AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

GUÍA PARA LA ADECUACIÓN DE LAS CLÍNICAS Y CONSULTAS PSICOLÓGICAS PROFESIONALES A LA LEY DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

Col·legi Oficial de Psicòlegs
Comunitat Valenciana

Versión 1.0
Diciembre 2008

1. INTRODUCCIÓN

El presente manual tiene como objetivo aportar unas orientaciones para la adecuación de las Clínicas y Consultas Psicológicas profesionales de los colegiados del Ilustre Colegio de Psicólogos de la Comunidad Valenciana a lo dispuesto en la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal (en adelante LOPD) así como a las normas que la desarrollan.

En este documento únicamente se aportan modelos orientativos, por lo que será responsabilidad del psicólogo concreto la adecuación de los mismos a su realidad.

Habrá de tenerse en cuenta que las obligaciones que aquí se mencionan son todas las que le corresponden al psicólogo cumplir pero no se detallan o desarrollan todas por la extensión del presente manual así como por la complejidad de algunas de ellas, que requieren del asesoramiento de profesionales: nos referimos particularmente a la adopción de medidas de seguridad tanto técnicas como organizativas entre las que destaca la redacción del documento de seguridad (que habrá de mantenerse actualizado) así como la realización de la auditoría en materia de protección de datos, a la que después nos referiremos.

ADVERTENCIAS EXPRESAS:

La presente documentación ha sido elaborada por el Ilustre Colegio Oficial de Psicólogos de la Comunidad Valenciana con el único objetivo de que los psicólogos puedan tener unas orientaciones en materia de Protección de Datos por lo que:

1. El Colegio de Psicólogos de la Comunidad Valenciana no será responsable en ningún caso de las obligaciones que cada psicólogo deba cumplir en relación con sus obligaciones en materia de Protección de Datos.

2. Se prohíbe expresamente la utilización de esta documentación por parte de terceros que no estén colegiados así como el uso por parte de colegiados con un fin distinto al cumplimiento de sus obligaciones. Particularmente queda prohibido y se perseguirá el uso de esta documentación para la realización de consultoría o proyectos a terceros. Queda prohibido – por tanto también – el cobro de cantidad de dinero alguna por esta documentación.

2. CONSIDERACIONES GENERALES

2.1. Objeto

La LOPD, en su Art. 1 establece como objetivo *"garantizar y proteger, en lo que concierne a los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar"*. La ley excluye a las personas jurídicas.

2.2. Normativa básica

- *Ley Orgánica 15/1999*, de 13 de diciembre, de Protección de Datos de Carácter Personal).

- *Real Decreto 1720/2007*, de 21 de Diciembre, por el que se aprueba el *Reglamento de desarrollo de la Ley Orgánica 15/99,* de 13 de diciembre, de Protección de Datos de Carácter Personal.

- *Real Decreto 428/1993*, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos.

- *Real Decreto 195/2000*, de 11 de febrero, por el que se establece el plazo para implantar las medidas de seguridad de los ficheros automatizados previstas por el reglamento aprobado por el Real Decreto 994/1999, de 11 de junio.

- Instrucciones y recomendaciones de la Agencia Española de Protección de Datos.

No obstante, los profesionales psicólogos tienen determinadas especialidades en las que entran en juego tanto la *Ley 1/2003* de 28 de enero, de Derechos e Información al Paciente de la Comunidad Valenciana, como la *Ley 41/2002,* de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.

2.3. Definiciones

a) *Afectado o interesado*: Persona física titular de los datos que sean objeto del tratamiento.

b) *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 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.

c) *Cesión o comunicación de datos*: Tratamiento de datos que supone su revelación a una persona distinta del interesado.

d) *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.

e) *Dato disociado*: aquél que no permite la identificación de un afectado o interesado.

f) *Datos de carácter personal*: Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables.

g) *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.

h) *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.

i) *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.

j) *Exportador de datos personales*: la persona física o jurídica, pública o privada, u órgano administrativo situado en territorio español que realice, conforme a lo dispuesto en el presente Reglamento, una transferencia de datos de carácter personal a un país tercero.

k) *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.

l) *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.

m) *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.
n) *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.

ñ) *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.

o) *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.

p) *Procedimiento de disociación*: Todo tratamiento de datos personales que permita la obtención de datos disociados.

q) *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.

r) *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 los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

s) *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.

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

En particular, en relación con lo dispuesto en el título VIII de este reglamento se entenderá por:

a) *Accesos autorizados*: autorizaciones concedidas a un usuario para la utilización de los diversos recursos. En su caso, incluirán las autorizaciones o funciones que tenga atribuidas un usuario por delegación del responsable del fichero o tratamiento o del responsable de seguridad.

b) *Autenticación*: procedimiento de comprobación de la identidad de un usuario.

c) *Contraseña*: información confidencial, frecuentemente constituida por una cadena de caracteres, que puede ser usada en la autenticación de un usuario o en el acceso a un recurso.

d) *Control de acceso*: mecanismo que en función de la identificación ya autenticada permite acceder a datos o recursos.

e) *Copia de respaldo*: copia de los datos de un fichero automatizado en un soporte que posibilite su recuperación.

f) *Documento*: todo escrito, gráfico, sonido, imagen o cualquier otra clase de información que puede ser tratada en un sistema de información como una unidad diferenciada.

g) *Ficheros temporales*: ficheros de trabajo creados por usuarios o procesos que son necesarios para un tratamiento ocasional o como paso intermedio durante la realización de un tratamiento.

h) *Identificación*: procedimiento de reconocimiento de la identidad de un usuario.

i) *Incidencia*: cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos.

j) *Perfil de usuario*: accesos autorizados a un grupo de usuarios.

k) *Recurso*: cualquier parte componente de un sistema de información.

l) *Responsable de seguridad*: persona o personas a las que el responsable del fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables.

m) *Sistema de información*: conjunto de ficheros, tratamientos, programas, soportes y en su caso, equipos empleados para el tratamiento de datos de carácter personal.

n) *Sistema de tratamiento*: modo en que se organiza o utiliza un sistema de información. Atendiendo al sistema de tratamiento, los sistemas de información podrán ser automatizados, no automatizados o parcialmente automatizados.

ñ) *Soporte*: objeto físico que almacena o contiene datos o documentos, u objeto susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar y recuperar datos.

o) *Transmisión de documentos*: cualquier traslado, comunicación, envío, entrega o divulgación de la información contenida en el mismo.
p) *Usuario*: sujeto o proceso autorizado para acceder a datos o recursos. Tendrán la consideración de usuarios los procesos que permitan acceder a datos o recursos sin identificación de un usuario físico.

Artículo 4.1 LOPD:
"Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido".

3. PECULIARIDADES DE LOS PSICÓLOGOS

3.1 Introducción

Caso práctico: Cuando son los propios pacientes los que acuden a la consulta del psicólogo, éste es a todos los efectos, el responsable del fichero, por lo que debe cumplir con todas las obligaciones que marcan tanto la LOPD como el Reglamento de Medidas de Seguridad (en adelante RMS).

Caso práctico 2: Cuando los pacientes acuden derivados de otros compañeros y/o de empresas aseguradoras, los responsables son dos: por un lado el propio psicólogo; y por otro lado el compañero/empresa aseguradora que deriva al paciente, por lo que cada uno debe cumplir con lo que marcan tanto la LOPD como el RMS.

3.2 Obligaciones a cumplir por los psicólogos

De acuerdo con la LOPD y el RMS, los psicólogos deben cumplir, principalmente, con las siguientes obligaciones:

1. Inscripción de los ficheros ante el Registro General de Protección de Datos (Art. 26 LOPD).

2. Cumplir con el deber de información y en los casos que sea necesario, recabar el consentimiento para el tratamiento de los datos (Art. 5, 6 y 7 de la LOPD).

3. Firmar contratos con aquellos terceros que para la prestación de un servicio necesiten acceder a datos de carácter personal titularidad del procurador (Art.12 de la LOPD).

4. Adoptar las medidas técnicas y organizativas (que se detallan en el Capítulo III y IV del RD 1720/2007) necesarias según el nivel de seguridad exigido por el fichero. Por ejemplo, redactar y mantener el Documento de Seguridad (Art. 88 del RD 1720/2007) o someterse a la auditoria en materia de protección de datos (Art. 96 del RD 1720/2007).

5. Formar e informar a sus trabajadores (en el caso de que los tenga) de las funciones y obligaciones que tienen respecto a la Protección de datos.

4. INSCRIPCIÓN DE LOS FICHEROS

Artículo 26 LOPD:
"Toda persona o entidad que proceda a la creación de ficheros de datos de carácter personal lo notificará previamente a la Agencia de Protección de Datos".

Los psicólogos están obligados a inscribir todos los ficheros que contengan datos de carácter personal, sean de tratamiento automatizado (a nivel informático) o bien Ficheros No Automatizados (Ficheros en papel), incluidos aquellos de los que ya se disponía con anterioridad a la entrada en vigor de la Ley Orgánica de Protección de Datos.
Los ficheros habituales que pueda disponer un psicólogo en su consulta serán, por ejemplo, los siguientes:

-AGENDA
-CONTABILIDAD Y FACTURACIÓN
-EMPLEADOS
-PACIENTES
-CURRICULUMS

Forma de cumplir con esta obligación: Para cumplir con esta obligación se puede utilizar el programa de Notificaciones Telemáticas a la AEPD de la propia AGENCIA (Formulario NOTA) (www.agpd.es)

O encargarlo a una empresa que se dedique a la Protección de Datos.

EN RESUMEN:
1. Detectar qué Ficheros se tienen en la consulta.
2. Detectar su sistema de tratamiento.
3. Implantar las medidas de seguridad acorde a los datos que contienen.
4. Inscribirlos en la Agencia de Protección de Datos

5. CONSENTIMIENTO

5.1 Principios generales

Artículo 6.1 LOPD:
"El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa".

1. El responsable del tratamiento deberá obtener el consentimiento del interesado para el tratamiento de sus datos de carácter personal salvo en aquellos supuestos en que el mismo no sea exigible con arreglo a lo dispuesto en las leyes.

La solicitud del consentimiento deberá ir referida a un tratamiento o serie de tratamientos concretos, con delimitación de la finalidad para los que se recaba, así como de las restantes condiciones que concurran en el tratamiento o serie de tratamientos.

2. Cuando se solicite el consentimiento del afectado para la cesión de sus datos, éste deberá ser informado de forma que conozca inequívocamente la finalidad a la que se destinarán los datos respecto de cuya comunicación se solicita el consentimiento y el tipo de actividad desarrollada por el cesionario. En caso contrario, el consentimiento será nulo.

5.2 Consentimiento para el tratamiento de datos de menores de edad

1. Podrá procederse al tratamiento de los datos de los mayores de catorce años con su consentimiento, salvo en aquellos casos en los que la Ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela. En el caso de los menores de catorce años se requerirá el consentimiento de los padres o tutores.

2. En ningún caso podrán recabarse datos del menor que permitan obtener información sobre los demás miembros del grupo familiar, o sobre las características del mismo, como los datos relativos a la actividad profesional de los progenitores, información económica, datos sociológicos o cualesquiera otros, sin el consentimiento de los titulares de tales datos. No obstante, podrán recabarse los datos de identidad y dirección del padre, madre o tutor con la única finalidad de recabar la autorización prevista en el apartado anterior.

3. Cuando el tratamiento se refiera a datos de menores de edad, la información dirigida a los mismos deberá expresarse en un lenguaje que sea fácilmente comprensible por aquéllos, con expresa indicación de lo dispuesto en este artículo.

4. Corresponderá al responsable del fichero o tratamiento articular los procedimientos que garanticen que se ha comprobado de modo efectivo la edad del menor y la autenticidad del consentimiento prestado en su caso, por los padres, tutores o representantes legales.

5.3 Forma de recabar el consentimiento

1. El responsable del tratamiento podrá solicitar el consentimiento del interesado a través del procedimiento establecido en este artículo, salvo cuando la Ley exija al mismo la obtención del consentimiento expreso para el tratamiento de los datos.

2. El responsable deberá informar al afectado y deberá concederle un plazo de treinta días para manifestar su negativa al tratamiento de sus datos, advirtiéndole de que en caso de no pronunciarse a tal efecto se entenderá que consiente el tratamiento de sus datos de carácter personal.

3. En todo caso, será necesario que el responsable del tratamiento pueda conocer si la comunicación ha sido objeto de devolución por cualquier causa, en cuyo caso no podrá proceder al tratamiento de los datos referidos a ese interesado.

4. Deberá facilitarse al interesado un medio sencillo y gratuito para manifestar su negativa al tratamiento de los datos. En particular, se considerará ajustado al presente reglamento los procedimientos en el que tal negativa pueda efectuarse, entre otros, mediante un envío prefranqueado al responsable del tratamiento, la llamada a un número telefónico gratuito o a los servicios de atención al público que el mismo hubiera establecido.

5. Cuando se solicite el consentimiento del interesado a través del procedimiento establecido en este artículo, no será posible solicitarlo nuevamente respecto de los

mismos tratamientos y para las mismas finalidades en el plazo de un año a contar de la fecha de la anterior solicitud.

5.4 Revocación del consentimiento

1. El afectado podrá revocar su consentimiento a través de un medio sencillo, gratuito y que no implique ingreso alguno para el responsable del fichero o tratamiento. En particular, se considerará ajustado al presente reglamento el procedimiento en el que tal negativa pueda efectuarse, entre otros, mediante un envío prefranqueado al responsable del tratamiento o la llamada a un número telefónico gratuito o a los servicios de atención al público que el mismo hubiera establecido.

No se considerarán conformes a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, los supuestos en que el responsable establezca como medio para que el interesado pueda manifestar su negativa al tratamiento el envío de cartas certificadas o envíos semejantes, la utilización de servicios de telecomunicaciones que implique una tarificación adicional al afectado o cualesquiera otros medios que impliquen un coste adicional al interesado.

2. El responsable cesará en el tratamiento de los datos en el plazo máximo de diez días a contar desde el de la recepción de la revocación del consentimiento, sin perjuicio de su obligación de bloquear los datos conforme a lo dispuesto en el art. 16.3 de la Ley Orgánica 15/1999, de 13 de diciembre.

6. DEBER DE INFORMACIÓN

Artículo 5.1 LOPD:
"Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:

a) *De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.*
b) *Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.*
c) *De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.*
d) *De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.*
e) *De la indentidad y dirección del responsable del tratamiento o, en su caso de su representante."*

Para el correcto cumplimiento de este deber, será necesaria la inclusión de cláusulas informativas tanto en las hojas de toma de datos para la confección de historias clínicas de los pacientes, así como en las facturas u otros documentos que contengan datos de carácter personal.

En el ANEXO III de este manual se encuentran distintos tipos de cláusulas a incluir en los documentos con los que trabaja el psicólogo o bien a exponer en carteles.

Por tanto: independientemente de la exigencia o no del consentimiento el psicólogo habrá de cumplir con el deber de información exigido por el artículo 5, que podrá cumplirse: bien mediante la incorporación de la cláusula correspondiente en su impreso o bien mediante la inserción de la misma en carteles visibles.

7. CONTRATOS DE TRATAMIENTO DE DATOS POR TERCEROS

Artículo 12.1 LOPD:
"No se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento"

En muchas ocasiones, los psicólogos necesitan contratar un tercero para asegurar el efectivo desarrollo de sus obligaciones y de su actividad, como puede ser la elaboración de nóminas, la facturación y la contabilidad, el mantenimiento informático, tanto a nivel de equipos como de aplicaciones de gestión de la clínica, o incluso con otros profesionales psicólogos que colaboran con el psicólogo y que a su vez le facturan, etc. En estos casos, cuando un tercero necesita acceder a un fichero con datos de carácter personal para la prestación de dicho servicio, ese acceso deberá estar regulado de la siguiente manera:

► Por contrato, que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido. En realidad, la Agencia sólo acepta la forma escrita, pudiendo celebrarse por medio de contrato de tratamiento por terceros o en forma de cláusula o anexo a otro contrato, como por ejemplo al de prestación de servicios.

► La ley distingue entre:

- Responsable del tratamiento: titular del fichero con datos de carácter personal. En realidad se trata del responsable del fichero.

- Encargado del tratamiento: tercero que accede a los datos para la prestación de un servicio al Responsable del tratamiento.

► Deberá establecerse expresamente:

- Que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas.

- Se estipularán las medidas de seguridad que el encargado del tratamiento está obligado a implementar.

► En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado también responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.

Siempre que haya algún tercero (no en régimen laboral, es decir: no un trabajador, sí alguien en régimen mercantil) que para prestarle un servicio al psicólogo acceda a datos del mismo, habrá de suscribirse el citado contrato. Para cumplir con la obligación desarrollada en este punto se adjunta un modelo de contrato y algunos ejemplos en el ANEXO III.

8. MEDIDAS DE SEGURIDAD

8.1. NIVELES DE SEGURIDAD

Atendiendo a la naturaleza de la información tratada, las medidas exigibles a los ficheros se pueden clasificar en tres niveles:

- Básico
- Medio
- Alto

El nivel de seguridad está íntimamente relacionado con la mayor o menor necesidad de garantizar la confidencialidad e integridad de la información. Los niveles están contemplados tanto en la LOPD (Art. 20.2.h) como en el Reglamento de Medidas de Seguridad (Artículo 81).

8.1.1 Nivel básico

Todos los ficheros o tratamientos de datos de carácter personal deberán adoptar las medidas de seguridad calificadas de nivel básico.

¿Quién no tiene al menos un fichero de nivel básico? Cualquier fichero con datos de carácter personal que no pueda calificarse de nivel medio o alto, tendrá este nivel, como por ejemplo el fichero de proveedores, contactos (o agenda o terceros), contabilidad y facturación, etc.

8.1.2 Nivel medio

Deberán implantarse, además de las medidas de seguridad de nivel básico, las medidas de nivel medio, en los siguientes ficheros o tratamientos de datos de carácter personal:

1. Los relativos a la comisión de infracciones administrativas o penales.
2. Aquellos cuyo funcionamiento se rija por el art. 29 de la Ley Orgánica 15/1999, de 13 de diciembre.
3. Aquellos de los que sean responsables Administraciones tributarias y se relacionen con el ejercicio de sus potestades tributarias.
4. Aquellos de los que sean responsables las entidades financieras para finalidades relacionadas con la prestación de servicios financieros.
5. Aquellos de los que sean responsables las Entidades Gestoras y Servicios Comunes de la Seguridad Social y se relacionen con el ejercicio de sus

competencias. De igual modo, aquellos de los que sean responsables las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social.

6. Aquellos que contengan un conjunto de datos de carácter personal que ofrezcan una definición de las características o de la personalidad de los ciudadanos y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos.

8.1.3 Nivel alto

Además de las medidas de nivel básico y medio, las medidas de nivel alto se aplicarán en los siguientes ficheros o tratamientos de datos de carácter personal:

1. Los que se refieran a datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual.
2. Los que contengan o se refieran a datos recabados para fines policiales sin consentimiento de las personas afectadas.
3. Aquellos que contengan datos derivados de actos de violencia de género.
4. A los ficheros de los que sean responsables los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones electrónicas respecto a los datos de tráfico y a los datos de localización, se aplicarán, además de las medidas de seguridad de nivel básico y medio, la medida de seguridad de nivel alto contenida en el art. 103 de este reglamento.
5. En caso de ficheros o tratamientos de datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual bastará la implantación de las medidas de seguridad de nivel básico cuando:
    - Los datos se utilicen con la única finalidad de realizar una transferencia dineraria a las entidades de las que los afectados sean asociados o miembros.
    - Se trate de ficheros o tratamientos no automatizados en los que de forma incidental o accesoria se contengan aquellos datos sin guardar relación con su finalidad.
6. También podrán implantarse las medidas de seguridad de nivel básico en los ficheros o tratamientos que contengan datos relativos a la salud, referentes exclusivamente al grado de discapacidad o la simple declaración de la condición de discapacidad o invalidez del afectado, con motivo del cumplimiento de deberes públicos.
7. Las medidas incluidas en cada uno de los niveles descritos anteriormente tienen la condición de mínimos exigibles, sin perjuicio de las disposiciones legales o reglamentarias específicas vigentes que pudieran resultar de aplicación en cada caso o las que por propia iniciativa adoptase el responsable del fichero.
8. A los efectos de facilitar el cumplimiento de lo dispuesto en este título, cuando en un sistema de información existan ficheros o tratamientos que en función de su finalidad o uso concreto, o de la naturaleza de los datos que contengan, requieran la aplicación de un nivel de medidas de seguridad diferente al del sistema principal, podrán segregarse de este último, siendo de aplicación en cada caso el nivel de medidas de seguridad correspondiente y siempre que puedan delimitarse los datos afectados y los usuarios con acceso a los mismos, y que esto se haga constar en el documento de seguridad.

8.2. ADOPCIÓN DE LAS MEDIDAS DE SEGURIDAD

Las medidas de seguridad se documentan y especifican en un manual conocido como *"Documento de Seguridad"*. La función de este documento es la de recoger todas aquellas medidas de carácter técnico y organizativo que deben implantarse en el tratamiento de ficheros por parte del Responsable de los mismos.

Dicho Documento de Seguridad, debe estar a disposición de la Agencia Española de Protección de Datos en caso de que ésta lo requiriese. Aunque si no lo hace, tendrá la consideración de documento interno de la organización.

Las medidas de seguridad se van aplicando de manera acumulativa en función de los niveles aplicados. De forma que los ficheros de cada nivel deben cumplir las medidas de dicho nivel y las de los niveles inferiores.

8.2.1 Medidas de Seguridad de Nivel básico

Las principales medidas de seguridad para los ficheros automatizados de nivel básico son las siguientes:

- **Funciones y obligaciones del personal.** Es en el Documento de Seguridad donde se han de recoger dichas obligaciones de cada usuario con acceso a los datos del sistema de información de la organización. El Responsable de Seguridad ha de adoptar las medidas para que los usuarios conozcan de forma comprensible las normas en materia de seguridad.
- **Tener habilitado un Registro de Incidencias.** Dicho Registro deberá aplicarse a todas las incidencias que afecten a los ficheros que contengan datos de carácter personal.
- **Llevar un control de acceso.** Los usuarios solo tendrán acceso a aquellos recursos que precisen para el desarrollo de sus funciones.
- **Gestionar los soportes que contengan datos de carácter personal**. Permitiendo así que estos sean identificados e identificables, además de estar inventariados y conocer que tipo de información contienen, salvo que las circunstancias físicas del soporte lo impidan. (Como por ejemplo una memoria USB muy pequeña).
- **Gestión de entradas y salidas de soportes y documentos.**
- **Habilitar un sistema que permita garantizar la correcta identificación y autenticación de los usuarios.**
- **Establecer un sistema de copias de respaldo y recuperación de la información.** Con periodicidad mínima de una semana.

A los ficheros no automatizados, además de aplicarles lo dispuesto en los capítulos I y II del RMS en lo relativo a:

- Niveles de seguridad.
- Alcance.
- Encargado del tratamiento.
- Prestaciones de servicios sin acceso a datos personales.
- Delegación de autorizaciones.
- Régimen de trabajo fuera de los locales del responsable del fichero o encargado del tratamiento.

- Copias de trabajo de documentos.
- Documento de seguridad.
- Funciones y obligaciones del personal.
- Registro de incidencias.
- Control de acceso.
- Gestión de soportes.

Se les aplicará además:

- **Criterios de archivo**. El criterio organizativo de los soportes deberá estar regulado en cada legislación y deberán garantizar la conservación de los documentos, así como su localización y consulta y posibilitar el ejercicio de derechos de acceso, rectificación, cancelación y oposición.
- **Disponer de mecanismos que obstaculicen la apertura de los dispositivos de almacenamiento** de los documentos que contengan datos de carácter personal.
- **Custodiar la documentación** con datos de carácter personal, cuando esta se encuentre fuera de los dispositivos de almacenamiento de dichos ficheros e impedir que una persona no autorizada acceda a dicha información.

8.2.2. Medidas de Seguridad de Nivel medio

Además de las medidas de seguridad de nivel básico, los ficheros que contengan datos de nivel medio deberán cumplir las siguientes medidas de seguridad.

Respecto a los ficheros automatizados:

- **Designar uno o varios Responsables de Seguridad**. Encargados de controlar y coordinar las medidas de seguridad definidas en el Documento de Seguridad.
- **Someter los sistemas de información e instalaciones de tratamiento y almacenamiento a una auditoría** bienal, que puede ser interna o externa y que verifique lo dispuesto en este apartado.
- **Disponer de registros de entrada y salida de soportes.**
- **Establecer un mecanismo que limite la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información**. (Bloqueo de contraseñas por exceso de intentos fallidos).
- **Control de acceso físico.** Solo el personal autorizado puede acceder a los lugares donde se encuentren los sistemas de información.
- **Consignar un Registro de incidencias más detallado** que el del nivel básico, y tener la autorización del Responsable del Fichero para la recuperación de los datos.

En cuanto a las medidas para los ficheros no automatizados, le serán de aplicación las de nivel medio, así como las siguientes medidas:

- Al igual que en los ficheros automatizados, habrá que designar un Responsable de Seguridad.
- Elaborar un informe de auditoria cada dos años de manera interna o externa.

8.2.3. Medidas de Seguridad de Nivel alto

Además de cumplir con las medidas de nivel básico y medio, los ficheros de nivel alto tendrán que cumplir con las siguientes medidas de seguridad, en función de si son automatizados o en soporte no automatizado.

Medidas de seguridad para los ficheros de nivel alto:

- **La identificación de los soportes que contengan datos de carácter personal considerados sensibles para la organización**, se podrá realizar utilizando sistemas de etiquetado comprensibles y con significado que permita a los usuarios identificar el contenido de los mismos.
- **La distribución de soportes se realizará cifrando los datos o mecanismo análogo** que garantice que dicha información no es accesible o manipulada durante su transporte.
- Evitar **el tratamiento de datos de carácter personal en dispositivos portátiles** que no permitan su cifrado.
- **Deberá conservarse una copia de respaldo de los datos y de los procedimientos de recuperación de los mismos en lugar diferente** a aquel donde se encuentren los equipos informáticos y que cumpla con las medidas de seguridad establecidas en el RMS.
- **Habilitar un Registro de accesos**, donde se indique: Fecha y hora en que se realizó, identificación del usuario, fichero accedido, tipo de acceso y si ha sido autorizado o denegado. Dicho Registro ha de estar bajo el control directo del Responsable de Seguridad y se ha de conservar durante un periodo mínimo de dos años. Asimismo, se debe realizar al menos una vez al mes un informe de las revisiones realizadas y los problemas detectados.
- **La transmisión de datos de carácter personal a través de redes públicas o redes inalámbricas** de comunicaciones electrónicas, se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

Las principales medidas de seguridad para los ficheros no automatizados de nivel alto son las siguientes.

- **Almacenamiento de la Información.** Los armarios, archivadores u otros elementos en los que se almacenen los ficheros no automatizados con datos de carácter personal deberán encontrarse en áreas en las que el acceso esté protegido con puertas de acceso dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente.
- **La copia o reproducción de documentos,** solo podrá ser realizada bajo el control del personal autorizado en el Documento de Seguridad. Se deberá destruir las copias o reproducciones desechadas de forma que se evite el acceso a la información contenida.
- **Acceso a la información.** Solo el personal autorizado podrá acceder a la información.
- **Traslado de documentación.** Siempre que se proceda al traslado físico de la documentación contenida en un fichero, deberán adoptarse medidas dirigidas a impedir el acceso o manipulación de la información objeto de traslado.

En conclusión: el psicólogo habrá de proteger la información (automatizada o no, según el caso) con las correspondientes medidas de seguridad que deberán documentarse en el Documento de Seguridad, que deberá mantenerse actualizado. Este documento puede llevarse y actualizarse en un procesador de textos o mediante una aplicación informática. En concreto una de las obligaciones importantes es el hecho de que los usuarios del sistema de información de la organización (es decir, aquellas personas que accedan a datos personales) conozcan de forma comprensible las normas en materia de seguridad. Por ello se aportan varios modelos de normas para que las firmen aquellas personas que accedan a datos personales de la clínica o consulta como **ANEXO V**.

9. INFRACCIONES Y SANCIONES

Según los artículos 44 y 45 de la LOPD, las infracciones se clasifican en leves, graves y muy graves.

9.1 Infracciones leves

Artículo 44.2 LOPD

- No atender, por motivos formales, 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 Agencia Española de Protección de Datos en el ejercicio de las competencias que tiene legalmente atribuidas, en relación con aspectos no sustantivos de la protección de datos.
- No solicitar la inscripción del fichero de datos de carácter personal en el Registro General de Protección de Datos, cuando no sea constitutivo de infracción grave.
- Proceder a la recogida de datos de carácter personal de los propios afectados sin proporcionarles la información que señala el artículo 5 de la LOPD.
- Incumplir el deber de secreto establecido en el artículo 10, salvo que constituya infracción grave.

Para las infracciones leves, se prevén **sanciones desde 601,01 € hasta 60.101,21 €.**

9.2 Infracciones graves

Artículo 44.3 LOPD.

- Proceder a la creación de ficheros de titularidad privada o iniciar la recogida de datos de carácter personal para los mismos con finalidades distintas de las que constituyen el objeto legítimo de la empresa o entidad.
- Proceder a la recogida de datos de carácter personal sin recabar el consentimiento expreso de las personas afectadas, en los casos en que éste sea exigible.
- Tratar los datos de carácter personal o usarlos posteriormente con

conculcación de los principios y garantías establecidos en la presente Ley o con incumplimiento de los preceptos de protección que impongan las disposiciones reglamentarias de desarrollo, cuando no constituya infracción muy grave.

- El impedimento o la obstaculización del ejercicio de los derechos de acceso y oposición y la negativa a facilitar la información que sea solicitada.
- Mantener datos de carácter personal inexactos o no efectuar las rectificaciones o cancelaciones de los mismos que legalmente procedan cuando resulten afectados los derechos de las personas que la presente Ley ampara.
- La vulneración del deber de guardar secreto sobre los datos de carácter personal incorporados a ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros, prestación de servicios de solvencia patrimonial y crédito, así como aquellos otros ficheros que contengan un conjunto de datos de carácter personal suficientes para obtener una evaluación de la personalidad del individuo.
- Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen.
- No remitir a la Agencia Española de Protección de Datos las notificaciones previstas en esta Ley o en sus disposiciones de desarrollo, así como no proporcionar en plazo a la misma cuantos documentos e informaciones deba recibir o sean requeridos por aquel a tales efectos.
- La obstrucción al ejercicio de la función inspectora.
- No inscribir el fichero de datos de carácter personal en el Registro General de Protección Datos, cuando haya sido requerido para ello por el Director de la Agencia Española de Protección de Datos.
- Incumplir el deber de información que se establece en los artículos 5, 28 y 29 de esta Ley, cuando los datos hayan sido recabados de persona distinta del afectado.

En el caso de las infracciones graves, las sanciones pueden ir desde 60.101,22 euros hasta los 300.506,05 €.

9.3 Infracciones muy graves

Artículo 44.4 LOPD.

- La recogida de datos en forma engañosa y fraudulenta.
- La comunicación o cesión de los datos de carácter personal, fuera de los casos en que estén permitidas.
- Recabar y tratar los datos de carácter personal cuando no medie el consentimiento expreso del afectado; recabar y tratar los datos cuando no lo disponga una ley o el afectado no haya consentido expresamente, o violentar la prohibición contenida en el apartado 4 del artículo 7.
- No cesar en el uso ilegítimo de los tratamientos de datos de carácter personal cuando sea requerido para ello por el Director de la Agencia Española de Protección de Datos o por las personas titulares del derecho de acceso.
- La transferencia temporal o definitiva de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento, con destino a países que no proporcionen un nivel de protección

equiparable sin autorización del Director de la Agencia Española de Protección de Datos.

- Tratar los datos de carácter personal de forma ilegítima o con menosprecio de los principios y garantías que les sean de aplicación, cuando con ello se impida o se atente contra el ejercicio de los derechos fundamentales.
- La vulneración del deber de guardar secreto sobre los datos de carácter personal, así como los que hayan sido recabados para fines policiales sin consentimiento de las personas afectadas.
- No atender, u obstaculizar de forma sistemática el ejercicio de los derechos de acceso, rectificación, cancelación u oposición.
- No atender de forma sistemática el deber legal de notificación de la inclusión de datos de carácter personal en un fichero.

En este caso, las sanciones son económicamente considerables, yendo **desde 300.506,06 € hasta los 601.012,1 Euros.**

ANEXOS

ANEXO I. INSCRIPCIÓN DE LOS FICHEROS EN EL REGISTRO GENERAL DE PROTECCIÓN DE DATOS

El primer paso a dar es la inscripción de los ficheros. Para ello habrá que seguir los siguientes pasos:

- Examinar que bases de datos se hallan en el sistema de información de la consulta y en los que se pueda introducir datos de carácter personal.
- Examinar todos los ficheros en papel que contengan datos de carácter personal y analizar su estructura, determinando a su vez el nivel de seguridad a aplicar.
- Inscribir los ficheros que encontremos en el Registro General de Protección de Datos mediante el programa de inscripción de ficheros **NOTA**.

La Agencia de Protección de Datos considera que no hay que inscribir cada una de las bases de datos o tablas que encontremos en el sistema sino que hay que tender a una agrupación lógica de los ficheros y a partir de ésta inscribirlos.

ANEXO II. CLÁUSULAS DE INFORMACIÓN

Éstas sirven para cumplir con el artículo 5 de la LOPD, en el que se dispone que se deberá informar a los titulares de los datos que hayan sido recabados. Para ello debemos seguir los siguientes pasos:

• Incorporar en los documentos de trabajo las cláusulas citadas a continuación y adaptarlas al caso concreto de cada consulta para que el cliente las firme.
• O -en el caso de los pacientes- confeccionar con ellas un cartel documento que esté exhibido claramente a los pacientes.

II.1. Cláusula a incluir en facturas, presupuestos, etc.

Le recordamos, que sus datos están recogidos en un fichero titularidad de [Nombre del psicólogo o clínica privada] con la finalidad de prestar sus servicios profesionales. De acuerdo con la Ley orgánica 15/1999 de Protección de datos de carácter personal puede ejercitar los derechos de acceso, rectificación, cancelación, y, en su caso, oposición enviando un escrito de solicitud y fotocopia del DNI a [Dirección de la clínica o consulta privada].

II.2. Cláusula de información para los trabajadores

En cumplimiento de la Ley Orgánica 15/1999 sobre Protección de datos de carácter personal se le informa que los datos personales que nos ha facilitado, serán (o han sido) incorporados en ficheros titularidad de [NOMBRE DE LA ENTIDAD] (En adelante, el RESPONSABLE), siendo los datos y finalidades correspondientes a los mismos los que se detallan a continuación:

- ***PERSONAL:*** *en el mismo se almacenan los datos necesarios para la*

elaboración de las nóminas de los trabajadores y el cálculo de las retenciones correspondientes al IRPF (situación personal y familiar, número de hijos, etc.) y control de pólizas de seguro contratadas, en su caso, por el RESPONSABLE, transferencias de nóminas, gestión de costes de empresa derivados directamente de su plantilla y control del trabajo.

- ***PREVENCIÓN DE RIESGOS:*** *información relativa al puesto de trabajo y situaciones de riesgo que conlleva el mismo, situación laboral del trabajador, formación recibida en materia de prevención de riesgos, material de protección entregado, cambios de sección del trabajador motivados por causas laborales o no laborales, accidentes laborales producidos, control de siniestralidad y medidas correctoras tomadas por el RESPONSABLE para evitar su repetición. Este fichero contiene información necesaria para lograr el efectivo control de la vigilancia de la salud de los trabajadores, revisiones periódicas, partes de baja, accidentes laborales, etc. Los datos contenidos en este fichero son tratados exclusivamente por personal sanitario o sometido a un estricto deber de secreto, no teniendo el RESPONSABLE acceso a la información almacenada, conforme establece la Ley de Prevención de Riesgos Laborales.*

Queda terminantemente prohibida la comunicación de los datos objeto de tratamiento, a terceras personas, salvo las legalmente establecidas o las necesarias para el cumplimiento de las finalidades de la relación contractual.

Asimismo le informamos de lo siguiente:

-La información de salud facilitada directamente por el trabajador o indirectamente a través de la Mutua de accidentes de trabajo y Enfermedades Profesionales que se encargue a su vez de la vigilancia de la salud, será incluida en un fichero titularidad del RESPONSABLE, y tratado por la Mutua o empresa que en esos momentos preste el servicio con el objeto de cumplir con las finalidades anteriormente detalladas

La información obtenida de las pruebas psicológicas a las que sea sometido el trabajador será comunicada al RESPONSABLE, a fin de que proceda a la emisión del correspondiente informe de aptitud, y a efectos de un seguimiento y control de las prestaciones.

-Los datos económicos de su nómina serán cedidos a la entidad financiera con la que el RESPONSABLE trabaje, para el correspondiente pago de nóminas a los trabajadores.

-La información de carácter fiscal y laboral recabada será comunicada a la Agencia Tributaria, Seguridad Social e INEM en los supuestos exigidos por la normativa aplicable.

-Si durante la vigencia de la relación laboral con el RESPONSABLE, usted es seleccionado para asistir a cursos de formación, sus datos personales serán cedidos al centro correspondiente donde se impartirán los mismos, a efectos de mantener un control de los asistentes y un adecuado desarrollo del curso.

Se le informa que conforme a lo dispuesto en la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, está obligado a informar de las variaciones que puedan experimentar sus datos facilitados. Asimismo, y si quiere ejercer sus derechos

de acceso rectificación, cancelación u oposición, puede hacerlo enviando una solicitud por escrito acompañada de una fotocopia de tu DNI dirigida a [NOMBRE ENTIDAD Y DIRECCIÓN]

II.3. Cláusula de hoja de paciente

Los datos de carácter personal recabados, serán incorporados a un fichero titularidad de [INDICAR EL NOMBRE DEL PSICÓLOGO O CLÍNICA PRIVADA], necesario para la correcta gestión y asesoramiento de los clientes, e imprescindible para la prestación de nuestros servicios y la debida atención psicológica.

Asimismo, le informamos que tan solo se recogerán los datos estrictamente necesarios para la prestación de los servicios psicológicos por parte de la clínica y que éstos no se comunicarán a terceros ajenos a la clínica, salvo en los supuestos legalmente previstos.

De acuerdo con lo dispuesto en la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, usted puede ejercitar sus derechos de acceso, rectificación, cancelación y, en su caso, oposición, enviando una solicitud por escrito, acompañada de una fotocopia de su DNI a: [INDICAR LA DIRECCIÓN DE LA CONSULTA DEL PSICÓLOGO O CLÍNICA PRIVADA]

Y para que quede constancia, lo firmo en _____, a __ de _____ de ____.

APELLIDOS Y NOMBRE.

ANEXO III. CONTRATOS DE ACCESO A DATOS POR TERCEROS

De acuerdo con el artículo 12 de la LOPD, el psicólogo deberá suscribir contratos con todas aquellas entidades que traten datos personales, tanto de los pacientes, proveedores, como de los trabajadores de la propia empresa. Los más típicos son los que realizan con la asesoría laboral, asesoría fiscal, mantenimiento informático, riesgos laborales, vigilancia de la salud, etc.

Se ha puesto a disposición distintos modelos de contrato de manera que se adapten a todo tipo de tratamiento de datos por terceros.

III.1. ACLARACIONES GENERALES

En los modelos que se presentan el Responsable del Fichero o del tratamiento será siempre el psicólogo o la clínica. El Encargado del tratamiento será (en dichos supuestos) la entidad o profesional que presta el servicio.

III.2. EJEMPLOS DE CONTRATOS

Los contratos (finalidades) tipo de servicios que se prestan por terceros al psicólogo son los siguientes:

- Contrato con la Asesoría Fiscal: Contrato pensado en el caso de que una asesoría nos preste únicamente asesoramiento fiscal y/o contable.
- Contrato con la Asesoría Laboral: En el caso de que una asesoría nos preste únicamente asesoramiento laboral.
- Contrato con la Asesoría Laboral, Contable y Fiscal: Es muy habitual que el asesoramiento laboral, contable y fiscal, sea prestado por la misma Asesoría. En ese caso se deberá firmar este contrato.
- Contrato de mantenimiento informático: Contrato a firmar con aquellas empresas que nos presten el servicio de mantenimiento informático, tanto si se refiere al mantenimiento de los equipos (PC's, impresoras, scanner, etc.) como si se refiere al mantenimiento de aplicaciones, programas informáticos, o la red de comunicaciones.
- Contrato de Prevención de Riesgos: Se ha de firmar en el caso de que la Clínica tenga contratada una empresa de prevención de riesgos y no se incluya la cláusula de Protección de datos en el contrato de prestación de servicios.

III.3. EJEMPLOS DE FINALIDADES

1. Finalidad Fiscal y Contable

El Encargado realizará el tratamiento de los datos por cuenta del Responsable del mismo, y conforme a sus instrucciones. La finalidad del tratamiento es posibilitar el asesoramiento y gestión fiscal del Responsable, servicio que implica: la revisión de libros contables, revisión, confección, presentación y pago (en su caso) de los diferentes impuestos y modelos tributarios, lo que conllevará, cuando sea necesario, comunicación de datos a la Agencia Tributaria, a los diferentes Registros (Mercantil, de Fundaciones, Asociaciones...), Ayuntamientos y demás Organismos según dicte la Normativa vigente en materia fiscal.

2. Laboral

La finalidad del tratamiento es posibilitar la confección de las nóminas, cartas de pago del IRPF, certificaciones de las retenciones del personal por año fiscal, resumen anual de retenciones, así como la confección y presentación ante la Agencia Tributaria de las declaraciones y documentos fiscales necesarios para la prestación de los servicios encomendados.

Además de las anteriores finalidades, se posibilita también el acceso a los datos necesarios para el pago de las cuotas empresa y obrera a la Seguridad Social, confeccionando los documentos de cotización que en cada momento tenga establecidos la Tesorería General de la Seguridad Social, remitiéndolos al Responsable o a la entidad bancaria por éste señalada. La confección de contratos de trabajo, presentación y recogida de contratos de trabajo de las oficinas de empleo, control y gestión de abono de prestaciones por enfermedad, tramitación de altas, bajas y modificaciones de la Seguridad Social, cálculo y confección de finiquitos, consultas sobre temas laborales y de seguridad social, emisión de

certificados de Seguridad Social y demás funciones permitidas por su sistema RED, solicitud de subvenciones o bonificaciones ante aquellos organismos públicos que las otorguen, comunicación de datos a la Generalitat Valenciana, ya sea para posibilitar el abono de la nómina de pago delegado, o para solicitar la creación, reducción o ampliación de las unidades concertadas con dicha Administración, representación ante las inspecciones de trabajo, servicios de mediación arbitraje y conciliación, órganos jurisdiccionales laborales, además de la confección de los recibos de cobro de salarios mensuales y pagas extraordinarias.

3. Entidad Financiera

La finalidad del tratamiento es posibilitar el asesoramiento jurídico y reclamaciones judiciales relacionados con el cobro de deudas de los clientes del Responsable que adquieren deudas con el mismo.

4. Mantenimiento Informático (Hardware)

El Responsable del fichero autoriza expresamente al Encargado a acceder a información de su titularidad exclusivamente para la realización de tareas de mantenimiento de Hardware del Responsable del fichero: resolución de incidencias, cambio y reparaciones de equipos, etc.….

5. Mantenimiento Informático (Software)

El Responsable del fichero autoriza expresamente al Encargado a acceder a información de su titularidad exclusivamente para la realización de tareas de mantenimiento del Software (indicar el nombre del software): actualizaciones, resolución de incidencias, etc.…

III.4. Modelo de contrato

MODELO CONTRATO DE ACCESO A DATOS POR CUENTA DE TERCEROS

En _____, a ___ de _____ de _____.

REUNIDOS

De una parte, D._____, mayor de edad, con DNI _____ y con domicilio, a efectos del presente contrato, la (INDICAR LA DIRECCION DEL RESPONSABLE DEL FICHERO).

Y de otra, D. _____, mayor de edad, con DNI _____ con domicilio, a efectos del presente contrato, en la (INDICAR LA DIRECCION DEL ENCARGADO DEL TRATAMIENTO)

INTERVIENEN

El primero, en nombre y representación de INDICAR EL NOMBRE DEL RESPONSABLE con CIF DEL RESPONSABLE (en adelante, el Responsable del tratamiento o _____).

El segundo, en nombre y representación de INDICAR EL NOMBRE DEL ENCARGADO con CIF _____ (en adelante, el Encargado del tratamiento o _____).

Ambas partes se declaran, según intervienen, con capacidad suficiente para suscribir el presente CONTRATO DE ACCESO A DATOS POR CUENTA DE TERCEROS, y puestas previamente de acuerdo,

MANIFIESTAN

I.- Que el Encargado del tratamiento se halla, en la actualidad, prestando determinados servicios (que se detallan en este contrato) al Responsable del fichero.

II.- Para el correcto cumplimiento de estos servicios, el Encargado trata datos de carácter personal titularidad del Responsable del fichero.

III.- En cumplimiento de lo dispuesto en la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal (en adelante, LOPD), es intención de ambas partes establecer las obligaciones y responsabilidades que corresponden a cada una de ellas en el tratamiento de los datos de carácter personal, con arreglo a las siguientes,

ESTIPULACIONES

PRIMERA.- Definiciones
De conformidad con las definiciones recogidas en la LOPD, a los efectos de lo dispuesto en este Contrato, se entenderá por:

Datos de carácter personal: cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, susceptible de recogida, registro, tratamiento o transmisión concerniente a una persona física identificada o identificable.

Fichero: todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

Tratamiento de datos: operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

Responsable del fichero o tratamiento: persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.

Encargado del tratamiento: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento y accede a los datos de carácter personal del responsable del fichero mediante contrato.

SEGUNDA.- De los datos facilitados por las partes

Los datos personales facilitados por las partes del presente contrato, para los casos en que éstos sean una persona física, o en el caso de representantes de una persona jurídica o administración, serán incorporados a un fichero cuya titularidad corresponde a cada una de las partes respectivamente. La finalidad de la recogida y tratamiento de la información es la gestión y mantenimiento de las relaciones comerciales o profesionales establecidas, así como la de mantenerle informado de nuevos servicios y ofertas. Asimismo ambas partes se dan por informadas de la posibilidad de ejercitar sus derechos de acceso, rectificación, cancelación y oposición, respecto de sus datos personales, pudiendo ejercitar estos derechos por escrito mediante carta dirigida al domicilio de la parte que corresponda.

TERCERA.- Finalidad que justifica el Tratamiento por parte del encargado

Las finalidades que justifican el acceso por parte del encargado a los datos del Responsable son exclusivamente las que se detallan en los anexos correspondientes.

Queda terminantemente prohibida la aplicación o utilización de los datos contenidos en estos ficheros con fines distintos a los aquí previstos, salvo autorización expresa, manifestada por escrito, del Responsable. Se prohíbe, asimismo, la comunicación de los datos objeto de tratamiento, ni siquiera para su conservación a otras personas, salvo las cesiones legalmente establecidas y las que resulten necesarias para el cumplimiento de las finalidades de la relación contractual.

En el caso de que el Encargado destine los datos a finalidad distinta de las señaladas, los comunique o utilice incumpliendo las estipulaciones del presente contrato, será considerado a todos los efectos, Responsable del Tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.

CUARTA.- Deber de secreto

El personal del Encargado del tratamiento tendrá la obligación de mantener el deber de secreto respecto a la información contenida en las bases de datos a las que, en su caso, hubieren tenido acceso, aun después de haber cesado su relación laboral con el Encargado.

Es obligación de este último comunicar este deber a su personal, así como cuidar de su cumplimiento.

QUINTA.- Seguridad de los datos.

En caso de ser realizados los servicios que impliquen tratamiento de datos personales objeto del presente contrato, en las propias instalaciones del Responsable en equipos de hardware y software de ésta, el Encargado deberá cumplir con las medidas de seguridad adoptadas por el Responsable para la protección de los datos personales, y que esta previamente le comunique.

En caso de ser realizado el servicio que implique tratamiento de datos personales fuera de las instalaciones del Responsable, éste adoptará las medidas de seguridad de nivel básico, medio o alto según corresponda, de acuerdo con los artículos 8 a 26 ambos inclusive, del Reglamento de Medidas de Seguridad de los Ficheros Automatizados que Contengan Datos de Carácter

Personal, aprobado por Real Decreto 994/1999, de 11 de junio así como cuantas medidas de seguridad sean exigidas por las leyes y reglamentos destinadas a preservar el secreto, confidencialidad e integridad en el tratamiento de datos personales, con objeto de garantizar la seguridad de los datos de carácter personal y evitar su alteración, tratamiento o acceso no autorizado, así como a adoptar en el futuro.

SEXTA.- Ejercicio de derechos por los interesados

Los derechos de acceso, rectificación y cancelación de los datos, se ejercerán por los interesados ante el Responsable del tratamiento.

SÉPTIMA.- Deber de devolución y no conservación

Una vez finalizada la prestación contractual, los datos de carácter personal deben ser devueltos al Responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto de tratamiento. Aquellos datos que no se devuelvan habrán de destruirse adoptando las medidas de seguridad para evitar el acceso por parte de terceros.

OCTAVA.- Responsabilidad

Ambas partes se comprometen a respetar, en el cumplimiento de las obligaciones que se derivan de este documento, toda la legislación y normativa que resulte aplicable, muy en particular, las obligaciones impuestas y determinadas por la Ley Orgánica 15/1999 de 13 de Diciembre, de Protección de Datos de Carácter Personal. Cada parte deberá hacer frente a la responsabilidad que se derive de su propio incumplimiento de dicha legislación y normativa.

NOVENA - Fuero

Las partes, para la resolución de cualquier conflicto que pudiera surgir en la interpretación y aplicación del presente contrato, se someten a la jurisdicción de los Juzgados y Tribunales de _____, con renuncia expresa al fuero que por Ley pudiera corresponderles.

Y en prueba de conformidad, las partes suscriben el presente contrato, en duplicado ejemplar y a un solo efecto, en la ciudad y fecha al inicio indicados.

Firmado:	Firmado:
D. _____	*D.* _____
EL RESPONSABLE	EL ENCARGADO

ANEXO IV. DOCUMENTO DE SEGURIDAD

El artículo 9 de la LOPD establece que el responsable del fichero, y en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativa que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, etc. Además el artículo 8 del Reglamento de Medidas de Seguridad establece que esas medidas estén contenidas en un documento denominado Documento de seguridad.

Debido a la complejidad de este apartado, se recomienda la contratación de un consultor especializado en Protección de Datos para su correcto cumplimiento.

No obstante, podemos encontrar diferentes modelos de Documento de seguridad en las páginas Web de la Agencia Española de Protección de Datos.

- Agencia Española de Protección de Datos:
  http://www.agpd.es

También existen aplicaciones informáticas que puede utilizar a tal efecto.

ANEXO V. FUNCIONES Y OBLIGACIONES DE LOS USUARIOS

Aportamos aquí un ejemplo de hoja informativa a firmar por las personas que en la organización accedan a datos personales. Habrá que adaptar este modelo en función de los datos a los que acceda: si son datos automatizados o no.

DECLARACIÓN DE ALTA DE USUARIO DEL SISTEMA DE INFORMACIÓN

D/Dª ……, mayor de edad, declara haber sido formado e informado de las obligaciones que asume como usuario del sistema de información de …….. con acceso a datos personales, especialmente de las siguientes:

1. OBLIGACIONES GENERALES

1. Guardar el necesario secreto respecto a cualquier tipo de información de carácter personal conocida en función del trabajo desarrollado, incluso una vez concluida la relación laboral con la organización.

2. Guardar todos los soportes físicos y/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.

3. Queda prohibido el traslado de cualquier soporte, listado o documento con datos de carácter personal en los que se almacene información titularidad de la organización fuera de los locales de la misma, sin autorización previa del Responsable de Seguridad. En el supuesto de existir traslado o distribución de

soportes y documentos se realizará cifrando dichos datos, o mediante otro mecanismo que el acceso o manipulación de la información por terceros.

4. Ficheros de carácter temporal o copias de documentos son aquellos en los que se almacenan datos de carácter personal, generados para el cumplimiento de una necesidad determinada o trabajos temporales y auxiliares, siempre y cuando su existencia no sea superior a un mes. Estos ficheros de carácter temporal o copias de documentos deben ser borrados una vez hayan dejado de ser necesarios para los fines que motivaron su creación y, mientras estén vigentes, deberán cumplir con los niveles de seguridad asignados por el Responsable de Seguridad. Si, transcurrido el mes, el usuario necesita continuar utilizando la información almacenada en el fichero, deberá comunicarlo al Responsable de Seguridad, para adoptar las medidas oportunas sobre el mismo.

5. Únicamente las personas autorizadas en un listado de accesos podrán introducir, modificar o anular los datos contenidos en los ficheros o documentos objeto de protección. Los permisos de acceso de los usuarios son concedidos por el Responsable de Seguridad. En el caso de que cualquier usuario requiera, para el desarrollo de su trabajo, acceder a ficheros o documentos a cuyo acceso no está autorizado, deberá ponerlo en conocimiento del Responsable de Seguridad correspondiente.

6. Comunicar al Responsable de Seguridad, conforme al procedimiento de notificación, las incidencias de seguridad de las que tenga conocimiento.

2. OBLIGACIONES RESPECTO A LA INFORMACIÓN CONTENIDA EN LOS FICHEROS AUTOMATIZADOS

1. Cambiar las contraseñas a petición del sistema o cuando corresponda.

2. Cerrar o bloquear todas las sesiones al término de la jornada laboral o en el supuesto de ausentarse temporalmente de su puesto de trabajo, a fin de evitar accesos no autorizados.

3. No copiar la información contenida en los ficheros en los que se almacenen datos de carácter personal al ordenador personal, disquetes, portátil o a cualquier otro soporte sin autorización expresa del Responsable de Seguridad correspondiente.

4. Guardar todos los ficheros con datos de carácter personal en la carpeta indicada por el Responsable de Seguridad correspondiente a fin de facilitar la aplicación de las medidas de seguridad que les correspondan.

5. Los usuarios tiene prohibido el envío de información de carácter personal de nivel alto, salvo autorización expresa del Responsable de seguridad que tenga asignada esta tarea. En todo caso, este envío únicamente podrá realizarse si se adoptan los mecanismos necesarios para evitar que la información no sea inteligible ni manipulada por terceros.

6. Los usuarios no podrán, salvo autorización expresa del Responsable de Seguridad que tenga asignada esta tarea, instalar cualquier tipo de programas informáticos o dispositivos ni en los servidores centrales ni en el ordenador empleado en el puesto de trabajo.

7. Queda prohibido:
a. Emplear identificadores y contraseñas de otros usuarios para acceder al sistema.
b. Intentar modificar o acceder al registro de accesos habilitado por el Responsable de Seguridad competente.
c. Burlar las medidas de seguridad establecidas en el sistema informático, intentando acceder a ficheros o programas cuyo acceso no le haya sido permitido.
d. Enviar correos masivos (spam) empleando la dirección de correo electrónico corporativa.
g. Y en general, el empleo de la red corporativa, sistemas informáticos y cualquier medio puesto al alcance del usuario vulnerando el derecho de terceros, los propios de la organización, o bien para la realización de actos que pudieran ser considerados ilícitos.
Las obligaciones sólo serán exigibles a los usuarios en tanto en cuanto la organización disponga los medios adecuados en cada caso.

3. OBLIGACIONES RESPECTO DE LA INFORMACIÓN CONTENIDA EN FICHEROS NO AUTOMATIZADOS

Por lo que respecta a los ficheros no automatizados tiene las siguientes obligaciones:

1. Mantener debidamente custodiadas las llaves de acceso a la organización, 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 seguridad competente cualquier hecho que pueda haber comprometido esa custodia.

2. 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.

3. Asegurarse de que no quedan documentos impresos que contengan datos de carácter personal impresos en la bandeja de salida de la impresora o fax.

4. Evitar (cuando se produzcan copias o reproducción de documentos) que puedan acceder a las copias personas no autorizadas a ello. Las obligaciones sólo serán exigibles a los usuarios en tanto en cuanto la organización disponga los medios adecuados en cada caso. El incumplimiento por parte de los usuarios de cualquiera de las obligaciones aquí establecidas será considerado como una falta grave, imponiéndose las sanciones previstas para este tipo de faltas especificadas el la normativa laboral de aplicación a la entidad.

Firmado: ……..……