Consejo General de la Psicología ESPAÑA
Miembro de la Federación Europea de Asociaciones de Psicólogos

Conde Peñalver, 45. 3º
28006 Madrid · España
Tel.: +34 91 444 90 20
Fax: +34 91 309 56 15
secop@cop.es
www.cop.es

CIRCULAR INFORMATIVA

Tratamiento y custodia de datos personales de pacientes en el ejercicio profesional de la psicología y uso de software de gestión clínica

Destinatarios: Profesionales de la psicología colegiados
Objeto: Recordatorio del marco de responsabilidades en materia de protección de datos en el uso de plataformas digitales de gestión clínica.

1. Introducción

El ejercicio profesional de la psicología implica el tratamiento de **datos personales especialmente sensibles**, en particular datos relativos a la salud.

La incorporación de **software de gestión clínica y plataformas digitales (SaaS)** en la práctica profesional aporta importantes ventajas organizativas y asistenciales, pero también exige **reforzar las garantías de protección de datos personales** y clarificar adecuadamente las responsabilidades entre los profesionales sanitarios y los proveedores tecnológicos.

Esta circular tiene como finalidad recordar el **marco normativo aplicable y las principales obligaciones que deben observar los profesionales de la psicología** en el uso de herramientas digitales para la gestión clínica.

2. Condición del profesional como responsable del tratamiento

El profesional de la psicología actúa como **responsable del tratamiento de los datos personales de sus pacientes**, ya que decide sobre la finalidad y los medios del tratamiento.

Esta responsabilidad se regula principalmente en:

- **Reglamento (UE) 2016/679 (RGPD)** relativo a la protección de datos personales.
- **Ley Orgánica 3/2018**, de Protección de Datos Personales y garantía de los derechos digitales.

El profesional es, por tanto, **el principal responsable de garantizar el tratamiento adecuado de los datos personales de los pacientes**.

Puntos clave para colegiados

- *El profesional **siempre es responsable frente al paciente**.*
- *Los **datos de salud requieren un nivel máximo de protección**.*
- *La digitalización de la práctica clínica **no reduce la responsabilidad del profesional**.*
- *Deben aplicarse **medidas técnicas y organizativas de seguridad adecuadas**.*

Conde Peñalver, 45. 3º
28006 Madrid · España
Tel.: +34 91 444 90 20
Fax: +34 91 309 56 15
secop@cop.es
www.cop.es

3. Uso de software clínico y plataformas digitales

Cuando se utilizan herramientas digitales de gestión clínica, el proveedor tecnológico actúa como **encargado del tratamiento**, es decir, trata los datos **por cuenta del profesional**.

No obstante, el uso de estos servicios **no transfiere la responsabilidad del tratamiento**, sino que únicamente supone la externalización de determinadas funciones técnicas.

Puntos clave

- *El **proveedor no es responsable directo frente al paciente**.*
- *El **profesional debe seleccionar y supervisar al proveedor tecnológico**.*
- *Es **obligatorio formalizar un contrato de encargo de tratamiento** conforme al RGPD.*

4. Requisitos para contratar proveedores tecnológicos

Antes de utilizar una plataforma digital de gestión clínica, el profesional debe formalizar un **contrato de encargo de tratamiento** con el proveedor tecnológico.

Este contrato debe garantizar, al menos:

- Confidencialidad en el tratamiento de los datos.
- Implementación de **medidas de seguridad adecuadas**.
- Uso de los datos **exclusivamente para la prestación del servicio contratado**.
- Regulación de posibles **subcontrataciones**.

Además, el profesional debe verificar que el proveedor ofrece **garantías técnicas y organizativas suficientes**.

Puntos clave

- *No utilizar **software sin garantías de cumplimiento del RGPD**.*
- *Verificar **dónde se almacenan los datos personales**.*
- *Exigir medidas de seguridad como **cifrado, control de accesos y registro de actividad**.*

Conde Peñalver, 45. 3º
28006 Madrid · España
Tel.: +34 91 444 90 20
Fax: +34 91 309 56 15
secop@cop.es
www.cop.es

5. Brechas de seguridad

Una **brecha de seguridad** implica cualquier incidente que provoque:

- acceso no autorizado a datos personales,
- pérdida de información,
- alteración de los datos,
- o divulgación indebida de los mismos.

Cuando se produce un incidente de seguridad:

1. El **proveedor tecnológico debe comunicarlo al profesional**.
2. El **profesional debe evaluar el riesgo para los derechos y libertades de los pacientes**.
3. En función del nivel de riesgo, deberá realizar las notificaciones correspondientes.

Enlaces de interés:

- Guia AEPD para notificación de brechas de datos
- Infografía
- Formulario de notificación de brecha a la AEPD

Notificación a la autoridad de control

Cuando exista riesgo para los derechos y libertades de los afectados, el profesional deberá **notificar la brecha a la Agencia Española de Protección de Datos (AEPD)** en un plazo máximo de **72 horas** desde que tenga conocimiento del incidente.

La notificación puede realizarse a través del formulario habilitado en la **Sede Electrónica de la AEPD**.

Comunicación a los pacientes

Cuando la brecha suponga **un alto riesgo para los derechos y libertades de los afectados,** el responsable del tratamiento deberá comunicar la incidencia a los pacientes **sin dilación indebida**, conforme al artículo 34 del RGPD.

*¿Qué significa **un alto riesgo para los derechos y libertades de los afectados?:** En palabras simples, significa que el uso o tratamiento de datos personales podría causar daños importantes a las personas cuyos datos se están usando.*

*Es decir, existe la posibilidad de que **los derechos fundamentales o la vida privada de una persona se vean perjudicados***

Esta comunicación deberá:

- utilizar **un lenguaje claro y comprensible**,

Conde Peñalver, 45. 3º
28006 Madrid · España
Tel.: +34 91 444 90 20
Fax: +34 91 309 56 15
secop@cop.es
www.cop.es

- explicar la naturaleza de la brecha,
- informar de las posibles consecuencias,
- indicar las medidas adoptadas para mitigar el incidente.

Puntos clave

- *El plazo máximo de notificación es **72 horas**.*
- *La **evaluación del riesgo corresponde al profesional**.*
- *En determinados casos será necesario **informar directamente a los pacientes**.*

6. Responsabilidad frente a los pacientes

El profesional responde frente al paciente **incluso cuando la brecha de seguridad se origine en los sistemas del proveedor tecnológico**.

No obstante, en caso de incumplimiento contractual por parte del proveedor, el profesional podrá **ejercer acciones de reclamación contra el mismo**.

Puntos clave

- *El paciente **reclama directamente al profesional**.*
- *El profesional puede **reclamar posteriormente al proveedor**.*
- *Puede existir **responsabilidad compartida**, pero el responsable visible ante el paciente es el profesional.*

7. Ejemplo práctico

Supuesto:

Un software de gestión clínica sufre un **ciberataque** que provoca la exposición de datos personales de pacientes.

Procedimiento:

1. El proveedor tecnológico **informa del incidente al profesional**.
2. El profesional **analiza la naturaleza del incidente y evalúa el riesgo**.
3. Si existe riesgo para los derechos de los afectados → **notificación a la AEPD**.
4. Si el riesgo es alto → **comunicación directa a los pacientes afectados**.

Conde Peñalver, 45. 3º
28006 Madrid · España
Tel.: +34 91 444 90 20
Fax: +34 91 309 56 15
secop@cop.es
www.cop.es

8. Distribución de responsabilidades

Ámbito	Profesional	Proveedor
Control del tratamiento	✓	✗
Seguridad técnica	Supervisa	Implementa
Notificación de brechas	✓ AEPD / pacientes	Informa al profesional
Responsabilidad frente al paciente	✓	✗

9. Recomendaciones finales

Se recomienda a los profesionales:

- Utilizar **software de gestión clínica con garantías de cumplimiento normativo**.
- Formalizar **contratos de encargo de tratamiento** con los proveedores tecnológicos.
- Aplicar **medidas de seguridad adecuadas** para la protección de datos.
- Establecer **protocolos internos de actuación ante brechas de seguridad**.

10. Conclusión

La digitalización de la práctica clínica no modifica el principio fundamental de responsabilidad del profesional sanitario.

El profesional de la psicología debe **garantizar en todo momento la confidencialidad, integridad y disponibilidad de los datos personales de sus pacientes**, incluso cuando utiliza herramientas tecnológicas proporcionadas por terceros.

Conde Peñalver, 45. 3º
28006 Madrid · España
Tel.: +34 91 444 90 20
Fax: +34 91 309 56 15
secop@cop.es
www.cop.es

11. FAQ

¿Es necesario disponer de un Delegado de Protección de Datos (DPD)?

La designación de un **Delegado de Protección de Datos (DPO)** es obligatoria cuando se cumplen determinadas circunstancias establecidas por el **RGPD y la LOPDGDD**.

Es obligatorio nombrar un DPO cuando:

- El centro realiza **tratamiento de datos de salud**, considerados **categorías especiales de datos**.
- Dicho tratamiento se realiza **a gran escala**.
- Se trata de **centros sanitarios, clínicas psicológicas, hospitales o entidades que gestionan historiales clínicos de numerosos pacientes**.
- El tratamiento de datos se realiza de forma **sistemática y organizada dentro de una actividad sanitaria**.

No suele ser obligatorio cuando:

- Se trata de un **psicólogo autónomo que atiende pacientes de forma individual**.
- El tratamiento de datos **no se realiza a gran escala**.

En cualquier caso, aunque no exista obligación de nombrar un DPO, los profesionales de psicología deben **cumplir igualmente con todas las obligaciones en materia de protección de datos**, como la confidencialidad, la seguridad de la información y la correcta gestión de los historiales clínicos.

Con más tiempo, este apartado de FAQ puede contener otras cuestiones que creáis que precisen aclaración