

Checklist RGPD 2026 para Psicólogos

Verifica el cumplimiento de tu consulta con el Reglamento General de Protección de Datos

Como psicólogo, tratas datos de salud (categoría especial según el RGPD), lo que implica obligaciones reforzadas. Marca cada punto que ya tienes implementado en tu consulta. Si hay elementos sin marcar, actúa cuanto antes para evitar sanciones de la AEPD.

1. DOCUMENTOS Y FORMULARIOS

- ☐ Consentimiento informado incluye cláusula de protección de datos
- ☐ El paciente firma el consentimiento antes de la primera sesión
- ☐ Conservas copia firmada del consentimiento en el expediente
- ☐ La hoja de información identifica al Responsable del Tratamiento
- ☐ Explicas la finalidad y los plazos de conservación de datos (recomendado: 5 años)
- ☐ Informas de los derechos ARSOPOL del paciente
- ☐ Para menores de 14 años, cuentas con consentimiento del representante legal

2. REGISTRO DE ACTIVIDADES DE TRATAMIENTO (RAT)

- ☐ Tienes un RAT documentado y actualizado (obligatorio al tratar datos de salud)
- ☐ El RAT recoge: finalidad, categorías de datos, destinatarios y plazos
- ☐ Describes las medidas de seguridad técnicas y organizativas aplicadas
- ☐ El RAT está disponible para la AEPD si lo solicita

3. MEDIDAS DE SEGURIDAD TÉCNICAS

- ☐ El ordenador/tablet tiene contraseña robusta y cifrado de disco activo
- ☐ Realizas copias de seguridad periódicas (mínimo semanal) y cifradas
- ☐ Tienes antivirus actualizado en todos los dispositivos
- ☐ Los expedientes en papel están bajo llave cuando no los usas
- ☐ No envías información clínica por WhatsApp no cifrado
- ☐ Las videoconferencias se hacen por plataformas con cifrado extremo a extremo
- ☐ Tienes procedimiento de destrucción segura de documentos en papel

4. PROVEEDORES Y ENCARGADOS DE TRATAMIENTO

- ☐ Tu software de gestión clínica tiene contrato de encargado de tratamiento
- ☐ Tu gestor contable/fiscal tiene cláusula de confidencialidad firmada

- ☐ Cualquier tercero que acceda a datos de pacientes tiene contrato firmado

5. WEB Y COMUNICACIONES DIGITALES

- ☐ Tu web tiene Política de Privacidad visible y actualizada
- ☐ Tienes banner de cookies con consentimiento por categorías
- ☐ Los formularios de contacto incluyen casilla de aceptación NO premarcada
- ☐ Tu web usa HTTPS (SSL activo)
- ☐ Solo envías emails/newsletter a quienes dieron consentimiento explícito
- ☐ Incluyes enlace de baja en cada comunicación comercial

6. DERECHOS DE LOS PACIENTES

- ☐ Tienes proceso para responder solicitudes de derechos en plazo (1 mes max)
- ☐ Sabes gestionar solicitudes de acceso, rectificación y supresión
- ☐