

DETALLE DE ACTUACIONES DEL SERVICIO DE CONSULTORÍA PARA EL CUMPLIMIENTO DE LA NORMATIVA GENERAL DE PROTECCIÓN DE DATOS (RGPD-LOPD)

PACK DE PROTECCIÓN ESTÁNDAR PERSONALIZADO TARIFA PLANA

Actuaciones de adecuación inicial el primer año:

1. **DESIGNACIÓN DEL DELEGADO EN PROTECCIÓN DE DATOS (DPO)** si resultase obligatorio o designación voluntaria si así lo decide el Responsable. En caso de no ser necesario se designará a un coordinador para la adaptación al RGPD y posterior auditoria anual.*
2. **Verificación de la LICITUD DEL TRATAMIENTO:** identificación y documentación de la finalidad y la base jurídica sobre la que se desarrollan los tratamientos (relación contractual, normativa con rango de ley, consentimiento inequívoco del interesado, interés legítimo del Responsable, etc.) (Art. 6 RGPD), prestando especial atención al tratamiento de categorías especiales de datos (Art. 9 RGPD) y el tratamiento de datos relativos a condenas e infracciones penales (Art. 10 RGPD).
3. Confección y elaboración personalizada del **REGISTRO DE ACTIVIDADES DEL TRATAMIENTO**, una vez analizados los datos y comprobado la licitud del tratamiento de acuerdo a lo indicado en el punto dos. (**Acreditación de la diligencia en el cumplimiento del Reglamento General de Protección de Datos - AEPD**).
4. Realización de un **ANÁLISIS DE RIESGOS**, con objeto de determinar qué actuaciones resultan necesarias llevar a cabo para eliminar o mitigar los riesgos de violaciones de seguridad.
5. **Implantación de las MEDIDAS DE SEGURIDAD:** asesoramiento e indicaciones del consultor con relación a las actuaciones que se han de llevar a cabo para implantar las medidas técnicas y organizativas necesarias, una vez revisado el resultado obtenido del análisis de riesgos indicado en el punto cuatro.
6. Aplicación de la **PROTECCIÓN DE DATOS DESDE EL DISEÑO Y POR DEFECTO:** asesoramiento e indicaciones del consultor de las medidas de seguridad que debe aplicar el responsable con anterioridad al inicio del tratamiento y también durante su desarrollo, cuando se diseña un tratamiento, un producto o un servicio que implique tratamientos de datos personales. — *Aplicación del criterio de la Responsabilidad Proactiva.*
7. Establecimiento de mecanismos y los procedimientos a seguir para la **NOTIFICACION DE QUIEBRAS DE SEGURIDAD** a la Agencia Española de Protección de Datos y, si resultase necesario, al afectado.
8. Realización de una **EVALUACIÓN DE IMPACTO** obligatoria, si se detecta que el tratamiento de datos entraña un alto riesgo para los derechos y libertades de las personas físicas. (Art. 35 y 36 RGPD)*
9. Detección de **TRATAMIENTO DE DATOS PERSONALES CON FINES DE VIGILANCIA** a través de sistemas de cámaras o videocámaras Videovigilancia y sistemas de alarma con dispositivo de captura fotográfica (Instrucción 1/2006, de 8 de Noviembre, de la Agencia Española de Protección de Datos).*
10. Detección de **TRANSFERENCIAS INTERNACIONALES DE DATOS:** comunicación y/o cesiones de datos personales a terceros países u organizaciones internacionales (Art. 44, 45, 46, 47 y 48 RGPD)*



11. **CONFECCIÓN Y REDACCIÓN PERSONALIZADA de la siguiente DOCUMENTACIÓN LEGISLATIVA**, una vez obtenidos los datos y la información necesaria:
 - 11.1 CONTRATOS CON LOS ENCARGADOS DEL TRATAMIENTO.
 - 11.2 CARTAS DE CONFIDENCIALIDAD PARA LOS USUARIOS CON ACCESO.
 - 11.3 GUÍA LOPD DEL USUARIO (formación básica sobre la normativa de protección de datos enfocada al personal que realiza tratamiento de datos de carácter personal durante sus funciones profesionales).
 - 11.4 TEXTOS LEGALES PARA LAS DISTINTAS FINALIDADES (deber de información en la captura de datos, consentimiento expreso y escrito para el tratamiento de categorías especiales de datos y para los envíos de comunicaciones comerciales a través de diferentes canales: e-mail, SMS, etc., Aviso Legal, Política de privacidad, Política de cookies, etc.).
 - 11.5 OTROS DOCUMENTOS que se estimen necesarios.
12. **DOCUMENTACIÓN de las MEDIDAS DE SEGURIDAD implantadas y las ACTUACIONES REALIZADAS.** (Acreditación de la diligencia en el cumplimiento del Reglamento General de Protección de Datos - AEPD).
13. Establecimiento de **procedimientos y canales para FACILITAR AL INTERESADO EL EJERCICIO DE SUS DERECHOS y la CAPACIDAD DE PODER ATENDER ESTAS PETICIONES** de forma eficiente y efectiva. (Art. 15, 16, 17 18, 19 20, 21 y 22 RGPD).
14. **GARANTÍAS DEL CUMPLIMIENTO DEL RGPD por parte del ENCARGADO DEL TRATAMIENTO y demás obligaciones que le afectan de manera directa** (Art. 28 y 29 RGPD).
15. Verificación del cumplimiento de los **PRINCIPIOS RELATIVOS AL TRATAMIENTO** (Art. 5 RGPD):
 - 15.1.1 **Licitud, lealtad y transparencia:** datos tratados de manera lícita, leal y transparente.
 - 15.1.2 **Limitación de la finalidad:** recogidos para fines determinados, explícitos y legítimos no pudiendo ser tratados ulteriormente de manera incompatible con dichos fines.
 - 15.1.3 **Minimización de datos:** adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.
 - 15.1.4 **Exactitud:** los datos deben ser exactos siendo actualizados si resultase necesarios. Si suprimirán o rectificarán, sin dilación indebida, los datos que sean inexactos con respecto a los fines para los que se tratan.
16. **Solicitud del CONSENTIMIENTO AL INTERESADO y la CAPACIDAD del Responsable DE DEMOSTRAR SU OBTENCIÓN** (Art. 7 RGPD).
17. **Cumplimiento del DEBER DE INFORMACIÓN** al interesado en la captura de sus datos personales. Cómo proceder cuando los datos no se hayan obtenido del interesado (información por capas, canales y métodos utilizados para facilitar dicha información y la capacidad de demostrar que las actuaciones son acordes al RGPD) (Art. 13 y 14 RGPD).
18. **Activación de PLATAFORMA PRIVADA RGPD-LOPD y el alojamiento de toda la documentación legislativa personalizada y actualizada.**
19. **Emisión de un CERTIFICADO RGPD-LOPD**, de disposición de un proyecto de adecuación a la normativa general de protección de datos.
20. **Servicio de ATENCIÓN JURÍDICA EL PRIMER AÑO** por parte de un consultor experto en protección de datos.
21. **Envío de BOLETINES Y OTRAS NOTICIAS E INFORMACIÓN DE INTERÉS** vía e-mail, **en materia de protección de datos.**
22. Asesoramiento para el desarrollo y la implantación de un **PLAN DE FORMACIÓN** sobre la Normativa General de Protección de Datos para los empleados y usuarios que realicen tratamientos de datos.



Actuaciones de revisión a partir del segundo año – AUDITORÍA:

23. **ENTREVISTA PERSONAL ANUAL, VÍA TELEFÓNICA, CON UN CONSULTOR**, quien determinará si las medidas técnicas y organizativas han sido debidamente implantadas en la entidad, así como si el resto de políticas y actuaciones establecidas resultan las más adecuadas acorde a la naturaleza, el ámbito, el contexto y los fines de tratamiento de datos. Si se detectasen nuevas zonas de riesgo o las medidas establecidas resultasen ineficientes, el consultor facilitará las indicaciones correspondientes.
24. **REVISIÓN Y ACTUALIZACIÓN DE MEDIDAS** tras el análisis de los mecanismos y procedimientos que se estén llevando a cabo de acuerdo a los siguientes apartados (Art. 24,25,26 y 32 RGPD):
 - 24.1 **Principios relativos al tratamiento** (Art. 5 RGPD):
 - 24.1.1 **Licitud, lealtad y transparencia:** datos tratados de manera lícita, leal y transparente.
 - 24.1.2 **Limitación de la finalidad:** recogidos para fines determinados, explícitos y legítimos no pudiendo ser tratados ulteriormente de manera incompatible con dichos fines.
 - 24.1.3 **Minimización de datos:** adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.
 - 24.1.4 **Exactitud:** los datos deben ser exactos siendo actualizados si resultase necesarios. Si suprimirán o rectificarán, sin dilación indebida, los datos que sean inexactos con respecto a los fines para los que se tratan.
 - 24.2 **Licitud del tratamiento:** identificar y documentar la base legal sobre la que se desarrollan los tratamientos (relación contractual, normativa con rango de ley, consentimiento inequívoco del interesado, interés legítimo del Responsable, etc.) (Art. 6 RGPD), prestando especial atención al tratamiento de categorías especiales de datos (Art. 9 RGPD) y el tratamiento de datos relativos a condenas e infracciones penales (Art. 10 RGPD).
 - 24.3 **Garantías del cumplimiento del RGPD por parte del Encargado del Tratamiento** y demás obligaciones que le afectan de manera directa (Art. 28 y 29 RGPD).
 - 24.4 Procedimientos y notificaciones de **QUIEBRAS DE SEGURIDAD**.
 - 24.5 **Garantías del cumplimiento del RGPD por parte de los usuarios autorizados** al tratamiento de los ficheros del Responsable.
 - 24.6 **Solicitud del consentimiento al interesado y la capacidad del Responsable de demostrar su obtención** (Art. 7 RGPD).
 - 24.7 **Cumplimiento del deber de información** al interesado en la captura de sus datos personales. Cómo proceder cuando los datos no se hayan obtenido del interesado (información por capas, canales y métodos utilizados para facilitar dicha información y la capacidad de demostrar que las actuaciones son acordes al RGPD) (Art. 13 y 14 RGPD).
 - 24.8 El establecimiento de **procedimientos y canales para facilitar al interesado el ejercicio de sus derechos** y tener **la capacidad de poder atender estas peticiones** de forma eficiente y efectiva. (Art. 15, 16, 17 18, 19 20, 21 y 22 RGPD).
 - 24.9 **Inclusión de Textos Legales** en páginas webs, blogs corporativos u otros entornos hipermedia asistidos por redes de ordenadores que se detecten: Reglamento Europeo de Protección de Datos —**RGPD**— y La Ley Orgánica de Protección de Datos —**LOPD**—, la Ley de Servicios de la Sociedad de la Información y el Comercio Electrónico —**LSSI+CE**— (Aviso Legal, Política de Privacidad y Política de Cookies).
25. **IMPLANTACIÓN DE MEDIDAS CORRECTORAS:** asesoramiento e indicaciones del consultor sobre las medidas correctoras y las actuaciones que se han de llevar a cabo aplicables a las deficiencias detectadas a la luz de los resultados obtenidos tras la auditoría anual.



26. **Recomendaciones y asesoramiento** para la **RECOGIDA Y TRATAMIENTO DE DATOS EN INTERNET** (páginas webs, redes sociales, blogs corporativos, etc), el tratamiento de datos en la nube “**CLOUD COMPUTING**” y la verificación de los procedimientos para atender los derechos de los ciudadanos.
27. **Revisión del PLAN DE FORMACIÓN RGPD-LOPD**: el consultor asesorará y facilitará recursos y herramientas para la correcta formación de empleados en materia de protección de datos.
28. **CONFECCIÓN Y REDACCION PERSONALIZADA** de toda la documentación legislativa que se estime necesaria tras la auditoría anual (Contratos de Encargo, Textos Legales, Documentos de Confidencialidad, etc).
29. **Actualización del REGISTRO DE ACTIVIDADES DEL TRATAMIENTO**
30. **Actualización del DOCUMENTO de MEDIDAS DE SEGURIDAD implantadas y ACTUACIONES REALIZADAS.** (Acreditación de la diligencia en el cumplimiento del Reglamento General de Protección de Datos - AEPD).
31. Servicio de **ATENCIÓN JURÍDICA PERMANENTE** por parte de un consultor experto en protección de datos.
32. **ALOJAMIENTO EN LA PLATAFORMA PRIVADA** de toda la documentación legislativa personalizada y actualizada una vez finalizada la revisión anual.
33. Emisión del **CERTIFICADO ANUAL RGPD-LOPD**, de disposición de un proyecto de adecuación a la normativa general de protección de datos.

NOTAS

**La Evaluación de Impacto se llevará a cabo previa aceptación del presupuesto.*

** La legitimación de los sistemas de cámaras o videocámaras se llevará a cabo previa aceptación del presupuesto.*

**Si la designación del Delegado en Protección de Datos resulta obligatoria, el Responsable podrá designar a PRODASUR, previa aceptación del presupuesto.*

**Si se detectasen Transferencias Internacionales de Datos, el consultor informará al Responsable y procederá a la legitimación de acuerdo a las disposiciones legales en materia de protección de datos, previa aceptación del presupuesto.*



PRODASUR es miembro de la Asociación Profesional de Consultores en Protección de Datos y de la Asociación Profesional de Privacidad. Prodasur le garantiza el servicio de consultoría contratado mediante una póliza de Responsabilidad Civil que cubre las posibles sanciones que le pudieran ser impuestas debido a deficiencias en el servicio prestado.