

ANEXO DE PROTECCIÓN DE DATOS PERSONALES - ENCARGADO DEL TRATAMIENTO

GRUPO DE PROTECCIÓN Y SEGURIDAD 909 SA será considerado ENCARGADO DEL TRATAMIENTO (en adelante ENCARGADO) cuando el CLIENTE actúe como profesional, fuera de la excepción doméstica prevista o es una empresa, y por ello según legislación vigente tendrá la consideración de RESPONSABLE DEL TRATAMIENTO (en adelante RESPONSABLE) de las imágenes y videos provenientes del sistema de captación.

Ambas partes tratarán los datos personales, conforme a lo dispuesto en el Reglamento (UE) 2016/679, de 27 de abril de 2016 (GDPR), y la Ley Orgánica 3/2018, de 5 de diciembre (LOPDGDD).

El RESPONSABLE declara que ha contratado los servicios del ENCARGADO consistentes en:

- Videovigilancia.
- Videoverificación.
- Otros servicios propios que pueden implicar el acceso a datos de carácter personal.

Siendo conocedor que, para el cumplimiento de dichos servicios, al ENCARGADO le resulta necesario el acceso y tratamiento de los datos personales de su competencia como RESPONSABLE.

La duración de este documento queda vinculada al tiempo establecido en el contrato de servicios que mantiene con el ENCARGADO.

En cumplimiento de lo dispuesto en el artículo 28 del GDPR, el ENCARGADO ofrece suficientes garantías para implementar políticas técnicas y organizativas apropiadas para aplicar las medidas de seguridad que establece la normativa vigente y proteger los derechos de los interesados, por lo cual ambas partes se someten a cumplir las siguientes obligaciones e instrucciones para el tratamiento de datos:

1. Objeto, naturaleza y finalidad del encargo

- Finalidad del encargo: Servicios de seguridad.
- Deber de informar el tratamiento al interesado: corresponderá exclusivamente al RESPONSABLE.
- Ubicación del tratamiento: en los locales del ENCARGADO, con autorización del RESPONSABLE para incorporar los datos a sus sistemas.

2. Tipo de datos personales y categoría de interesados

- Tipo de datos personales a los que tendrá acceso el ENCARGADO: datos personales básicos (nombre y apellidos, número de DNI, dirección postal, número de teléfono, dirección de correo electrónico, datos bancarios, imagen y voz).
- Categorías de interesados: Empleados, Clientes y usuarios, Proveedores, Asociados y miembros, Propietarios o arrendatarios, Personas de contacto.
- Operaciones de tratamiento autorizadas: las estrictamente necesarias para alcanzar la finalidad del encargo.

3. Obligaciones y derechos del RESPONSABLE

El RESPONSABLE adoptara todas las obligaciones impuestas por la normativa de protección de datos y en concreto y de forma no limitativa, las siguientes:

- Obligación de determinar las medidas de seguridad necesarias.
- Obligación de comunicar las brechas de seguridad en setenta y dos horas a la Agencia Española de Protección de Datos y, en su caso, a los interesados.
- Obligación de instalar carteles informativos donde se haga mención expresa al RGPD, quien es el responsable de los datos y la dirección de correo donde cualquier interesado pueda ejercer sus derechos.
- Obligación de disponer de un documento informativo, a disposición de cualquier interesado, donde haciendo mención al RGPD, se informe del tratamiento de los datos personales, del titular de los mismos, los fines de la captación de las imágenes, los derechos con que cuenta cualquier persona que pueda verse afectada y la dirección de correo donde poder ejercerlos.

El RESPONSABLE garantiza que los datos facilitados al ENCARGADO se han obtenido lícitamente y que son adecuados, pertinentes y limitados a los fines del tratamiento.

El RESPONSABLE pondrá a disposición del ENCARGADO cuanta información sea necesaria para ejecutar las prestaciones objeto del encargo.

El RESPONSABLE realizará, en caso de ser exigible por la normativa de protección de datos, una evaluación del impacto en la protección de datos personales de las operaciones de tratamiento.

El RESPONSABLE advierte al ENCARGADO de que, si determina por su cuenta los fines y los medios del tratamiento, se considerará responsable del tratamiento y estará sujeto a cumplir las disposiciones de la normativa vigente aplicables como tal.

4. Obligaciones y derechos del ENCARGADO

El ENCARGADO se obliga a respetar todas las obligaciones que pudieran corresponderle como encargado del tratamiento conforme a lo dispuesto en la normativa vigente y cualquier otra disposición o regulación que le fuera igualmente aplicable.

El ENCARGADO no destinará, aplicará o utilizará los datos a los que tenga acceso para un fin distinto al encargo o que suponga el incumplimiento de este contrato.

El ENCARGADO pondrá a disposición del RESPONSABLE la información necesaria para demostrar el cumplimiento del contrato, permitiendo las inspecciones y auditorías necesarias para evaluar el tratamiento.

El ENCARGADO designará un delegado de protección de datos y comunicará su identidad y datos de contacto al responsable. Puede contactar con el delegado de protección de datos del ENCARGADO enviando un correo electrónico a: dpo@gps909.com

Identificación del Delegado de Protección de Datos

Nombre: ADELDPD CONSULTORES IBIZA SL
Dirección: Cº Viejo de San Mateo, Km. 2,700, 07813 Puig d'en Valls
CIF: B16638942
Teléfono: 971334757
E-mail: delegado@adelopdconsultores.com
Web: www.adelopdconsultores.com

5. Personal autorizado para realizar el tratamiento

El ENCARGADO garantiza que el personal autorizado para realizar el tratamiento se ha comprometido de forma expresa y por escrito a respetar la confidencialidad de los datos o que está sujeto a una obligación legal de confidencialidad de naturaleza legal.

El ENCARGADO adoptará medidas para asegurar que cualquier persona que actúe bajo su autoridad y tenga acceso a datos personales sólo pueda tratarlos siguiendo las instrucciones del RESPONSABLE o esté obligada a ello en virtud de la legislación vigente.

El ENCARGADO manifiesta que el personal autorizado para realizar el tratamiento ha recibido la formación necesaria para asegurar que no se pondrá en riesgo la protección de datos personales.

6. Medidas de seguridad

El ENCARGADO manifiesta estar al corriente en lo que concierne a las obligaciones derivadas de la normativa de protección de datos, especialmente en lo que se refiere a la implantación de las medidas de seguridad para las diferentes categorías de datos y de tratamiento establecidas en el artículo 32 del GDPR.

El ENCARGADO expone que se implementarán adecuadamente dichas medidas de seguridad y ayudará al RESPONSABLE a cumplir las obligaciones establecidas en los artículos del 32 al 36 del GDPR, teniendo en cuenta la naturaleza del tratamiento y la información a disposición del ENCARGADO.

El RESPONSABLE realizará un análisis de los posibles riesgos derivados del tratamiento para determinar las medidas de seguridad apropiadas para garantizar la seguridad de la información tratada y los derechos de los interesados y, si determinara que existen riesgos, trasladará al ENCARGADO un informe con la evaluación de impacto para que proceda a la implementación de medidas adecuadas para evitarlos o mitigarlos.

El ENCARGADO, por su parte, deberá analizar los posibles riesgos y otras circunstancias que puedan incidir en la seguridad que le sean atribuibles, debiendo informar, si los hubiere, al RESPONSABLE para evaluar su impacto.

De todas formas, el ENCARGADO, implementará medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo que entrañe el tratamiento, que en su caso incluya, entre otros:

- Seudonimización y cifrado de datos personales.
- Garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.
- Restaurar la disponibilidad y el acceso a datos de forma rápida en caso de incidente físico o técnico.
- Procedimientos de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

En concreto, se han implementado las medidas técnicas y organizativas que, con carácter enunciativo que no limitativo, se indican a continuación:

- Medidas organizativas. Política de Seguridad de la Información y de Protección de Datos de obligado cumplimiento para todo el personal de la organización, con un modelo de gobierno claramente definido. Segregación de Funciones. Inventario de Activos.
- Medidas relativas al personal. Programa anual de formación en seguridad y privacidad. Impartición de acciones formativas, concienciación y sensibilización, en modalidad presencial, on-line y mixta, para empleados. Incorporación de condiciones en los contratos con empleados que recogen obligaciones concretas en materia de seguridad y privacidad.
- Deber de confidencialidad y secreto. Incorporación de condiciones en los contratos con empleados y proveedores que recogen la obligación de confidencialidad y el deber de secreto.

- Gestión de incidentes. Procedimiento de gestión y notificación de eventos (incidentes, vulnerabilidades, problemas, etc.), en virtud del cual los eventos se gestionan adecuadamente y se comunican al RESPONSABLE.
- Medidas relacionadas con el control del acceso físico y ambiental. Medidas de seguridad perimetrales. Protección contra el acceso no autorizado. Autorización previa para sacar de las instalaciones los soportes de almacenamiento que contengan datos personales. Entradas y salidas de las zonas de seguridad de las instalaciones restringidas y supervisadas.
- Medidas relativas al control de acceso lógico. Procedimiento de gestión de cuentas de usuarios. ID único asignado e inequívoco para cada cuenta de usuario. Trazabilidad y registro de los cambios en las cuentas de usuarios. Cuentas de acceso privilegiado restringidas. Requisitos de complejidad y seguridad de contraseñas. Roles y permisos formalmente documentados. Bloqueo de Pantallas. Registro y revisión de roles y autorizaciones concedidas.
- Medidas relativas al control de transferencia, almacenamiento y portabilidad. Transferencias y almacenamiento de datos personales cifrados, cuando corresponda. Registro de las transmisiones de datos personales a través de un soporte físico. Canal de comunicación seguro para la administración remota de los sistemas de información. Medidas para evitar la posibilidad de una exportación no autorizada de datos personales. Soporte físico utilizado para la transmisión de los datos personales cifrados. Eliminación segura de soportes informáticos.
- Control de resiliencia operacional. Herramientas para detectar y prevenir intrusiones y ciberataques. Herramientas o servicios para detectar y limitar el impacto de los ataques de denegación de servicio. Segmentación de redes de telecomunicaciones mediante cortafuegos. Medidas de protección contra las catástrofes naturales. Política de copias de seguridad.
- Control de aseguramiento y cumplimiento. Revisiones periódicas de: seguridad de los sistemas informáticos, copias de seguridad, planes de continuidad TI, controles de seguridad física y ambiental, procesos de gestión de la seguridad de la información. Procedimientos para garantizar el cumplimiento de los requisitos legales y reglamentarios.

7. Violación de la seguridad

Las violaciones de seguridad de que tenga conocimiento el ENCARGADO deberán notificarse, sin dilación indebida y en un máximo de 48 horas, al RESPONSABLE para su conocimiento y aplicación de medidas para remediar y mitigar los efectos ocasionados. No será necesaria la notificación cuando sea improbable que comporte un riesgo para los derechos y las libertades de las personas físicas.

La notificación de una violación de seguridad deberá contener, como mínimo, la siguiente información:

- Descripción de la naturaleza de la violación.
- Categorías y el número aproximado de interesados afectados.
- Categorías y el número aproximado de registros de datos afectados.
- Posibles consecuencias.
- Medidas adoptadas o propuestas para remediar o mitigar los efectos.
- Datos de contacto donde pueda obtenerse más información (DPO, responsable de seguridad, etc.).

8. Comunicación de los datos a terceros

El ENCARGADO no podrá comunicar los datos a terceros destinatarios, salvo que hubiera obtenido una autorización previa y por escrito del RESPONSABLE; la cual, de existir, se anejará al presente contrato.

La transmisión de datos a autoridades públicas en el ejercicio de sus funciones, no son consideradas comunicaciones de datos, por lo que no se precisará de la autorización del RESPONSABLE si dichas transmisiones son necesarias para alcanzar la finalidad del encargo.

9. Transferencias internacionales de datos

El ENCARGADO no podrá realizar transferencias de datos a terceros países u organizaciones internacionales no establecidos en la UE, salvo que hubiera obtenido una autorización previa y por escrito del RESPONSABLE; la cual, de existir, se anexará al presente contrato.

10. Subcontratación del tratamiento de datos

El ENCARGADO no podrá subcontratar a un tercero la realización de ningún tratamiento de datos que le hubiera encomendado el RESPONSABLE, salvo que este lo autorice de manera previa y por escrito, y quede constancia anexando la autorización al presente contrato.

11. Derechos de los interesados

El ENCARGADO creará, siempre que sea posible y teniendo cuenta la naturaleza del tratamiento, las condiciones técnicas y organizativas necesarias para asistir al RESPONSABLE en su obligación de responder a las solicitudes de los derechos del interesado.

En caso de que el ENCARGADO reciba una solicitud para el ejercicio de estos derechos, debe comunicarlo al RESPONSABLE de forma inmediata mediante correo electrónico del RESPONSABLE y, en ningún caso, más allá de 3 días laborable siguiente al de la recepción de la solicitud, adjuntando otras informaciones que puedan ser relevantes para resolverla.

12. Responsabilidad

Conforme al artículo 82 del GDPR, el RESPONSABLE responderá de los daños y perjuicios causados en cualquier operación de tratamiento en que participe y no cumpla lo dispuesto en el GDPR, y el ENCARGADO únicamente responderá de los daños y perjuicios causados por el tratamiento cuando no haya cumplido con las obligaciones del GDPR dirigidas específicamente al ENCARGADO o haya actuado al margen o en contra de las instrucciones legales del RESPONSABLE. Del mismo modo, el ENCARGADO estará exento de responsabilidad si demuestra que no es en modo alguno responsable del hecho que haya causado los daños y perjuicios.

13. Fin de la prestación de servicio

Una vez finalice la prestación de servicios objeto de este contrato, si el ENCARGADO hubiera almacenado datos personales, o cualquier otro documento y/o soporte que se le hubiera facilitado por cualquier medio, deberá devolverlas o suprimirlas a elección del RESPONSABLE, incluidas las copias existentes. El ENCARGADO deberá emitir un certificado de devolución o destrucción si así lo exigiera el RESPONSABLE.

No procederá la supresión de datos cuando se requiera su conservación por una obligación legal, en cuyo caso el ENCARGADO procederá a la custodia de los mismos bloqueando los datos y limitando su tratamiento en tanto que pudieran derivarse responsabilidades de su relación con el RESPONSABLE.

El ENCARGADO mantendrá el deber de secreto y confidencialidad de los datos incluso después de finalizar la relación objeto de este contrato.

GRUPO DE PROTECCIÓN Y SEGURIDAD 909 SA

C.I.F. A-07404197 – Inscrita en la D.G.S. el 30-10-90, con el número 1.835

Camino Viejo de San Mateo, Km. 2.700 - 07813 Puig d'en Valls (Illes Balears)