal de notificación de ficheros a la AEPD.

El régimen sancionador normalmente se aplica en función de las infracciones detectadas:

Sanciones Leves: Multa de 900€ a 40.000€

Sanciones Graves: Multa de 40.001€ a 300.000€

Sanciones Muy Graves: Multa de 300.001€ a 600.000€

La AEPD en determinados casos podrá evitar la apertura de procedimiento sancionador, sustituyéndolo por un apercibimiento.

Los plazos de prescripción de las infracciones son de 1 año para las leves, 2 anos en caso de graves y 3 años en casos de muy graves.

¿Las sanciones por incumplimientos de la LOPD dependen del volumen de negocio o de los archivos?

Las sanciones dependen en gran medida del nivel de seguridad aplicable a los ficheros afectados por alguna infracción. Los datos más sensibles requieren la aplicación de las medidas mas exigentes y estos son también los más castigados. No obstante la reciente aprobación de la Ley de Economía Sostenible introdujo algunos cambios con el objeto de graduar las sanciones y aplicar atenuantes. A partir de su entrada en vigor se tendrá en cuenta también el volumen de negocio del infractor y el esfuerzo realizado en la implantación las medidas de seguridad.