

Condiciones Específicas – Servicios Protección de Datos

PRIMERA. – Objeto y alcance.

- 1.1. Las presentes Condiciones Específicas regulan las especificaciones técnicas respecto a los servicios de consultoría y asesoramiento legal en materia de protección de datos que se suscriban entre Grupo Adaptalia Legal-Formativo S.L. (en adelante, GrupoAdaptalia® o el "Prestador") y el Cliente, y que aparecen identificados en la Hoja de Encargo o Propuesta Comercial.
- 1.2. Dicha Hoja de Encargo o Propuesta Comercial irá acompañada de una Condiciones Generales de Contratación Simplificadas, que implicarán mediante su firma, la aceptación igualmente de (i) las [Condiciones Generales Ampliadas](#) así como de (ii) las presentes Condiciones Específicas, si los servicios contratados se corresponden con uno o varios de los que detallan en la siguiente cláusula "Segunda – Detalle de los servicios en Protección de Datos".

SEGUNDA – Detalle de los servicios en Protección de Datos

- 1.1. De conformidad con la normativa de protección de protección de datos y, en concreto, el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en adelante, "RGPD"), la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, "LOPDGDD"), así como normativas conexas que pudieran ser de aplicación; GrupoAdaptalia® lleva a cabo los siguientes servicios en materia de protección de datos que se especificarán a continuación : (i) Adaptación a la normativa y asesoramiento en protección de datos, (ii) Delegado de Protección de Datos, (iii) Comercio Electrónico. (iv) Auditorías en Protección de Datos, y (v) Evaluaciones de Impacto

1.2. Adaptación a la normativa y asesoramiento en protección de datos (primer y sucesivos años)

Es objeto del presente servicio la contratación de GrupoAdaptalia® en materia de adaptación y seguimiento de protección de datos. En este sentido, se realizarán diferentes hitos en función del servicio:

1) Primer año. Los servicios que GrupoAdaptalia® prestará al Cliente se dividirán en las siguientes fases o hitos:

- i. Recogida de toda la documentación e información necesaria para la prestación del servicio (levantamiento de evidencias o toma de datos).
- ii. Elaboración de la documentación necesaria para cumplir con la normativa de protección de datos. Entre dicha documentación se encontrarán:
 1. Guía de implantación.
 2. Informes de necesidad (EIPD / DPO).
 3. Elaboración del Registro de Actividades del Tratamiento (RAT), indicando en cumplimiento del artículo 30 del RGPD:
 - a. Identificación de las actividades del tratamiento.
 - b. Relación de las medidas técnico – organizativas de seguridad adoptadas por la organización.
 4. Análisis de Riesgos
 5. Entrega de textos y clausulados legales:

- a. Comunicaciones internas: documentación para empleados y protocolos de actuación.
 - b. Comunicaciones externas: documentación para clientes y proveedores.
 - 6. Documentación página web (LSSICE)
 - a. Aviso legal
 - b. Política de cookies
 - c. Política de privacidad.
 - 7. Declaración de adecuación, una vez completada la misma.
 - 8. Seguimiento, control y soporte de la implantación mediante correo electrónico y teléfono.
 - 9. Análisis de violaciones de seguridad: necesidad de comunicar a la AEPD y/o a los afectados.
- 2) **Segundo año:** Los servicios que GrupoAdaptalia® prestará al Cliente se dividirán en las siguientes fases o hitos:
- a) Seguimiento, control y soporte vía telefónica o correo electrónico.
 - b) Actualización de toda la documentación generada en el año anterior.
 - c) Declaración de adecuación, una vez completada la misma.
 - d) Análisis de violaciones de seguridad: necesidad de comunicar a la AEPD y/o a los afectados.

1.3. Delegado de Protección de Datos (primer año y sucesivos)

Es objeto del presente servicio la contratación y designación de GrupoAdaptalia® como Delegado de Protección de Datos (en adelante, "DPO") y el desarrollo de las funciones y obligaciones competentes de ambas Partes (esto es, GrupoAdaptalia® y el Cliente) en el marco de la prestación del servicio, de conformidad con los artículos 37, 38 y 39 del RGPD y artículos 34,35,36 y 37 de la LOPDGDD.

En este sentido, **corresponde a GrupoAdaptalia®**:

1. **Comunicar sus datos de contacto como DPO a la Agencia Española de Protección de Datos (en adelante, "AEPD") en nombre y representación del Cliente llevar a cabo cualquier otra actuación, trámite o gestión que sea necesaria ante la autoridad de control en el marco de la prestación del servicio, de conformidad con el ANEXO AUTORIZACIÓN DE REPRESENTACIÓN, que debe rellenar y firmar el Cliente, junto con la suscripción de la Hoja de Encargo o Propuesta Comercial y (ii) Condiciones Generales Simplificadas.**
2. Informar y asesorar al Cliente y, en especial, a las personas designadas responsables en materia de protección de datos, a las personas de contacto y a las personas empleadas que se ocupen del tratamiento, sobre las obligaciones del RGPD, la LOPDGDD y demás legislación española aplicable en materia de protección de datos al sector de la de actividad del Cliente.
3. Supervisar de forma continua el cumplimiento de lo dispuesto en la normativa sobre protección de datos, debiendo con carácter enunciativo y no limitativo:

- **Recabar información para la elaboración del Registro de Actividades de Tratamiento;** analizar y comprobar que las actividades de tratamiento son conformes a la normativa; y recomendar, a la luz de las actividades descritas, las medidas técnicas organizativas apropiadas para cada una de ellas a fin de garantizar y poder demostrar el cumplimiento de la normativa sobre protección de datos.
 - **Recabar información para la elaboración del Análisis de Riesgos;** detectar el conjunto de amenazas en materia de protección de datos en función de los tratamientos identificados en el Registro de Actividades de Tratamiento y, proponer y cotejar las medidas de mitigación para reducir el riesgo inherente, como mínimo, a un riesgo residual con nivel Tolerable.
 - **Supervisar las políticas de protección de datos del Cliente, tanto a nivel organizativo como a nivel externo con clientes y proveedores,** lo que incluye:
 - i. La revisión de protocolos internos para garantizar la confidencialidad y seguridad de los datos personales.
 - ii. Las cláusulas legales donde se informe a los clientes y potenciales sobre el tratamiento de sus datos.
 - iii. Los contratos de encargado del tratamiento con los prestadores de servicios que puedan acceder y/o tratar los datos de carácter personal por cuenta del Cliente.
 - **Supervisar la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento,** debiendo velar porque las personas responsables en materia de protección de datos dentro de la organización y las personas empleadas que acceden y/o tratan datos, tengan unos conocimientos suficientes sobre la normativa de protección de datos en función del puesto y las funciones desempeñadas.
 - **Supervisar las auditorías realizadas en materia de protección de datos.**
4. **Ofrecer el asesoramiento que solicite el Cliente acerca de la evaluación de impacto relativa a la protección de datos (en adelante, «EIPD»)** y supervisar su aplicación informándole, entre otras, sobre las siguientes cuestiones:
- Si debe llevarse a cabo o no una EIPD.
 - Qué metodología debe seguirse al llevar una EIPD.
 - Qué salvaguardias (incluidas medidas técnicas y organizativas) deben aplicarse para mitigar cualquier riesgo para los derechos e intereses de los particulares.
 - Si la EIPD se ha llevado a cabo correctamente o no y si sus conclusiones son conforme al RGPD.
5. **Cooperar con la autoridad de control y actuar como punto de contacto ante cualquier cuestión relativa al tratamiento de los datos personales y, en especial, cuando:**
- La autoridad de control ejerza sus poderes de investigación, correctivos, de autorización y consultivos.
 - Se haya llevado a cabo una EIPD, y se concluya que el Cliente no puede adoptar medidas técnicas y organizativas para reducir el riesgo hasta un nivel considerado aceptable.
 - El Cliente desee consultar a la autoridad de control sobre cualquier asunto.

6. **Actuar como intermediario entre los interesados y el Cliente, sobre todo, en los casos de reclamación.** En este sentido, los interesados podrán ponerse en contacto con GrupoAdaptalia® para plantearle cualquier cuestión relativa al tratamiento de sus datos personales, dirigirle las solicitudes de ejercicio de derechos o acudir a él con carácter previo a la presentación de una reclamación ante la autoridad de control. Respecto a este último caso, si el interesado decidiese acudir a GrupoAdaptalia® como DPO antes de presentar una reclamación ante la AEPD o las autoridades autonómicas de protección de datos, deberá comunicar al afectado la decisión que se hubiera adoptado en el plazo máximo de dos (2) meses a contar desde la recepción de la reclamación. Si, por el contrario, el interesado presentara directamente la reclamación ante la AEPD o las autoridades de control autonómicas, éstas podrán remitir la reclamación a GrupoAdaptalia® a fin de que responda en el plazo de un (1) mes.
7. **Desempeñar sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y los fines del tratamiento (enfoque basado en el riesgo). Ello no implica que GrupoAdaptalia® deba desatender la supervisión de la observancia de las normas en las operaciones de tratamiento que tengan comparativamente menor riesgo, sino que debe centrarse principalmente en los ámbitos de mayor riesgo.**

Así, a título de ejemplo, este enfoque selectivo y pragmático permitirá asesorar al Cliente sobre:

- o Qué metodología usar si se realiza una EIPD.
 - o Cuándo y cómo debe realizarse una auditoría de protección de datos.
 - o Qué actividades de formación internas proporcionar al personal o a los directivos encargados de las actividades de protección de datos.
 - o A qué operación de tratamiento dedicar más tiempo y recursos.
8. **Guiar al Cliente sobre cómo actuar ante una violación de seguridad**, y asesorarle sobre si debe notificarse a la AEPD en el plazo de setenta y dos (72) horas (en cuyo caso lo haría GrupoAdaptalia® en su representación) y, si además, debe comunicarse a los afectados.
 9. **Programar reuniones presenciales, videoconferencias o llamadas telefónicas con el Cliente, según sus necesidades**, a efectos de que GrupoAdaptalia® pueda, verificar la realidad de los tratamientos, y ejercer sus labores de asesoramiento y supervisión. En este sentido, los segundos y sucesivos de contratación. GrupoAdaptalia® emitirá un informe de seguimiento como DPO.

Por otro lado, y con el fin de garantizar el desarrollo adecuado de las funciones de GrupoAdaptalia® como DPO, el Cliente se compromete a:

1. **Publicar los datos de contacto del DPO y comunicarlo internamente.** Tras la designación de GrupoAdaptalia® como DPO, es menester del Cliente:
 - Publicar sus datos de contacto en las políticas de privacidad expuestas a los interesados.
 - Comunicar su designación a las personas empleadas.Los datos de contacto incluirán información que permita a las personas interesadas y personas empleadas comunicarse con el DPO de forma fácil, por ejemplo, mediante una dirección postal, un número de teléfono específico o una dirección de correo específica.
2. **Permitir su participación en todas las cuestiones relativas a la protección de datos personales**, de forma que el DPO sea considerado como un interlocutor dentro de la organización y forma parte de los correspondientes grupos de trabajo que se ocupen de las actividades del tratamiento.

En consecuencia, la organización deberá garantizar que:

- Se invita al DPO a participar con regularidad en las reuniones con los cuadros directivos altos y medios.
 - Está presente cuando se toman decisiones con implicaciones para la protección de datos.
 - Se tiene debidamente en cuenta la opinión del DPO de forma que, en caso de desacuerdo, el Cliente debe documentar los motivos por los que no se sigue el consejo del DPO.
 - Se consulta con prontitud una vez que se haya producido una violación de seguridad de los datos o cualquier otro incidente (no más de veinticuatro (24) horas desde su conocimiento).
3. **Garantizar su independencia.** El Cliente debe ser capaz de velar en todo momento por que el DPO desempeña sus funciones y cometidos de forma autónoma e independiente. Por tanto, GrupoAdaptalia® no podrá recibir ninguna instrucción relativa al ejercicio de sus tareas a fin de garantizar el debido cumplimiento de la normativa por la organización. Así, no podrá recibir instrucciones sobre el modo de ocuparse de un asunto como: el resultado que debe alcanzarse, la forma de resolver una queja o sobre si debe consultarse a la autoridad competente.
4. **No destituirlo ni sancionarlo.** EL Cliente tampoco podrá destituirlo o sancionarlo si está en desacuerdo con la valoración o los consejos del DPO en tanto ello supondría quebrantar su autonomía, independencia e imparcialidad en el desarrollo de sus funciones.
5. **Proporcionarle recursos necesarios.** El Cliente debe respaldar al DPO proporcionándole los recursos necesarios para que lleve a cabo sus tareas y acceda a los datos personales y operaciones de tratamiento.

Siendo esto así, el Cliente deberá garantizar especialmente los siguientes aspectos:

- Facilitar a GrupoAdaptalia® el acceso a los servicios y departamentos de toda la empresa (departamento de recursos humanos, departamento TIC, etc) a efectos de tener un mayor conocimiento sobre el tratamiento de los datos que realiza cada departamento y poder, de este modo, desempeñar sus funciones de forma más eficaz. Igualmente, la alta dirección debe estar fácilmente accesible y mostrar su apoyo activo a la labor del DPO de forma que GRUPO ADAPTALIA pueda recabar información relevante para la resolución de cualquier cuestión en materia de protección de datos.
 - Conceder tiempo suficiente a GrupoAdaptalia® para desempeñar sus funciones y resolver las consultas planteadas. GrupoAdaptalia® se compromete a contestar en un plazo máximo de veinticuatro (24) horas. Ahora bien, el desarrollo de sus funciones y el tiempo de resolución efectivo de las consultas planteadas, dependerá de cuán compleja sea la cuestión, de la información facilitada por el Cliente y de la necesidad de acudir a otras fuentes de información que pueden no estar fácilmente accesibles o disponibles.
6. **Reportar cualquier iniciativa de cambio o modificación en el tratamiento de los datos, así como cualquier tipo de cuestión o duda que le haya surgido al Cliente.** Esta información podrá facilitarse:
- Mediante consultas vía mail o llamada telefónica.
 - A través de las reuniones presenciales o videoconferencias, que tendrán lugar entre el equipo de trabajo de GrupoAdaptalia® y las personas de la organización implicadas en el tratamiento.
7. **No conflicto de intereses:** de conformidad con la normativa sobre protección de datos, nada obsta a que el Cliente pueda nombrar como DPO a una persona jurídica, siempre y cuando no exista un conflicto de intereses entre las personas del equipo de trabajo.

A tales efectos:

- Aunque la constitución del DPO en equipo de trabajo, permite combinar las destrezas y puntos fuertes individuales de varios profesionales especializados en materia de protección de datos GrupoAdaptalia®, con la finalidad de entablar comunicaciones entre el Cliente y GrupoAdaptalia® como DPO, designará a una persona física de contacto.
- GrupoAdaptalia® cuenta con una política interna que evita que el equipo de trabajo que desempeña las funciones de DPO para el Cliente, sea el mismo que realice las auditorías y/o evaluaciones de impacto, a fin de evitar poner en riesgo las labores de supervisión e imparcialidad.

Los profesionales o personas empleadas asignadas al Cliente en el servicio que se trate podrán ser modificados o sustituidos por GrupoAdaptalia® cuando así lo considere oportuno o sea necesario en atención a las necesidades del cliente o del asunto a tratar.

1.4. Comercio Electrónico

Es objeto del presente servicio la adecuación de la página web indicada por el CLIENTE que disponga de comercio electrónico, de conformidad con el RGPD, la LOPDGDD, la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (en adelante, "LSSICE") así como Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias (en adelante, "Ley General de Consumidores y Usuarios").

Por ello, GrupoAdaptalia®, realizará las siguientes actuaciones:

1. **Levantamiento de evidencias**, para conocer la metodología de recogida de datos de carácter personal, los productos / servicios ofertados, así como el funcionamiento íntegro de la página web. Esta actuación podrá desarrollarse a través de una reunión telemática / presencial como a través del envío de un cuestionario para su cumplimentación.
2. **Elaboración de la documentación precisa**, para cumplir con las normativas indicadas anteriormente. En este sentido se entregará:
 - Términos y condiciones del uso del sitio web.
 - Condiciones generales de venta.
 - Política de privacidad (primera y segunda capa).
 - Política de cookies (primera y segunda capa).

1.5. Auditorías en Protección de Datos

Es objeto del presente servicio la realización de una **auditoría en materia de protección de datos**. En este sentido, el alcance de los servicios prestados conlleva:

- a) Valoración del nivel de cumplimiento normativo en materia de protección de datos, sin estar supeditado a un tipo de actividad de tratamiento, categoría de interesados o categoría de datos determinadas.
- b) Valoración del nivel de cumplimiento normativo en materia de sociedad de la información, estando supeditado a la valoración de la correcta gestión de las cookies en la web, así como a las condiciones de uso que regula las mismas.

- c) Revisión de la captación de clientes potenciales, leads y/o clientes, en cumplimiento de la normativa de protección de datos (RGPD y LOPDGDD) así como de la Ley 11/2022, de 28 de junio, General de Telecomunicaciones.

Con la realización de la auditoría se pretende evidenciar que el Cliente cumple con un nivel adecuado que garantice el correcto cumplimiento de la normativa de protección de datos, teniendo en cuenta el principio de accountability o responsabilidad proactiva, a través de un sistema de cumplimiento que lo avale. Para ello se analizará:

1. **Tratamiento de datos:** se analizará si el Cliente cumple con el debido análisis sobre el conjunto de tratamiento que lleva a cabo, garantizando la existencia de los siguientes documentos, información o procesos:
 - Registro de actividades del tratamiento que recoja todos los tratamientos que lleva a cabo el Cliente, así como su debida actualización.
 - Procedimiento que permita garantizar la privacidad sobre los tratamientos que se están llevando a cabo, como los nuevos tratamientos que se puedan producir en un futuro.
 - La existencia de procesos que evalúen la idoneidad del tratamiento de datos y los riesgos inherentes al mismo.
 - Análisis que garanticen la licitud de los tratamientos (artículo 6 del RGPD).
 - Debida identificación de aquellos tratamientos que operen con categorías especiales de datos (artículo 9 del RGPD).
 - Debida identificación de aquellos tratamientos que afecten a colectivos vulnerables, como son, a título enunciativo y no limitativo, menores o personas con discapacidad.
 - Debida identificación de los criterios aplicados y la irreversibilidad de los tratamientos que no requieren identificación por recabarse anónimamente o por emplear técnicas de anonimizado (artículo 11 del RGPD).
 - Decisiones individuales automatizadas, incluida la posible elaboración de perfiles (artículo 22 del RGPD).
 - Proceso de formación y concienciación de los empleados en materia de protección de datos.
2. **Principios relativo al tratamiento:** análisis de cumplimiento de los principios relativos al tratamiento (artículo 5 del RGPD).
3. **Ejercicios de derechos:** análisis con el fin de garantizar la existencia de procedimientos definidos que determinen la forma en la que se procede ante el ejercicio de derechos por parte de las personas interesadas (artículos 12 y del 15 al 22 del RGPD).
4. **Medidas de seguridad y brechas de seguridad:** revisión sobre si las medidas de seguridad técnicas y organizativas son acordes a la apreciación del riesgo, garantizando la seguridad de los datos personales y sus tratamientos.
5. **Relaciones con terceros:** estudio exhaustivo sobre la regulación que el Cliente mantiene con terceros. Para ello, se deberá garantizar:
 - Existencia de relaciones de corresponsabilidad del tratamiento (artículo 26 del RGPD).
 - Existencia de un proceso de verificación de la idoneidad de los encargados del tratamiento (artículo 28 del RGPD).

- La existencia de una correcta regulación, a título contractual de las relaciones que mantiene con los encargados del tratamiento (artículo 28 del RGPD).
 - La existencia de una correcta gestión de responsabilidades en la comunicación de datos de carácter personal, así como el proceso que se sigue en dicha comunicación.
 - Control y regulación de las transferencias internacionales de datos (artículo 49 del RGPD).
 - Existencia de un procedimiento de archivo de la documentación que avale estas decisiones.
6. **Análisis de riesgos y evaluaciones de impacto:** análisis de las evaluaciones del riesgo en función de los tratamientos llevados a cabo, con el enfoque de su impacto a los derechos y libertades de las personas físicas (artículo 35 del RGPD).
7. **Correcta gestión de las condiciones de la página web:** se llevará a cabo un control sobre la correcta gestión de la/s distinta/s página/s web/s que pudiera tener el Cliente así como las condiciones que regulan las mismas (gestión de cookies, revisión aviso legal y condiciones de uso de la página web y política de privacidad).

Por todo lo anterior, GrupoAdaptalia® se compromete a la realización de las siguientes fases:

- a) **Levantamiento de evidencias:** se realizará una/s reunión/es, bien presenciales bien de forma telemática con los interlocutores asignados con el fin de conocer la organización, así como los tratamientos que lleva a cabo el Cliente.
- b) **Elaboración del informe de auditoría:** En este documento se incluirán la totalidad de los puntos indicados anteriormente. El informe establecerá la conformidad, disconformidad u observaciones de cada uno de los controles indicados anteriormente, estableciendo medidas recomendadas o correctoras.

Asimismo, se entregará sellado en el tiempo con el fin de dotarle de máxima transparencia y rigor.

1.6. Evaluaciones de Impacto

Es objeto del presente contrato la **realización de una Evaluación de Impacto relativa a la Protección de Datos** (en adelante, "Evaluación de Impacto" o "EIPD") sobre el tratamiento indicado y establecido en el Contrato de Prestación de servicios.

De conformidad con el artículo 35.7) del RGPD, la estructura de las diferentes etapas a seguir en la ejecución de la EIPD, serán las siguientes:

- Descripción sistemática de la actividad de tratamiento.
- Evaluación de la necesidad y proporcionalidad del tratamiento respecto a su finalidad.
- Evaluación de los riesgos.
- Análisis de las medidas previstas para afrontar los riesgos, incluidas las garantías, medidas de seguridad y mecanismos que garanticen la protección de datos de datos personales.

Teniendo en cuenta el contenido mínimo exigido en la normativa de protección de datos, GrupoAdaptalia®, llevará a cabo la EIPD sobre el tratamiento objeto del contrato, siguiendo la siguiente metodología, etapas y/o fases de ejecución:

1. Contexto:

- o **Descripción del ciclo de vida de los datos.** Se llevará a cabo una descripción detallada del ciclo de vida y del flujo de datos con ayuda de material gráfico, identificando:
 - La tipología y clasificación de los datos objeto del tratamiento
 - Las vías de entrada o formas de captura de los datos
 - La base de legitimación para el tratamiento de los datos

- Los intervinientes en el tratamiento, con especial incidencia en los departamentos que participan activamente del procesado de los datos, encargados de tratamiento, etc.
 - Las tecnologías, sistemas, aplicaciones, dispositivos y técnicas empleadas para el procesamiento de los datos
 - Posibles terceros a los que se puedan comunicar o ceder los datos que no participen en el procesado de los datos
 - Plazos, criterios y formas de destrucción de los datos
- o **Análisis de la necesidad y proporcionalidad del tratamiento.** En esta segunda fase, se analizará el ciclo de vida de los datos desde la perspectiva del principio de minimización de los datos y el juicio de proporcionalidad.

Ello supone considerar si el tratamiento, tal y como está definido, es *necesario* y *proporcional* a la finalidad prevista. Es decir, evaluar si la finalidad es adecuada y pertinente y si se puede conseguir por otros medios; por ejemplo, con carácter enunciativo y no limitativo: utilizando otros datos, reduciendo el número de personas afectadas (de manera cuantitativa y cualitativa), haciendo uso de otras tecnologías menos invasivas o bien aplicando otros procedimientos o medios de tratamiento.

2. Gestión de riesgos

- o **Identificación del origen de los riesgos.** Se identificarán los potenciales escenarios de riesgo que pueden afectar negativamente a los derechos y libertades de las personas derivados de un inadecuado tratamiento de sus datos.

Las amenazas o potenciales escenarios de riesgos se categorizarán en 3 tipos, en base a la tipología del daño que pueden producir en los datos:

- *Acceso ilegítimo a los datos (hacking, malware, robo, fuga de información, acceso intencionado por parte de personal no autorizado, ausencia de base de legitimación para el tratamiento, etc)* □ Confidencialidad
 - *Modificación no autorizada (errores en los procesos de recopilación y captura de la información, ataque para la suplantación de identidad, etc)* □ Integridad.
 - *Eliminación de los datos (causas naturales como fuego, agua o cualquier otro desastre ambiental; corte en el suministro electrónico o fallos en servicios de comunicaciones; error humano o ataque intencionado que provoque borrado o pérdida de los datos, etc)* □ Disponibilidad.
- o **Evaluación de los riesgos.** Consiste en valorar y estimar la probabilidad y el impacto de que el riesgo se materialice. Es decir, supone calcular la probabilidad de que las anteriores amenazas se produzcan por el daño que puede ocasionar en los derechos y libertades de los interesados si esta amenaza efectivamente se materializa.

A título enunciativo y no limitativo, los posibles daños que pueden ocasionar en el interesado son:

- *Daño físico.* Conjunto de acciones que pueden provocar un daño en la integridad física del interesado.
- *Daño material.* Conjunto de acciones que pueden provocar pérdidas económicas, de patrimonio, de empleo, etc.
- *Daño moral.* Conjunto de acciones que pueden provocar un daño moral o mental en el interesado, como una depresión, fobias, acoso, etc.

Para calcular el riesgo (probabilidad x impacto) se empleará la metodología de valoración basada en los cuatro niveles de la ISO/IEC 29134: 2017. Siguiendo esta metodología, se

asignarán los valores "1. Despreciable", "2. Limitado", "3. Significativo" y "4. Máximo" tanto a la probabilidad como al impacto de forma que se enfrenten y concluyan que el riesgo es "Bajo", "Medio", "Alto" o "Muy alto".

No existen parámetros tasados en la normativa que permitan asignar de forma eminentemente objetiva los anteriores valores, por lo que tal asignación se realizará en función del contexto de los tratamientos y de la experiencia profesional y conocimientos de

- o **Gestión de los riesgos.** Esta última consiste en articular las medidas técnicas, organizativas y legales necesarias para tratar el riesgo y conducirlo hasta un nivel considerado aceptable para garantizar los derechos y libertades de los interesados.

Para ello, se establecerán medidas de control que reduzcan los niveles de probabilidad y/o impacto y, por tanto, el resultado "Medio", "Alto" o "Muy Alto" del riesgo. En caso de que el resultado del riesgo sea "Bajo", esto es, que el nivel de riesgo inherente sea inferior al considerado aceptable, no existirá la necesidad de implementar controles o medidas adicionales.

3. **Conclusión y plan de acción:** El resultado de la EIPD se materializará en un informe que documentará:
 - o Las fases anteriores
 - o El resultado final obtenido del análisis de las fases anteriores
 - o El plan de acción que incluya las medidas de control a implantar para gestionar los riesgos identificados y poder garantizar los derechos y libertades de las personas físicas
 - o Si procede, el resultado de la consulta previa a la autoridad de control (en el caso español, la AEPD) prevista en el art.36 del RGPD. Esta consulta se realizará si aun implementando las medidas de control que se establezcan en la subfase anterior, el riesgo residual sigue siendo alto o muy alto, o no se considera aceptable dentro de unos límites razonables. En tal caso, debe suspenderse el tratamiento hasta que la AEPD se pronuncie, quien podrá establecer condiciones y medidas para autorizar el tratamiento o indicar que en ningún caso podrá llevarse a cabo el tratamiento.
4. **Supervisión y revisión.** Es fundamental una adecuada supervisión y posterior revisión de la implantación de las medidas definidas en la EIPD para verificar en la práctica que efectivamente el nivel de riesgo residual se encuentra por debajo del nivel de riesgo aceptable.

A tal efecto, es recomendable que si el Cliente ha designado a un Delegado de Protección de Datos, éste se encargue de supervisar y garantizar la implantación de las medidas técnicas y organizativas resultantes de la EIPD, según las funciones que le asisten en virtud del art.37 del Reglamento General de Protección de Datos.

Finalmente, siempre y cuando exista una variación relevante en el contexto de las actividades de tratamiento que pueda suponer un incremento de riesgo asociado al mismo, deberá realizarse una actualización de la EIPD.

Control de versiones

Versión	Fecha	Descripción
1.0 (versión actual)	05/03/2026	Elaboración de las Condiciones Específicas – Servicios Protección de Datos

Anexo – Contrato de Encargado de Tratamiento (Servicios Protección de Datos)

De una parte, **EL CLIENTE** (en adelante, «**RESPONSABLE DEL TRATAMIENTO**» o «**RESPONSABLE**»).

De otra parte, **GRUPO ADAPTALIA LEGAL-FORMATIVO, S.L.** con domicilio en C/ Julián Camarillo nº 26, 4ª izquierda, 28037, Madrid, España y NIF B86260247 (en adelante, «**ENCARGADO DEL TRATAMIENTO**» o «**ENCARGADO**»).

MANIFIESTAN

1. Que ambas PARTES se encuentran vinculadas por una relación contractual de carácter mercantil para la **prestación de los servicios de consultoría y asesoramiento legal en materia de protección de datos** (en adelante, el «**SERVICIO**»), en virtud del contrato de prestación de servicios firmado entre las partes.
2. Que, en cumplimiento del artículo 28 del Reglamento (UE) 2016/679 General de Protección de Datos (en adelante, «RGPD») y artículo 33 de la Ley 3/2018, de 5 de diciembre, de Protección de Datos personales y garantía de los derechos digitales (en adelante, «LOPDGDD»), las PARTES de forma libre y espontánea voluntad acuerdan regular el tratamiento de los datos de carácter personal de conformidad con las siguientes:

CLÁUSULAS

1. Objeto del Encargo del Tratamiento

Mediante las presentes cláusulas se habilita al ENCARGADO DE TRATAMIENTO, por cuenta del RESPONSABLE DEL TRATAMIENTO, el tratamiento de los datos de carácter personal necesarios para prestar el SERVICIO.

EL ENCARGADO únicamente realizará los tratamientos estrictamente necesarios para la prestación del referido servicio, no pudiendo llevar a cabo acciones no permitidas por el RESPONSABLE.

2. Identificación de las categorías de interesados, datos personales y naturaleza

Para la ejecución de las prestaciones derivadas del cumplimiento del referido contrato de prestación de servicios, el RESPONSABLE DEL TRATAMIENTO puede llegar a poner a disposición del ENCARGADO DEL TRATAMIENTO y/o permitirle el acceso a la información que se describe a continuación:

2.1. Categoría de interesados y datos personales objeto de tratamiento:

Clientes	▪ Datos identificativos ▪ Datos profesionales ▪ Información presente en posibles solicitudes de ejercicio de derechos y/o reclamaciones en materia de protección de datos.
-----------------	--

Proveedores	▪ Datos identificativos ▪ Datos profesionales ▪ Información presente en posibles solicitudes de ejercicio de derechos y/o reclamaciones en materia de protección de datos.
Personas empleadas	▪ Datos identificativos. ▪ Datos profesionales. ▪ Información presente en posibles solicitudes de ejercicio de derechos y/o reclamaciones en materia de protección de datos.
Terceros/otros usuarios	▪ Datos identificativos. ▪ Datos profesionales. ▪ Información presente en posibles solicitudes de ejercicio de derechos y/o reclamaciones en materia de protección de datos.

2.2. Naturaleza del tratamiento:

Recogida	Recopilación de datos que contienen información de índole personal.
Estructuración	Organización de datos y darle una estructura que facilite su acceso y manejo
Consulta	Visualización de los datos en el sistema o dispositivo donde están almacenados.
Registro	Almacenamiento de información en un sistema o dispositivo, automatizado o manual, para su procesamiento posterior.
Comunicación por transmisión	Transmitir los datos a otro receptor desde su sistema o dispositivo de origen mediante medios electrónicos (en caso de posibles gestiones y/o trámites ante la Agencia Española de Protección de Datos)
Conservación	Almacenamiento de información por un periodo temporal específico.

3. Duración

La duración del presente contrato quedará supeditada a la continuidad del servicio principal contratado, siendo renovado automáticamente salvo decisión en contra por alguna de las PARTES.

4. Obligaciones del Encargado de Tratamiento

EL ENCARGADO DEL TRATAMIENTO y todo su personal se obliga a:

1. Utilizar los datos personales objeto de tratamiento, o los que recoja para su tratamiento, sólo para la finalidad objeto de este encargo. En ningún caso podrá utilizar los datos para fines propios o diferentes a los establecidos por el RESPONSABLE.
2. Tratar los datos de acuerdo con las instrucciones documentadas del RESPONSABLE que, en todo caso, implicará la prohibición de efectuar como consecuencia de la prestación del servicio transferencias internacionales que requieran de solicitud de autorización a la autoridad de control por tratarse de países y/u organizaciones que no cumplan con un nivel adecuado de protección o no se cuente con las garantías necesarias para llevar a cabo la exportación de los datos personales.

Si el ENCARGADO considera que alguna de las instrucciones infringe el RGPD o cualquier otra disposición en materia de protección de datos de la Unión o de los Estados miembros, informará inmediatamente al RESPONSABLE.

3. Garantizar que las personas autorizadas para tratar datos personales se comprometan, de forma expresa y por escrito, a respetar la confidencialidad, el secreto profesional y a cumplir las medidas de seguridad correspondientes, de las que hay que sensibilizar, formar e informar convenientemente. El deber de secreto y confidencialidad respecto a los datos de carácter personal a los que haya tenido acceso en virtud del presente encargo perdurará indefinidamente.
4. No subcontratar ninguna de las prestaciones que formen parte del objeto de este contrato que comporten el tratamiento de datos personales, salvo los servicios auxiliares necesarios para el normal funcionamiento de los servicios del ENCARGADO (a título enunciativo y no limitativo, mantenimiento informático). Si fuera necesario subcontratar algún tratamiento, este subcontratista o SUBENCARGADO, que también tiene la condición de encargado de tratamiento, está obligado igualmente a cumplir las obligaciones establecidas en este documento para el ENCARGADO y las instrucciones que dicte el RESPONSABLE. Corresponde al ENCARGADO inicial regular la nueva relación de forma que el SUBENCARGADO quede sujeto a las mismas condiciones (instrucciones, obligaciones, medidas de seguridad...) y con los mismos requisitos formales que él, en lo referente al adecuado tratamiento de los datos personales y a la garantía de los derechos de las personas afectadas. En el caso de incumplimiento por parte de Subencargado, el Encargado inicial seguirá siendo plenamente responsable ante el responsable en lo referente al cumplimiento de las obligaciones.
5. Llevar, por escrito, un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta del RESPONSABLE, que contenga al menos:
 - El nombre y los datos de contacto del RESPONSABLE por cuenta del cual actúa como ENCARGADO y, en su caso, del representante del RESPONSABLE o del ENCARGADO y del delegado de protección de datos, si lo tuviera.
 - Las categorías de tratamientos efectuados por cuenta del RESPONSABLE.
 - En su caso, las transferencias de datos personales a un tercer país u organización internacional, incluida la identificación de dicho tercer país u organización internacional y, cuando sean necesarias, la documentación de garantías adecuadas adoptadas.
 - Cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad que incluyan, con carácter enunciativo y no limitativo:
 - i. La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.
 - ii. La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.
 - iii. El proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

- iv. La pseudonimización y el cifrado de datos personales, en su caso.

Este Registro deberá estar a disposición y se facilitará al Responsable y a la autoridad de control, si así lo solicitara, no sin antes consensuarlo con el Responsable.

6. No comunicar los datos a terceras personas, salvo que cuente con la autorización expresa del RESPONSABLE del tratamiento, o en los supuestos legalmente admisibles.

El ENCARGADO comunicará los datos a otros ENCARGADOS del tratamiento del mismo RESPONSABLE, de acuerdo con las instrucciones del RESPONSABLE. En este caso, el RESPONSABLE identificará, de forma previa y por escrito, la entidad a la que se deben comunicar los datos, los datos comprometidos y las medidas de seguridad a aplicar para proceder a la comunicación.

El ENCARGADO mantendrá a disposición del RESPONSABLE la documentación acreditativa del cumplimiento de las obligaciones de comunicación a terceros y/o transferencias.

7. Asistir al RESPONSABLE del tratamiento, teniendo en cuenta la naturaleza del mismo y a través de medidas técnicas y organizativas apropiadas, siempre que sea posible, para que éste pueda dar cumplimiento en la respuesta al ejercicio de los derechos de acceso, rectificación, supresión y oposición, limitación del tratamiento, portabilidad de datos personales y a no ser objeto de decisiones individualizadas automatizadas (incluida la elaboración de perfiles).

Cuando los interesados ejerzan los derechos de acceso, rectificación, supresión y oposición, limitación del tratamiento, portabilidad de datos y a no ser objeto de decisiones individualizadas automatizadas ante el ENCARGADO del tratamiento, éste debe comunicarlo al correo electrónico facilitado por el RESPONSABLE. La comunicación debe hacerse de forma inmediata y en ningún caso más allá del quinto (5) día laborable siguiente al de la recepción de la solicitud, juntamente, en su caso, con otras informaciones que puedan ser relevantes para resolver la solicitud.

El ENCARGADO del tratamiento notificará al RESPONSABLE del tratamiento, sin dilación indebida, y en cualquier caso antes del plazo máximo de setenta y dos (72) horas, desde que se tenga constancia, y a través del correo electrónico facilitado por el RESPONSABLE, las violaciones de la seguridad de los datos personales a su cargo de las que tenga conocimiento, juntamente con toda la información relevante para la documentación y comunicación de la incidencia. No será necesaria la notificación al RESPONSABLE, cuando sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas.

8. Dar apoyo al RESPONSABLE de la realización de las evaluaciones de impacto relativas a la protección de datos y de las consultas previas a la autoridad de control, en su caso y cuando proceda, conforme a la normativa de protección de datos que resulte de aplicación y/o a las instrucciones que emita la autoridad de control nacional.
9. Poner a disposición del RESPONSABLE toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en la normativa de protección de datos, así como permitir la realización de auditorías, incluidas inspecciones, que pudiera realizar el RESPONSABLE u otro auditor designado por éste. Para este tipo de acciones, se establece un aviso previo por escrito de un (1) mes.
10. Implantar las medidas de seguridad técnicas y organizativas necesarias para garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento. A efectos de determinar las medidas de seguridad objeto de implantación, habrá que atender al análisis de riesgos, y evaluación de impacto, si procediera, en la que se determinará las medidas más adecuadas para garantizar la seguridad del tratamiento, las cuales deberán ser adoptadas, documentando todo lo actuado. En cualquier caso, podrán acordarse aquellas que se establezcan en códigos de conducta, sellos, certificaciones o cualquier norma o estándar internacional actualizado de cumplimiento de protección de datos y seguridad de la información. Al respecto, el ENCARGADO tiene implementadas las medidas técnicas y organizativas que se describen en el **Apéndice 1. Medidas organizativas y técnicas.**

11. Designar un delegado de protección de datos y comunicar su identidad y datos de contacto al RESPONSABLE, si es que procede y en su caso.

5. Obligaciones del Responsable del Tratamiento

Por su parte, las obligaciones del RESPONSABLE son las siguientes

- a) Entregar al ENCARGADO los datos a los que se refiere la cláusula 2 de este contrato.
- b) Dar las instrucciones que correspondan para llevar a cabo el tratamiento.
- c) Realizar análisis de riesgos y una evaluación del impacto en la protección de datos personales de las operaciones de tratamiento a realizar por el ENCARGADO, cuando proceda.
- d) Realizar las consultas previas que correspondan.
- e) Velar, de forma previa y durante todo el tratamiento, por el cumplimiento del RGPD por parte del ENCARGADO.
- f) Supervisar el tratamiento, incluida la realización de inspecciones y auditorías.

6. Destino de los datos

Una vez finalizada la prestación del servicio, el ENCARGADO deberá devolver al RESPONSABLE del tratamiento los datos de carácter personal y, si procede, los soportes donde consten, una vez cumplida la prestación; o destruirlo, o entregar a un nuevo ENCARGADO que designe por escrito el RESPONSABLE

La devolución debe comportar el borrado total de los datos existentes en los equipos informáticos utilizados por el ENCARGADO, también en las copias de seguridad. No obstante, el ENCARGADO puede conservar una copia, con los datos debidamente bloqueados, mientras puedan derivarse responsabilidades de la ejecución de la prestación o tenga obligación legal para ello.

No procederá la destrucción de los datos cuando exista una previsión legal que obligue a su conservación, en cuyo caso deberán ser devueltos al RESPONSABLE DEL TRATAMIENTO, que garantizará su conservación mientras tal obligación persista.

En todo caso, se aplicarán plazos de devolución o destrucción de los datos más restrictivos (es decir, antes de la finalización de la relación contractual); si al RESPONSABLE, en virtud del principio de limitación del plazo de conservación, se le aplicaran legalmente y/o hubiera establecido plazos de conservación inferiores a la vigencia del contrato. Al respecto, el RESPONSABLE deberá informar al ENCARGADO de los plazos de conservación aplicables al/ a los tratamiento/s realizados en su nombre y emitir, si es necesario, instrucciones precisas para proceder a la devolución o destrucción efectiva de los datos en el tiempo estipulado.

7. Exoneración de responsabilidad

El ENCARGADO responderá, conforme al artículo 82.2 del RGPD, frente al RESPONSABLE por cualquier daño, perjuicio, sanción o gasto que derive de (i) del incumplimiento por el ENCARGADO de las obligaciones que le sean directamente atribuibles conforme al RGPD o a la normativa nacional que lo desarrolle, o (ii) la realización de operaciones de tratamiento fuera o en contradicción con las instrucciones documentadas del RESPONSABLE.

El ENCARGADO no asumirá responsabilidad alguna por los daños que resulten de (i) instrucciones ilegales o contrarias al RGPD impartidas por el RESPONSABLE, siempre que hubiera advertido previamente de ello por escrito, o (ii) hechos atribuibles exclusivamente a terceros ajenos al ENCARGADO que constituyan fuerza mayor o ataque deliberado ("acto de tercero malintencionado"), siempre que el Encargado pueda demostrar la adopción de las medidas técnicas y organizativas adecuadas conforme al artículo 32 RGPD y al Apéndice 1 del presente contrato.

Cuando, con arreglo al artículo 82 RGPD, el RESPONSABLE sea obligado a indemnizar a un interesado por un daño que corresponda en todo o en parte al ENCARGADO aquel tendrá derecho a repetir contra este último la parte proporcional al grado de culpa del ENCARGADO. Si el ENCARGADO

satisface la indemnización, podrá reclamar al RESPONSABLE la parte que le sea imputable en idénticos términos.

8. Legislación y jurisdicción

El presente contrato contempla las exigencias de la legislación española y europea vigente en materia de protección de datos personales, particularmente por lo establecido en el RGPD y LOPDGDD.

Las PARTES con expresa renuncia de su fuero, someten todas las interpretaciones y/o conflictos que pudieran surgir derivados de este contrato a los Juzgados y Tribunales del Madrid.

Apéndice 1. Medidas organizativas y técnicas

EL ENCARGADO tiene implementadas las siguientes medidas técnicas y organizativas para la debida protección de los datos personales:

MEDIDAS ORGANIZATIVAS:

- I. Se ha desplegado un Sistema de Gestión de Protección de Datos (SGPD) en el que se incorporan políticas y procedimientos, para garantizar el debido cumplimiento de la normativa de protección de datos.
- II. Se ha establecido una estructura organizativa para la gestión y coordinación de la protección de datos y la seguridad de la información, de forma documentada. En dicha estructura se han definido roles y funciones, así como los procedimientos y protocolos para la resolución de incidencias y aplicación de mejoras de forma coherente y ejecutiva.
- III. Se garantiza que el ENCARGADO y sus trabajadores solamente pueden tratar y acceder a los tratamientos de datos de carácter personal a los que esté autorizado por RESPONSABLE DEL TRATAMIENTO y que sean necesarios para el desarrollo de las funciones recogidas en el presente acuerdo y de lo dispuesto en el contrato principal, independientemente del dispositivo de tratamiento. Para ello:
 - i. Se llevan a cabo planes de formación y concienciación de los trabajadores respecto a la aplicación de la normativa de protección de datos y de las medidas de seguridad básicas, así como acciones que permitan el conocimiento de las responsabilidades en la aplicación de los procedimientos en materia de Protección de Datos y Seguridad de la Información;
 - ii. Se garantiza la firma y el compromiso por parte de los trabajadores y el personal respecto a la confidencialidad más estricta de los datos personales y de cualquier otro tipo de información empresarial;
 - iii. Se garantiza el conocimiento de los protocolos en caso de violación de seguridad o ejercicio de derechos;
 - iv. Se establece para los trabajadores y personal políticas de uso de los dispositivos y medios proporcionados por la empresa, para evitar usos no propios de su responsabilidad o función. El uso de dispositivos que contengan datos o información empresarial debe ser estrictamente profesional y no personal;
 - v. Se asegura que los datos, sistemas de información o recursos sean usados únicamente para el desarrollo de los procesos de negocio definidos de conformidad con la prestación del presente servicio;
 - vi. Se garantiza que los trabajadores no incurran en actividades que puedan ser consideradas ilícitas o ilegales o que infrinjan los derechos de las partes, de sus clientes o de terceros;
 - vii. Se garantiza el cumplimiento de la política de accesos a la información, mediante la observancia de la política contraseñas indicada por la empresa, así como la confidencialidad

y salvaguarda de sus propias contraseñas. Los identificadores de usuario son personales e intransferibles y están asignados de forma inequívoca a personas identificables;

- viii. Se han establecido designaciones internas de responsables en materia de protección de datos.

MEDIDAS TÉCNICAS:

EL ENCARGADO está certificado en el Esquema Nacional de Seguridad (nivel medio), respecto a los sistemas de información que dan soporte a la actividad de consultoría de cumplimiento normativo, entre los que se encuentran los servicios de consultoría y asesoramiento legal en materia de protección de datos. Pueden consultarse dicha certificación en la página web del ENCARGADO: www.grupoadaptalia.es.

A título enunciativo y no limitativo, dichas medidas técnicas, incluyen:

- i. Gestión de soportes informáticos
- ii. Control de acceso a equipos y sistemas informáticos
- iii. Identificación y autenticación
- iv. Copias de seguridad
- v. Protección de equipos y transmisión segura de datos
- vi. Protección de redes propias
- vii. Protección en redes ajenas
- viii. Control de acceso físico

Control de versiones

Versión	Fecha	Descripción
1.0 (versión actual)	05/03/2026	Elaboración del Anexo – Encargado de Tratamiento