

CONTRATO COMMUNICADIA COMO ENCARGADO DE TRATAMIENTO

Uno. OBJETO DEL ENCARGO

Mediante las presentes cláusulas se habilita a VANESA GORDO LOMA OSORIO, como Titular de Agencia de comunicación, diseño gráfico y desarrollo web para organizaciones **COMMUNICADIA** con domicilio en Miguel Villanueva 7, 1 izda 26001 Logroño (La Rioja) y con NIF número 16591993T, teléfono número 941 25 95 99 y correo electrónico info@communicadia.com en calidad de **ENCARGADO DEL TRATAMIENTO**, para tratar por cuenta del RESPONSABLE DEL TRATAMIENTO o cliente, los datos de carácter personal necesarios para prestar el servicio de comunicación, diseño gráfico y desarrollo web celebrado con el cliente y de conformidad con el artículo 28 del REGLAMENTO (UE) 2016/679, de 27 de abril de 2016 del Parlamento Europeo y del Consejo relativo a la Protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de los mismos (en adelante RGPD) y normativa de desarrollo.

Dos. IDENTIFICACIÓN DE LA INFORMACIÓN AFECTADA

Para la ejecución de las prestaciones derivadas del cumplimiento del objeto de este encargo, el RESPONSABLE DEL TRATAMIENTO, pone a disposición del ENCARGADO DEL TRATAMIENTO, la información que se describe a continuación:

- Dirección mails de sus clientes y/o usuarios de su web.
- Nombre y apellidos de cliente/contacto de la empresa cliente

De todas/algunas las categorías de datos antes descritas, informar que se realizan operaciones de: Consulta, uso, almacenaje, copia y en su caso borrado o supresión respecto de los datos de carácter personal de contacto relativos a los trabajadores, clientes, potenciales clientes, contactos comerciales proporcionados por el cliente necesarios para llevar a cabo los servicios contratados por el cliente o responsable de tratamiento.

Tres. DURACIÓN

El presente acuerdo estará vigente mientras perdure la vigencia del contrato de servicios.

Una vez finalice el presente contrato, el encargado del tratamiento debe devolver al responsable o transmitir a otro encargado que designe el responsable los datos personales, y o suprimir cualquier copia que esté en su poder. No obstante, podrá mantener bloqueados los datos para atender posibles responsabilidades administrativas o jurisdiccionales.

Cuatro. OBLIGACIONES DEL ENCARGADO DEL TRATAMIENTO

El encargado del tratamiento, y todo su personal se obliga a:

1. Utilizar los datos personales a los que tenga acceso sólo para la finalidad objeto de este encargo. En ningún caso podrá utilizar los datos para fines propios.
2. Tratar los datos de acuerdo con las instrucciones del responsable del tratamiento. Si el encargado del tratamiento considera que alguna de las instrucciones infringe el RGPD o cualquier otra disposición en materia de protección de datos, el encargado informará inmediatamente al responsable.

3. No comunicar los datos a terceras personas, salvo que cuente con la autorización expresa del responsable del tratamiento, en los supuestos legalmente admisibles.
4. Mantener el deber de secreto respecto a los datos de carácter personal a los que haya tenido acceso en virtud del presente encargo, incluso después de que finalice el contrato.
5. Garantizar que las personas autorizadas para tratar datos personales se comprometan, de forma expresa y por escrito, a respetar la confidencialidad y a cumplir las medidas de seguridad correspondientes, de las que hay que informarles convenientemente.
6. Mantener a disposición del responsable la documentación acreditativa del cumplimiento de la obligación establecida en el apartado anterior.
7. Garantizar la formación necesaria en materia de protección de datos personales de las personas autorizadas para tratar datos personales.
8. Cuando las personas afectadas ejerzan los derechos de acceso, rectificación, supresión y portabilidad de datos y oposición y limitación del tratamiento ante el encargado del tratamiento, este deberá comunicarlo por correo electrónico a la dirección que indique el responsable con la mayor prontitud. La comunicación debe hacerse de forma inmediata y en ningún caso más allá del día laborable siguiente al de la recepción de la solicitud, juntamente, en su caso, con otras informaciones que puedan ser relevantes para resolverla. Asistirá al responsable, siempre que sea posible, para que este pueda cumplir y dar respuesta a las solicitudes de ejercicio de derechos.
9. Previo a la realización de comunicaciones comerciales, consultar los sistemas de exclusión publicitaria que pudieran afectar a su actuación y en concreto el fichero *Lista Robinson* gestionado por la Asociación Española de Economía Digital (ADIGITAL), excluyendo del tratamiento los datos de los interesados inscritos que hubieran manifestado su oposición o negativa a recibir publicidad.

- [Enlace al servicio de consulta de la Lista Robinson](#)

No será necesaria la consulta si se ha obtenido el consentimiento previo de los interesados por parte de la empresa.

10. Llevar, por escrito, un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta del responsable, que contenga:
 - a) El nombre y los datos de contacto del encargado o encargados y de cada responsable por cuenta del cual actúe el encargado y, en su caso, del representante del responsable o del encargado y del delegado de protección de datos.
 - b) Las categorías de tratamientos efectuados por cuenta del responsable.
 - c) Una descripción general de las medidas técnicas y organizativas de seguridad apropiadas que esté aplicando y que sean necesarias para garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento de los datos personales. En todo caso, el encargado deberá implantar mecanismos para:
 - I. Garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.
 - II. Restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.
 - III. Verificar, evaluar y valorar, de forma regular, la eficacia de las medidas técnicas y organizativas implantadas para garantizar la seguridad del tratamiento.
 - IV. Seudonimizar y cifrar los datos personales, en su caso.



Las medidas de seguridad que el encargado adopta, a título enunciativo no exhaustivo, son las recogidas en el anexo I de este contrato.

11. Notificación de violaciones de la seguridad de los datos

El encargado del tratamiento notificará al responsable del tratamiento, sin dilación indebida y a través de la dirección de correo electrónico que le indique 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. Asimismo, notificará cualquier fallo que haya sufrido en sus sistemas de tratamiento y gestión de la información y que pueda poner en peligro la seguridad de los datos personales tratados, su integridad o disponibilidad, así como cualquier posible vulneración de la confidencialidad como consecuencia de la puesta en conocimiento de terceros de los datos e informaciones accedidos durante la ejecución del contrato.

Se facilitará, como mínimo, la información siguiente:

- a) Descripción de la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados.
- b) Datos de la persona de contacto para obtener más información.
- c) Descripción de las posibles consecuencias de la violación de la seguridad de los datos personales
- d) Descripción de las medidas adoptadas o propuestas para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

Si no es posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.

Encargado de Tratamiento a petición del responsable, comunicará en el menor tiempo posible las violaciones de la seguridad de los datos a los interesados, cuando sea probable que la violación suponga un alto riesgo para los derechos y las libertades de las personas físicas.

La comunicación debe realizarse en un lenguaje claro y sencillo y deberá, incluir los elementos que en cada caso señale el responsable, como mínimo los aspectos indicados en el párrafo anterior.

12. Poner disposición del responsable toda la información necesaria para demostrar el cumplimiento de sus obligaciones, así como para la realización de las auditorías o las inspecciones que realicen el responsable u otro auditor autorizado por él.

13. Destino de los datos:

Suprimir, devolver al responsable del tratamiento o entregar, en su caso, a un nuevo encargado según determine Ana SM, todos los datos de carácter personal una vez finalizada la prestación del servicio de tratamiento encargado.

No procede la destrucción de los datos cuando exista una previsión legal que obligue a su conservación, en cuyo caso deben devolverse al responsable que garantizará su conservación, debidamente bloqueados, mientras tal obligación persista.

La devolución debe comportar el borrado total de los datos existentes en los equipos informáticos utilizados por el encargado. No obstante, el encargado puede conservar una copia de los datos

debidamente bloqueados, mientras puedan derivarse responsabilidades de la ejecución de los servicios prestados al responsable del tratamiento.

14. SUBCONTRATACIÓN.

No se autoriza al encargado para subcontratar ninguna de las prestaciones que formen parte del objeto de este contrato y que comporten el tratamiento de datos personales, salvo los servicios auxiliares necesarios para el normal funcionamiento de los servicios del encargado.

Si fuera necesario subcontratar algún tratamiento distinto del anterior indicado, este hecho se deberá comunicar previamente y por escrito al responsable, con una antelación de 30 días, indicando los tratamientos que se pretenden subcontratar e identificando de forma clara e inequívoca la empresa subcontratista y sus datos de contacto. La subcontratación podrá llevarse a cabo si el responsable no manifiesta su oposición en el plazo establecido.

El subcontratista, que también tendrá la condición de encargado del tratamiento, está obligado igualmente a cumplir las obligaciones establecidas en este documento para el encargado del tratamiento y las instrucciones que dicte el responsable.

Corresponde al encargado inicial regular la nueva relación, de forma que el nuevo encargado quede sujeto a las mismas condiciones (instrucciones, obligaciones, medidas de seguridad, etc.) 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 del subencargado, el encargado inicial seguirá siendo plenamente responsable ante el responsable en lo referente al cumplimiento de las obligaciones.

15. Una vez se finalice la prestación de los servicios el encargado debe devolver al responsable del tratamiento los datos de carácter personal y, si procede, los soportes donde consten, una vez cumplida la prestación.

La devolución debe comportar el borrado total de los datos existentes en los equipos informáticos utilizados por el encargado. No obstante, el encargado puede conservar una copia, con los datos debidamente bloqueados, mientras puedan derivarse responsabilidades de la ejecución de la prestación.

Cinco. OBLIGACIONES DEL RESPONSABLE DEL TRATAMIENTO

Corresponde al responsable del tratamiento:

1. Entregar al encargado los datos necesarios para que pueda prestar el servicio.
2. Velar, de forma previa y durante todo el tratamiento, por el cumplimiento del RGPD y de este contrato por parte del encargado.
3. Supervisar el tratamiento.

Este documento entra en vigor para las partes, en lugar y fecha de aceptación del contrato de servicios.

ANEXO I. MEDIDAS DE SEGURIDAD QUE EL ENCARGADO ADOPTA.

A título enunciativo no exhaustivo, son las siguientes:

MEDIDAS ORGANIZATIVAS. Todo el personal con acceso a los datos personales tiene conocimiento de sus obligaciones con relación a los tratamientos de datos personales y son informados acerca de dichas obligaciones y en especial de confidencialidad y secreto que persiste incluso cuando finalice la relación laboral del trabajador con la empresa.

MEDIDAS TÉCNICAS

Identificación

- Se dispone de perfiles con derechos de administración para la instalación y configuración del sistema y usuarios sin privilegios o derechos de administración para el acceso a los datos personales.
- Se garantizará la existencia de contraseñas para el acceso a los datos personales almacenados en sistemas electrónicos. La contraseña tendrá al menos 8 caracteres, mezcla de números y letras.
- Cuando a los datos personales accedan distintas personas, para cada persona con acceso a los datos personales, se dispondrá de un usuario y contraseña específicos (identificación inequívoca).
- Se debe garantizar la confidencialidad de las contraseñas, evitando que queden expuestas a terceros.

Deber de salvaguarda. Se exponen algunas de las medidas técnicas para garantizar la salvaguarda de los datos personales:

- **ACTUALIZACIÓN DE ORDENADORES Y DISPOSITIVOS:** Los dispositivos y ordenadores utilizados para el almacenamiento y el tratamiento de los datos personales se mantienen actualizados en la media posible.
- **ANTIVIRUS:** En los ordenadores y dispositivos donde se realice el tratamiento automatizado de los datos personales se dispondrá de un sistema de antivirus que garantice en la medida posible el robo y destrucción de la información y datos personales. El sistema de antivirus deberá ser actualizado de forma periódica.
- **CORTAFUEGOS O FIREWALL:** Para evitar accesos remotos indebidos a los datos personales se velará para garantizar la existencia de un firewall activado en aquellos ordenadores y dispositivos en los que se realice el almacenamiento y/o tratamiento de datos personales.
- **CIFRADO DE DATOS:** Cuando se precise realizar la extracción de datos personales fuera del recinto donde se realiza su tratamiento, ya sea por medios físicos o por medios electrónicos, se deberá valorar la posibilidad de utilizar un método de encriptación para garantizar la confidencialidad de los datos personales en caso de acceso indebido a la información.
- **COPIA DE SEGURIDAD:** Periódicamente se realizará una copia de seguridad en un segundo soporte distinto del que se utiliza para el trabajo diario. La copia se almacenará en lugar seguro, distinto de aquél en que esté ubicado el ordenador con los ficheros originales, con el fin de permitir la recuperación de los datos personales en caso de pérdida de la información.

Las medidas de seguridad serán revisadas de forma periódica, la revisión podrá realizarse por mecanismos automáticos (software o programas informáticos) o de forma manual.