

## REGISTRO DE ACTIVIDADES COMO RESPONSABLE DEL TRATAMIENTO (GENERAL)

### 1. Identificación de la organización Responsable del tratamiento

De conformidad con lo dispuesto en el Reglamento (UE) 2016/679 de 27 de abril de 2016 (GDPR), la organización Responsable del tratamiento es quién determina los fines y los medios del tratamiento de datos personales (Ficheros).

Nombre fiscal	ASOCIACION DE HUESOS DE CRISTAL DE ESPAÑA
NIF	G81109100
Actividad	Asociación de personas con Osteogénesis Imperfecta
Dirección	C/ San Ildefonso, 8 - 28012 Madrid (Madrid)
Teléfono	914678266
E-mail	ahuce@ahuce.org
Marca comercial	ASOCIACION DE HUESOS DE CRISTAL DE ESPAÑA
Web	<a href="http://www.ahuce.org/">http://www.ahuce.org/</a>
E-mail Notificación AEPD	ahuce@ahuce.org
E-mail ejercicio derechos	ahuce@ahuce.org
Representante legal	GERARDO MUÑOZ FERNANDEZ
Responsable de privacidad (DSPO)	GERARDO MUÑOZ FERNANDEZ
Encargado de privacidad (DSPP)	GERARDO MUÑOZ FERNANDEZ
Número empleados	3

### 2. Identificación de los tratamientos de datos personales tratados por cuenta propia

Un fichero es un conjunto estructurado de datos personales accesibles con arreglo a criterios determinados y susceptibles de tratamiento para un fin específico.

Fichero	Descripción
1 LABORAL Y RR HH	Registro de datos de personal para fines organizativos, así como para la confección de nóminas y gestión del resto de obligaciones fiscales y laborales que puedan derivarse de la relación laboral.
2 PROVEEDORES	Registro de datos de proveedores para la adecuada prestación del servicio contratado, así como para el cumplimiento de las obligaciones fiscales o contables que se puedan derivar de la relación contractual.
3 SOCIOS Y VOLUNTARIOS	Registro de datos de socios, colaboradores y voluntarios con la finalidad de organizar la actividad asociativa de la entidad, así como para la gestión administrativa, fiscal y contable de la misma.
4 DONANTES	Registro de datos de identificación de donantes para la gestión de los donativos realizados con la finalidad de cumplir con las correspondientes obligaciones legales, fiscales y contables.
5 PATROCINADORES	Registro de datos de patrocinadores para la gestión administrativa de la entidad, así como para la gestión legal, fiscal y contable de la misma.
6 MEDICOS	Registro de datos de profesionales médicos que integran el Comité Científico de la entidad para la gestión administrativa del mismo.
7 FISIOTERAPEUTAS	Registro de datos de fisioterapeutas que colaboran con la entidad para la organización de la misma, así como para el cumplimiento de las correspondientes obligaciones fiscales y contables.
8 CONTROL HORARIO	Registro y control de entradas y salidas de los empleados a las instalaciones

### 3. Registro de las actividades del tratamiento

De conformidad con el artículo 30 del Reglamento (UE) 2016/679 de 27 de abril de 2016 (GDPR), la Organización deberá llevar y conservar actualizado un Registro de las actividades de tratamiento efectuadas bajo su responsabilidad, en formato electrónico, que contenga:

- Nombre y datos contacto del Responsable del tratamiento, y en su caso, del Corresponsable del tratamiento, del Representante del Responsable y del Delegado de protección de datos (DPO).
- Fines del tratamiento.
- Descripción de las categorías de interesados.
- Descripción de las categorías de datos.
- Categorías de Destinatarios.
- Transferencias de datos a terceros países, con la identificación de los mismos y documentación de garantías adecuadas.
- Cuando sea posible:
  - Plazos previstos para la supresión de las diferentes categorías de datos.
  - Descripción general de las medidas técnicas y organizativas de seguridad.

Los Responsables del tratamiento, o sus Representantes, deberán poner a disposición de la Autoridad de control este Registro de actividades, cuando ésta lo solicite.

Este Registro se ha documentado para cada uno de los Ficheros descritos en el apartado 2 y se detallan a continuación. Al final del documento se detalla una descripción general de las medidas técnicas y organizativas implementadas por la Organización, desde el diseño y por defecto en todas las fases del tratamiento.

### LABORAL Y RR HH

Descripción	Registro de datos de personal para fines organizativos, así como para la confección de nóminas y gestión del resto de obligaciones fiscales y laborales que puedan derivarse de la relación laboral.
Finalidades	Prevención de riesgos laborales, Gestión de nóminas, Recursos humanos
Legitimación	Para la ejecución de un CONTRATO o precontrato con el interesado
Categorías de interesados	Empleados
Criterios de conservación	<b>Conservados durante MÁS TIEMPO DEL NECESARIO para alcanzar los fines</b> por una OBLIGACIÓN LEGAL
Sistema de tratamiento	Parcialmente Automatizado (Mixto)
<b>Categorías de datos</b>	
Datos identificativos	DNI o NIF, Nombre y apellidos, Dirección postal o electrónica, Teléfono, Firma manual, Núm. de SS SS o mutualidad
Datos sensibles	No existen
Otro tipo de datos	Características personales, Académicos y profesionales, Detalles de empleo, Económicos, financieros y de seguro, Transacciones de bienes y servicios
<b>Categorías de destinatarios</b>	
Cesiones	Órganos judiciales, Bancos, cajas de ahorro y cajas rurales, Organismos de la Seguridad Social, Administración tributaria, Fuerzas y cuerpos de seguridad, Administración pública con competencia en la materia
Transferencias internacionales	No existen

### PROVEEDORES

Descripción	Registro de datos de proveedores para la adecuada prestación del servicio contratado, así como para el cumplimiento de las obligaciones fiscales o contables que se puedan derivar de la relación contractual.
Finalidades	Otras finalidades: Gestión de proveedores, contable, fiscal y administrativa
Legitimación	Para la ejecución de un CONTRATO o precontrato con el interesado
Categorías de interesados	Proveedores
Criterios de conservación	<b>Conservados durante MÁS TIEMPO DEL NECESARIO para alcanzar los fines por una OBLIGACIÓN LEGAL</b>
Sistema de tratamiento	Parcialmente Automatizado (Mixto)
<b>Categorías de datos</b>	
Datos identificativos	DNI o NIF, Nombre y apellidos, Dirección postal o electrónica, Teléfono, Firma manual
Datos sensibles	No existen
Otro tipo de datos	Características personales, Información comercial, Económicos, financieros y de seguro, Transacciones de bienes y servicios
<b>Categorías de destinatarios</b>	
Cesiones	Órganos judiciales, Bancos, cajas de ahorro y cajas rurales, Administración tributaria, Fuerzas y cuerpos de seguridad, Administración pública con competencia en la materia
Transferencias internacionales	No existen

### SOCIOS Y VOLUNTARIOS

Descripción	Registro de datos de socios, colaboradores y voluntarios con la finalidad de organizar la actividad asociativa de la entidad, así como para la gestión administrativa, fiscal y contable de la misma.
Finalidades	Otras finalidades: Gestión de asociados y voluntarios
Legitimación	Para la ejecución de un CONTRATO o precontrato con el interesado
Categorías de interesados	Asociados y miembros, Otros colectivos de interesados: Voluntarios
Criterios de conservación	<b>Conservados durante MÁS TIEMPO DEL NECESARIO para alcanzar los fines</b> por una OBLIGACIÓN LEGAL
Sistema de tratamiento	Parcialmente Automatizado (Mixto)
<b>Categorías de datos</b>	
Datos identificativos	DNI o NIF, Nombre y apellidos, Dirección postal o electrónica, Teléfono, Firma manual, Marcas físicas, Datos genéticos
Datos sensibles	Salud
Otro tipo de datos	Características personales, Circunstancias sociales
<b>Categorías de destinatarios</b>	
Cesiones	Órganos judiciales, Bancos, cajas de ahorro y cajas rurales, Entidades sanitarias, Organismos de la Seguridad Social, Administración tributaria, Fuerzas y cuerpos de seguridad, Administración pública con competencia en la materia
Transferencias internacionales	No existen

### DONANTES

Descripción	Registro de datos de identificación de donantes para la gestión de los donativos realizados con la finalidad de cumplir con las correspondientes obligaciones legales, fiscales y contables.
Finalidades	Otras finalidades: Gestión de donativos
Legitimación	<b>Tratamiento lícito SIN NECESIDAD DE CONSENTIMIENTO</b> por una OBLIGACIÓN LEGAL del Responsable del tratamiento
Categorías de interesados	Otros colectivos de interesados: Donantes
Criterios de conservación	<b>Conservados durante MÁS TIEMPO DEL NECESARIO para alcanzar los fines</b> por una OBLIGACIÓN LEGAL
Sistema de tratamiento	Parcialmente Automatizado (Mixto)
<b>Categorías de datos</b>	
Datos identificativos	DNI o NIF, Nombre y apellidos, Dirección postal o electrónica, Teléfono, Firma manual
Datos sensibles	No existen
Otro tipo de datos	Características personales, Económicos, financieros y de seguro
<b>Categorías de destinatarios</b>	
Cesiones	Órganos judiciales, Bancos, cajas de ahorro y cajas rurales, Administración tributaria, Fuerzas y cuerpos de seguridad, Administración pública con competencia en la materia
Transferencias internacionales	No existen

### PATROCINADORES

Descripción	Registro de datos de patrocinadores para la gestión administrativa de la entidad, así como para la gestión legal, fiscal y contable de la misma.
Finalidades	Otras finalidades: Gestión de patrocinadores
Legitimación	<b>Tratamiento lícito SIN NECESIDAD DE CONSENTIMIENTO</b> por una OBLIGACIÓN LEGAL del Responsable del tratamiento
Categorías de interesados	Otros colectivos de interesados: Patrocinadores
Criterios de conservación	<b>Conservados durante MÁS TIEMPO DEL NECESARIO para alcanzar los fines</b> por una OBLIGACIÓN LEGAL
Sistema de tratamiento	Parcialmente Automatizado (Mixto)
<b>Categorías de datos</b>	
Datos identificativos	DNI o NIF, Nombre y apellidos, Dirección postal o electrónica, Teléfono, Firma manual
Datos sensibles	No existen
Otro tipo de datos	Características personales, Económicos, financieros y de seguro
<b>Categorías de destinatarios</b>	
Cesiones	Órganos judiciales, Bancos, cajas de ahorro y cajas rurales, Administración tributaria, Fuerzas y cuerpos de seguridad, Administración pública con competencia en la materia
Transferencias internacionales	No existen

### MEDICOS

Descripción	Registro de datos de profesionales médicos que integran el Comité Científico de la entidad para la gestión administrativa del mismo.
Finalidades	Otras finalidades: Gestión de datos de médicos con fines organizativos del Comité Científico
Legitimación	Consentimiento INEQUÍVOCO mediante una clara acción del interesado
Categorías de interesados	No existen
Criterios de conservación	Conservados INDEFINIDAMENTE mientras sea necesario para mantener el fin del tratamiento
Sistema de tratamiento	Parcialmente Automatizado (Mixto)
<b>Categorías de datos</b>	
Datos identificativos	DNI o NIF, Nombre y apellidos, Dirección postal o electrónica, Teléfono, Firma manual
Datos sensibles	No existen
Otro tipo de datos	Características personales, Académicos y profesionales, Detalles de empleo
<b>Categorías de destinatarios</b>	
Cesiones	Órganos judiciales, Fuerzas y cuerpos de seguridad, Administración pública con competencia en la materia
Transferencias internacionales	No existen

### FISIOTERAPEUTAS

Descripción	Registro de datos de fisioterapeutas que colaboran con la entidad para la organización de la misma, así como para el cumplimiento de las correspondientes obligaciones fiscales y contables.
Finalidades	Otras finalidades: Gestión de datos de fisioterapeutas con fines organizativos
Legitimación	Consentimiento INEQUÍVOCO mediante una clara acción del interesado
Categorías de interesados	Otros colectivos de interesados: Fisioterapeutas
Criterios de conservación	Conservados INDEFINIDAMENTE mientras sea necesario para mantener el fin del tratamiento
Sistema de tratamiento	Parcialmente Automatizado (Mixto)
<b>Categorías de datos</b>	
Datos identificativos	DNI o NIF, Nombre y apellidos, Dirección postal o electrónica, Teléfono, Firma manual
Datos sensibles	No existen
Otro tipo de datos	Características personales, Detalles de empleo
<b>Categorías de destinatarios</b>	
Cesiones	Órganos judiciales, Fuerzas y cuerpos de seguridad, Administración pública con competencia en la materia
Transferencias internacionales	No existen

### CONTROL HORARIO

Descripción	Registro y control de entradas y salidas de los empleados a las instalaciones
Finalidades	Gestión de nóminas, Recursos humanos
Legitimación	<b>Tratamiento lícito SIN NECESIDAD DE CONSENTIMIENTO</b> por una OBLIGACIÓN LEGAL del Responsable del tratamiento
Categorías de interesados	Empleados
Criterios de conservación	Conservados durante NO MÁS TIEMPO DEL NECESARIO para alcanzar los fines
Sistema de tratamiento	Parcialmente Automatizado (Mixto)
<b>Categorías de datos</b>	
Datos identificativos	DNI o NIF, Nombre y apellidos, Firma manual
Datos sensibles	No existen
Otro tipo de datos	Detalles de empleo
<b>Categorías de destinatarios</b>	
Cesiones	Órganos judiciales, Bancos, cajas de ahorro y cajas rurales, Administración tributaria, Fuerzas y cuerpos de seguridad, Administración pública con competencia en la materia
Transferencias internacionales	No existen

## MEDIDAS TÉCNICAS Y ORGANIZATIVAS DE SEGURIDAD

### Locales o delegaciones

SEDE PRINCIPAL		
Tipo de acceso al local	Puerta cerrada con control de acceso (portero, timbre, llave, huella dactilar, etc.).	Sin riesgo
Sistema general de control de llaves	Las llaves se guardan en un lugar seguro y con acceso autorizado a las mismas	Bajo
Otras medidas de seguridad	NO EXISTEN medidas de seguridad.	Bajo

### Departamentos

OFICINA		
Permiso:	Limitado a personal autorizado en todo el Departamento.	Bajo
Acceso:	Acceso al Departamento regido por las medidas de seguridad del Local.	Bajo
Control de llaves:	NO EXISTEN llaves ya que el acceso al Departamento se rige por las medidas de seguridad del Local.	Bajo
Otras medidas de seguridad:	NO EXISTEN otras medidas de seguridad.	Bajo

### Confidencialidad de la información

Información del tratamiento al interesado		
¿Se informa al interesado de los detalles del tratamiento?	Sí, con cláusulas genéricas de protección de datos. <i>Se deberá facilitar la información específica del tratamiento de forma clara y transparente.</i>	Medio
¿Se informa al interesado de los derechos que le asisten?	Sí, con cláusulas genéricas de protección de datos. <i>Se deberá facilitar la información de todos los derechos que asisten al interesado.</i>	Medio
Transporte y transmisión de datos		
Transporte de los soportes dentro de la empresa	NO SE TRANSPORTAN soportes dentro de la Empresa.	Sin riesgo
Transporte de los soportes fuera de la empresa	NO SE TRANSPORTAN soportes fuera de la Empresa.	Sin riesgo
Procedimientos con datos automatizados (digital)		
Acceso durante el tratamiento digital (pantallas)	NO SE TRATAN ficheros con datos personales a la vista de personas no autorizadas.	Sin riesgo
Almacenamiento de los soportes digitales	Se guardan en un Mobiliario y/o Departamento con medidas de seguridad.	Bajo
Destrucción de soportes digitales	Formateo y desechado	Bajo
Procedimientos con datos no automatizados (documentos)		

<b>Acceso durante el tratamiento manual (documentos)</b>	NO SE TRATAN documentos con datos personales a la vista de personas no autorizadas.	Sin riesgo
<b>Almacenamiento de documentos</b>	Se guardan en un Mobiliario y/o Departamento con medidas de seguridad.	Bajo
<b>Destrucción de documentos</b>	Destructora de papel.	Bajo
Registro de accesos a categorías especiales de datos		
<b>¿Se lleva un registro de accesos a categorías especiales de datos?</b>	No. <i>Plantearse la necesidad de activar un registro de accesos a la aplicación según el tipo de datos que contiene.</i>	Medio

### Sistemas de información

Acceso a equipos informáticos		
<b>Control de acceso a equipos informáticos</b>	Usuario y contraseña personalizados.	Bajo
<b>Control de acceso a ficheros con datos personales</b>	Acceso a los ficheros y/o programa mediante contraseña.	Bajo
<b>Otros tipos de acceso a equipos informáticos</b>	Ninguno	Sin riesgo
Acceso a redes informáticas		
<b>Acceso directo a los sistemas de información (conexión de red)</b>	Usuario y contraseña personalizados.	Bajo
<b>Acceso inalámbrico a los sistemas de información (Wifi, Bluetooth, etc.)</b>	Acceso restringido por clave de seguridad.	Bajo
<b>Acceso remoto a los sistemas de información</b>	Usuario y contraseña personalizados.	Bajo
<b>Cifrado de las conexiones remotas</b>	Sí.	Bajo
Sistema de identificación y autenticación		
<b>Sistema de identificación (USUARIO)</b>	Palabra identificativa y personalizada para cada usuario.	Bajo
<b>Sistema de autenticación (CONTRASEÑA)</b>	Contraseña personalizada para cada usuario.	Bajo
<b>Cifrado de la contraseña</b>	La contraseña está cifrada	Bajo
<b>Combinación de caracteres</b>	Se ha implementado un sistema que comprueba que la combinación de caracteres sea segura	Sin riesgo
<b>Intentos reiterados de acceso</b>	Se ha implementado un sistema que impide los intentos reiterados no autorizados	Bajo
<b>Caducidad de la contraseña</b>	La contraseña se cambia al menos una vez al año	Bajo

### Integridad de la información

Copias de respaldo		
<b>Ubicación de las copias</b>	Se guardan en un <i>Hardware</i> distinto del que las crea (copia de red).	Bajo
<b>Periodicidad de programación</b>	Semanalmente, como mínimo.	Bajo
<b>Periodicidad de comprobación de datos</b>	A partir de 6 meses desde la creación. <i>Se deberán comprobar las copias, como máximo, cada 6 meses.</i>	Alto

<b>Método de comprobación de datos</b>	Aplicación informática de verificación de copias.	Bajo
Copias de respaldo externas		
<b>Ubicación de las copias externas</b>	Servicios <i>Backup</i> de Internet.	Bajo
<b>Periodicidad de programación de las copias externas</b>	Mensualmente. <i>Se deberán realizar semanalmente si ha habido actualizaciones.</i>	Alto
<b>Cifrado de los datos de las copias externas</b>	NO se cifran las copias porque no salen de los locales de la empresa.	Sin riesgo
Disponibilidad de los datos		
<b>Actualización de <i>software</i></b>	SE ACTUALIZAN periódicamente los sistemas operativos y las aplicaciones informáticas con las últimas versiones disponibles	Bajo
<b>Sistemas de detección de intrusos y prevención de fuga de información</b>	EXISTEN sistemas de protección tipo <i>firewall</i> , antivirus, <i>antispam</i> , <i>antiphishing</i> , <i>antimalware</i> , <i>antiransomware</i> , etc.	Bajo
<b>Disponibilidad de los servicios de información</b>	NO SE HAN TOMADO SUFICIENTES medidas para garantizar la disponibilidad de los datos <i>Se deben tomar medidas adecuadas para garantizar la disponibilidad de los servicios de información.</i>	Medio
<b>Restauración de los servicios de información</b>	NO SE HAN TOMADO SUFICIENTES medidas para restaurar rápidamente la disponibilidad y el acceso a los datos <i>Se deben tomar medidas adecuadas para restaurar rápidamente la disponibilidad y el acceso a los datos</i>	Medio
<b>Resiliencia de los servicios de información</b>	NO SE HAN TOMADO SUFICIENTES medidas para anticiparse y adaptarse a cambios imprevistos en los servicios de información <i>Se deben tomar medidas adecuadas para garantizar la resiliencia de los servicios de información.</i>	Medio
<b>Procesos de verificación, evaluación y valoración de las medidas de seguridad</b>	NO SE HAN ESTABLECIDO SUFICIENTES procesos para verificar, evaluar y valorar la eficacia de las medidas de seguridad <i>Se deben establecer procesos para verificar, evaluar y valorar la eficacia de las medidas de seguridad adoptadas.</i>	Alto

### Tratamientos específicos

Tratamientos específicos		
<b>Tratamiento de datos de niños menores de 14 años</b>	Se tratan datos OCASIONALMENTE de niños menores de 14 años	Bajo
<b>Tratamiento de datos de personas en situación de vulnerabilidad</b>	Se tratan datos HABITUALMENTE de personas en situación de vulnerabilidad y NO EXISTE riesgo para sus derechos y libertades	Bajo
<b>Tratamiento de datos que puede invadir la intimidad de las personas</b>	NO SE REALIZAN tratamientos que pueden invadir la intimidad de las personas	Sin riesgo
<b>Vulneración de los derechos y libertades fundamentales</b>	NO SE REALIZAN tratamientos que vulneren los derechos o libertades fundamentales	Sin riesgo

### Organización

Organización		
<b>Política de información</b>	EXISTE un protocolo documentado para informar y comunicar el tratamiento al interesado	Bajo

<b>Derechos del interesado</b>	EXISTE un protocolo documentado para gestionar y registrar los derechos del interesado	Bajo
<b>Política de seguridad</b>	EXISTE un protocolo documentado para garantizar la seguridad de los datos personales	Bajo
<b>Violaciones de la seguridad</b>	EXISTE un protocolo documentado para gestionar y registrar las violaciones de la seguridad	Bajo
<b>Formación en protección de datos</b>	[Se facilita suficiente formación al personal autorizado para tratar datos] mediante la publicación de la política de seguridad	Bajo
<b>Delegado de protección de datos (DPO)</b>	[No precisa un DPO porque la actividad principal de la empresa] CONSISTE en tratar datos personales pero NO a GRAN ESCALA, ni regulados en el art. 34 de la LOPDGDD.	Bajo
<b>Evaluación de impacto (DPIA)</b>	[No precisa realizar una DPIA porque] el tratamiento no comporta un alto riesgo para los derechos y libertades de las personas físicas.	Bajo