

# **ANEXO DE ENCARGO DE TRATAMIENTO A EFECTOS DE LA NORMATIVA EUROPEA DE PROTECCIÓN DE DATOS PERSONALES A LAS CONDICIONES GENERALES DE CONTRATACIÓN DE ACCEPTABLE**

## **ANEXO**

### **ACTUACIÓN DEL ENCARGADO DEL TRATAMIENTO PARA LA GESTIÓN DEL SERVICIO DE CONTRATACIÓN, RESOLUCIÓN DE INCIDENCIAS Y CONSULTORIA LEGAL SOBRE CONTRATACIÓN ELECTRONICA DE ACCEPTABLE (ARAGONESA DE LEGISLACIÓN Y ACREDITACIÓN S.L.)**

#### **1. Objeto del encargo del tratamiento**

**ACCEPTABLE** actuará como encargado del tratamiento para tratar por cuenta **DEL USUARIO** , en calidad de responsable del tratamiento, los datos de carácter personal estrictamente necesarios para prestar el servicio que en adelante se especifica:

**PRESTACIÓN DEL SERVICIO DE CONTRATACIÓN, INSERCIÓN Y ALMACENAMIENTO DE DATOS MEDIANTE BLOCKCHAIN, RESOLUCIÓN DE INCIDENCIAS Y CONSULTORIA LEGAL SOBRE CONTRATACIÓN ELECTRONICA DE ACCEPTABLE**

#### **2. TRATAMIENTOS A REALIZAR E IDENTIFICACIÓN DE LA INFORMACIÓN AFECTADA**

El servicio contratado supone el tratamiento de datos personales de usuarios del servicio y del personal.

##### **Tratamientos a realizar:**

Recogida  Registro  Estructuración  Modificación  Conservación  Extracción  
 Consulta  Comunicación por transmisión  Difusión  Interconexión  Cotejo  
 Limitación  Supresión  Destrucción  Comunicación  Acceso

##### **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 de **ACCEPTABLE** , los datos estrictamente necesarios para el desarrollo de la actividad:

- **SERVICIO DE CONTRATACIÓN, INSERCIÓN Y ALMACENAMIENTO DE DATOS MEDIANTE BLOCKCHAIN, RESOLUCIÓN DE INCIDENCIAS Y CONSULTORIA LEGAL SOBRE CONTRATACIÓN ELECTRONICA DE ACCEPTABLE**

2.1 El tratamiento de los datos que el encargado del tratamiento se compromete a realizar en el marco del presente servicio se limitará a las actuaciones necesarias para desarrollar correctamente la prestación del **SERVICIO DE CONTRATACIÓN, INSERCIÓN Y ALMACENAMIENTO DE DATOS MEDIANTE BLOCKCHAIN, RESOLUCIÓN DE INCIDENCIAS Y CONSULTORIA LEGAL SOBRE CONTRATACIÓN ELECTRONICA DE ACCEPTABLE** .

2.2 El encargado del tratamiento se compromete a efectuar dicho tratamiento de acuerdo con lo dispuesto en las condiciones de contratación , con las instrucciones que reciba documentadamente del responsable del tratamiento y, en todo caso, con las normas legales y reglamentarias aplicables.

2.3 El acceso por parte del encargado del tratamiento a los datos de carácter personal contenidos en los tratamientos del responsable se realizará única y exclusivamente para la finalidad prevista en el presente servicio, de forma que el encargado del tratamiento pueda prestar al responsable del tratamiento el servicio acordado.

El responsable del tratamiento podrá efectuar las comprobaciones pertinentes a fin de que ACCEPTABLE haya implementado garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con los requisitos del Artículo 28 del Reglamento Europeo de Protección de Datos y garantice la protección de los derechos de los interesados

### **3. Duración**

El presente servicio entra en vigor en el día de la firma del presente documento anexo a las condiciones de contratación y estará vigente hasta la fecha de terminación de la relación de la prestación de servicios por parte del encargado del tratamiento a favor del responsable del tratamiento.

Una vez cumplida la prestación contractual, y en el momento en que, en cumplimiento de las condiciones pactadas o legalmente previstas, finalice la relación entre ambas partes, el encargado del tratamiento deberá destruir o devolver los datos de carácter personal facilitados por el responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento, según le indique el responsable.

No obstante, podrá mantener bloqueados los datos para atender posibles responsabilidades administrativas o jurisdiccionales.

#### 4. Obligaciones del encargado del tratamiento

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

- ✓ Utilizar los datos personales objeto de tratamiento, o los que recoja para su inclusión, sólo para la finalidad objeto de este encargo, sin que pueda utilizarlos con fines propios.
- ✓ Tratar los datos de acuerdo con las instrucciones documentadas del responsable del tratamiento.
- ✓ Llevar, por escrito, un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta del responsable, que contenga:
  - 1 El nombre y los datos de contacto del encargado o encargados y de cada responsable por cuenta del cual actúe el encargado.
  - 2 Las categorías de tratamientos efectuados por cuenta de cada responsable.
  - 3 Una descripción general de las medidas técnicas y organizativas de seguridad apropiadas que esté aplicando.
- ✓ No comunicar los datos a terceras personas, salvo que cuente con la autorización expresa del responsable del tratamiento, en los supuestos legalmente admisibles. Si el encargado quiere subcontratar tiene que informar al responsable y solicitar su autorización previa.  
La falta de autorización podrá dar lugar a la resolución del contrato por parte del **RESPONSABLE** sin que este deba dar compensación alguna al **ADJUDICATARIO** por dicha resolución.

EL USUARIO AUTORIZA LA SUBCONTRATACIÓN DE LOS SIGUIENTES SERVICIOS:

- D. Roberto L. Ferrer Serrano Letrado del R. e I. Colegio de Zaragoza, nº 2870
- Sistemas de almacenamiento en proveedores de servicios AMAZON y OVH

- ✓ 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 servicio.
- ✓ 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.
- ✓ Mantener a disposición del responsable la documentación acreditativa del cumplimiento de sus obligaciones.
- ✓ Garantizar la formación necesaria en materia de protección de datos personales de las personas autorizadas para tratar datos personales.

- ✓ Cuando las personas afectadas ejerzan los derechos de acceso, rectificación, supresión y oposición, limitación del tratamiento y portabilidad de datos ante el encargado del tratamiento, éste debe comunicarlo por correo electrónico a la dirección electrónica proporcionada por el responsable del tratamiento. La comunicación debe hacerse teniendo en cuenta la naturaleza del tratamiento y el volumen o la calidad de la información a su disposición, juntamente, en su caso, con otras informaciones que puedan ser relevantes para resolver la solicitud.
- ✓ Notificación de violaciones de la seguridad de los datos

El encargado del tratamiento notificará fehacientemente al responsable del tratamiento, sin dilación indebida y como máximo en el plazo de 24h desde que tenga conocimiento, a través de la dirección de correo electrónico a la dirección electrónica proporcionada por el responsable del tratamiento, 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.

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 y 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.

El encargado del tratamiento, a petición del responsable, comunicará en el menor tiempo posible esas 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:

- a) La naturaleza de la violación de datos.

- b) Datos del punto de contacto del responsable o del encargado donde se pueda obtener más información.
  - c) Describir las posibles consecuencias de la violación de la seguridad de los datos personales.
  - d) Describir las medidas adoptadas o propuestas por el responsable del tratamiento 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.
- ✓ Poner a disposición del responsable toda la información necesaria para demostrar el cumplimiento de sus obligaciones, incluidas las evaluaciones de impacto en su caso, así como para la realización de las auditorías o las inspecciones que realicen el responsable u otro auditor autorizado por él.
  - ✓ 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, previstas en el artículo 32 del Reglamento Europeo de Protección de Datos, ayudándole a garantizar el cumplimiento de sus obligaciones previstos en los arts. 32 a 36 del Reglamento Europeo de Protección de Datos.

Asimismo, y de acuerdo con lo establecido en la normativa de Protección de Datos, el encargado del tratamiento adoptará las medidas técnicas y organizativas necesarias para garantizar la seguridad, integridad y confidencialidad de los datos de carácter personal a los que tenga acceso, trate o transmita para prestar el **SERVICIO DE CONTRATACIÓN, INSERCIÓN Y ALMACENAMIENTO DE DATOS MEDIANTE BLOCKCHAIN, RESOLUCIÓN DE INCIDENCIAS Y CONSULTORIA LEGAL SOBRE CONTRATACIÓN ELECTRONICA DE ACCEPTABLE**. En particular, el encargado del tratamiento se obliga a aplicar a dichos datos las medidas, normas y procedimientos adecuados para garantizar la seguridad de los datos personales y como mínimo las descritas en las CLAUSULAS ADICIONALES.

#### **5. Obligaciones del responsable del tratamiento**

Corresponde al responsable del tratamiento:

- a) Entregar al encargado los datos necesarios para que pueda prestar el servicio.
- b) Velar, de forma previa y durante todo el tratamiento, por el cumplimiento del RGPD por parte del encargado.
- c) Supervisar el tratamiento.
- d) Cumplir en todo momento la normativa de protección de datos de carácter personal.

## **6. Empleados del encargado del tratamiento**

El encargado del tratamiento permitirá el acceso a los datos personales únicamente a aquellos de sus empleados que tengan necesidad de acceder a los mismos, de manera que puedan llevar a cabo sus funciones para la correcta prestación del servicio al USUARIO

No obstante, queda autorizado el tratamiento de los datos del RESPONSABLE que realicen las personas físicas que presten sus servicios al ENCARGADO, actuando dentro del marco organizativo de éste en virtud de una relación mercantil o profesional y no laboral.

El encargado del tratamiento les informará de las obligaciones contenidas en este servicio y les exigirá su cumplimiento. En particular, deberá advertirles del carácter confidencial de los datos y la información contenida en los ficheros y de la responsabilidad en que pueden incurrir en caso de divulgarla ilícitamente.

## **7. Secreto profesional y prohibición de cesión de datos personales.**

El encargado del tratamiento se compromete a guardar bajo su control y custodia todos los datos suministrados por el responsable del tratamiento en el marco del servicio prestado al USUARIO y a no divulgarlos, transferirlos, o de cualquier forma comunicarlos, ni siquiera para su conservación, a otras personas. Estas obligaciones subsistirán aun después de finalizar el presente servicio.

## **8. Responsabilidades**

El encargado del tratamiento será considerado responsable del tratamiento de datos de carácter personal, respondiendo de las infracciones en que hubiese incurrido personalmente, en el caso de que destine los datos a otra finalidad distinta de la establecida en este servicio, los comunique a terceras personas, vulnere el deber de guardar secreto sobre los mismos o los utilice indebidamente.

## **CLAUSULAS ADICIONALES**

### **OBLIGACIONES MÍNIMAS DE SEGURIDAD QUE DEBERÁ IMPLEMENTAR EL ENCARGADO DEL TRATAMIENTO EN RELACIÓN A LA INFORMACIÓN A QUE ACCEDA TITULARIDAD DEL RESPONSABLE DEL TRATAMIENTO**

#### **OBLIGACIONES DE CONTEXTO:**

El encargado del tratamiento deberá realizar el tratamiento de los datos personales titularidad del responsable a que acceda deberá establecer un contexto de tratamiento de los datos respetuoso con lo establecido en la normativa de protección de datos de carácter personal,

realizar el correspondiente análisis de riesgos a que estos se encuentren sometidos y a actualizarlo teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, en la forma prevista en el artículo 32 del vigente Reglamento Europeo de Protección de Datos.

## **IDENTIFICACIÓN**

Solo con autorización expresa de la dirección de la Entidad podrán utilizarse dispositivos de esta con fines no profesionales. Cuando el mismo ordenador o dispositivo se utilice para el tratamiento de datos personales y fines de uso personal se recomienda disponer de varios perfiles o usuarios distintos para cada una de las finalidades. Deben mantenerse separados los usos profesional y personal del ordenador.

Se recomienda disponer 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. Esta medida evitará que en caso de ataque de ciberseguridad puedan obtenerse privilegios de acceso o modificar el sistema operativo.

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. En ningún caso se compartirán las contraseñas ni se dejarán anotadas en lugar común y el acceso de personas distintas del usuario.

## **FUNCIONES Y OBLIGACIONES DEL PERSONAL**

Las funciones y obligaciones de cada uno de los usuarios o perfiles de usuario con acceso a datos y a los sistemas estarán claramente definidas y documentadas.

El personal deberá encontrarse debidamente formado y concienciado en materia de tratamiento de datos de carácter personal.

## **ALMACENAMIENTO SEGURO DE SOPORTES Y DOCUMENTOS**

Cuando los soportes y/o documentos del responsable del tratamiento se encuentren dentro de los locales del encargado, se adoptarán las medidas necesarias para impedir la sustracción, pérdida o acceso indebido a la información contenida en los mismos.

## **TRASLADO SEGURO DE SOPORTES Y DOCUMENTOS**

Cuando los soportes y/o documentos del responsable del tratamiento salgan fuera de los locales del encargado, se adoptarán las medidas necesarias para impedir la sustracción, pérdida o acceso indebido a la información contenida en los mismos durante el transporte.

## **DESTRUCCIÓN Y REUTILIZACIÓN DE EQUIPOS Y SOPORTES**

Los documentos físicos o lógicos, de cualquier tipo, que puedan contener datos personales, deberán ser eliminados o destruidos de forma segura para garantizar que no se va a poder acceder a ellos a partir del momento de su destrucción.