

## 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 quien determina los fines y los medios del tratamiento de datos personales (Ficheros).

<b>Nombre fiscal</b>	Asociación Española de Esclerodermia
<b>NIF</b>	G81188435
<b>Actividad</b>	Asociación asistencia enfermedades.
<b>Dirección</b>	C/ Comunidad de La Rioja, 2 - 28231 Las Rozas (Madrid)
<b>Teléfono</b>	911 649 908
<b>E-mail</b>	presidencia@esclerodermia.com
<b>Marca comercial</b>	
<b>Web</b>	esclerodermia.com
<b>E-mail Notificación AEPD</b>	info@esclerodermia.com
<b>E-mail ejercicio derechos</b>	info@esclerodermia.com
<b>Representante legal</b>	Alfonso Sánchez Lorite
<b>Responsable seguridad (DSPO)</b>	Alfonso Sánchez Lorite
<b>Encargado seguridad (DSPP)</b>	Alfonso Sánchez Lorite

### Identificación del Delegado de protección de datos (DPO)

Nombre	CONSULTING NORMATIVO, SL
Dirección	Fénix, 19, 28023 MADRID
Nif	B86932084
Teléfono	9121009359
E-mail	administracion@fundacionprotecciondedatos.es
Web	

### 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.

Tratamiento	Descripción
1 LABORAL Y RR. HH.	Gestión administrativa y laboral del personal empleado en la organización

2 CLIENTES Y PROVEEDORES	Gestión comercial con clientes y proveedores. Incluye datos de contacto de personas físicas que presten servicios a una persona jurídica, inclusive los profesionales individuales
3 FISCAL Y CONTABLE	Registro de las obligaciones fiscales y contables sujetas a la actividad económica
4 CONTACTOS	Comunicación, información y gestión sobre productos y servicios. Incluye contactos web y redes sociales
5 CURRÍCULUMS	Gestión de candidatos a empleados
6 VIDEOVIGILANCIA	Grabación audiovisual de personas por motivos de seguridad
7 REGISTRO JORNADA LABORAL	Registro horario de la jornada laboral para dar cumplimiento al RDL 8/2019, de medidas urgentes de protección social y de lucha contra la precariedad laboral en la jornada de trabajo
8 IMÁGENES	Gestión de audiovisuales para su publicación en los medios de comunicación
9 VOLUNTARIOS	Organización de actividades sociales. Personas, socias o no, que colaboran en la organización de las actividades de la asociación
10 USUARIOS	Gestión de usuarios de la entidad. Incluye datos relacionados con el usuario (representante legal, familiares, características personales y sociales, etc.)
11 USUARIOS SALUD	Gestión administrativa de datos de salud de los usuarios. Incluye el historial clínico y el control sanitario

### 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 de 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 esta lo solicite.

Este Registro se ha documentado para cada uno de los Tratamientos 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.

## 1. LABORAL Y RR. HH.

<b>Tratamiento</b>	
Descripción	Gestión administrativa y laboral del personal empleado en la organización
Finalidades	Prevención de riesgos laborales servicio externo, Gestión de nóminas, Recursos humanos
Legitimación	• Para la ejecución de un CONTRATO o precontrato con el interesado (artículo 6.1.b GDPR)
Origen de los datos	El mismo interesado o su representante legal
Categorías de interesados	Empleados
Criterios de conservación	Conservados mientras existan prescripciones legales que dictaminen la custodia
Sistema de tratamiento	Parcialmente Automatizado
<b>Categorías de datos</b>	
Datos identificativos	DNI/NIF/NIE/Pasaporte, Nombre y apellidos, Dirección postal o electrónica, Teléfono, Firma manual, Núm. de SS o mutualidad
Categorías de datos especiales o penales	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	<ul style="list-style-type: none"> <li>• Organismos de la Seguridad Social</li> <li>• Administración tributaria</li> <li>• Administración pública con competencia en la materia</li> </ul>
Transferencias internacionales	No existen

## 2. CLIENTES Y PROVEEDORES

<b>Tratamiento</b>	
Descripción	Gestión comercial con clientes y proveedores. Incluye datos de contacto de personas físicas que presten servicios a una persona jurídica, inclusive los profesionales individuales
Finalidades	Gestión contable, fiscal y administrativa
Legitimación	• Por un INTERÉS LEGÍTIMO del Responsable del tratamiento o Tercero (artículo 6.1.f GDPR)
Origen de los datos	El mismo interesado o su representante legal
Categorías de interesados	Proveedores, Clientes y usuarios
Criterios de conservación	Conservados durante no más tiempo del necesario para mantener el fin del tratamiento o mientras existan prescripciones legales que dictaminen su custodia
Sistema de tratamiento	Parcialmente Automatizado
<b>Categorías de datos</b>	
Datos identificativos	DNI/NIF/NIE/Pasaporte, Nombre y apellidos, Dirección postal o electrónica, Teléfono, Firma manual
Categorías de datos especiales o penales	No existen
Otro tipo de datos	Características personales, Circunstancias sociales, Información comercial, Transacciones de bienes y servicios
<b>Categorías de destinatarios</b>	
Cesiones	
Transferencias internacionales	No existen

### 3. FISCAL Y CONTABLE

<b>Tratamiento</b>	
Descripción	Registro de las obligaciones fiscales y contables sujetas a la actividad económica
Finalidades	Gestión contable, fiscal y administrativa
Legitimación	• Por una OBLIGACIÓN LEGAL del Responsable del tratamiento (artículo 6.1.c GDPR)
Origen de los datos	El mismo interesado o su representante legal
Categorías de interesados	Proveedores, Clientes y usuarios
Criterios de conservación	Conservados mientras existan prescripciones legales que dictaminen la custodia
Sistema de tratamiento	Parcialmente Automatizado
<b>Categorías de datos</b>	
Datos identificativos	DNI/NIF/NIE/Pasaporte, Nombre y apellidos, Dirección postal o electrónica, Teléfono
Categorías de datos especiales o penales	No existen
Otro tipo de datos	No existen
<b>Categorías de destinatarios</b>	
Cesiones	• Bancos, cajas de ahorro y cajas rurales • Administración tributaria
Transferencias internacionales	No existen

## 4. CONTACTOS

<b>Tratamiento</b>	
Descripción	Comunicación, información y gestión sobre productos y servicios. Incluye contactos web y redes sociales
Finalidades	Publicidad y prospección comercial
Legitimación	• Consentimiento EXPLÍCITO para fines determinados (artículo 6.1.a GDPR)
Origen de los datos	El mismo interesado o su representante legal
Categorías de interesados	Personas de contacto, Clientes y usuarios, Solicitantes
Criterios de conservación	Conservados durante no más tiempo del necesario para mantener el fin del tratamiento o mientras existan prescripciones legales que dictaminen su custodia
Sistema de tratamiento	Parcialmente Automatizado
<b>Categorías de datos</b>	
Datos identificativos	DNI/NIF/NIE/Pasaporte, Nombre y apellidos, Dirección postal o electrónica, Teléfono
Categorías de datos especiales o penales	No existen
Otro tipo de datos	Información comercial
<b>Categorías de destinatarios</b>	
Cesiones	
Transferencias internacionales	No existen

## 5. CURRÍCULUMS

<b>Tratamiento</b>	
Descripción	Gestión de candidatos a empleados
Finalidades	Recursos humanos
Legitimación	• Consentimiento INEQUÍVOCO mediante una clara acción del interesado (artículo 6.1.a GDPR)
Origen de los datos	El mismo interesado o su representante legal
Categorías de interesados	Empleados, Solicitantes
Criterios de conservación	Conservados durante un máximo de 1 año
Sistema de tratamiento	Parcialmente Automatizado
<b>Categorías de datos</b>	
Datos identificativos	DNI/NIF/NIE/Pasaporte, Nombre y apellidos, Dirección postal o electrónica, Teléfono, Imagen, Firma manual
Categorías de datos especiales o penales	No existen
Otro tipo de datos	Características personales, Circunstancias sociales, Académicos y profesionales, Detalles de empleo
<b>Categorías de destinatarios</b>	
Cesiones	
Transferencias internacionales	No existen

## 6. VIDEOVIGILANCIA

<b>Tratamiento</b>	
Descripción	Grabación audiovisual de personas por motivos de seguridad
Finalidades	Videovigilancia
Legitimación	• Por un INTERÉS LEGÍTIMO del Responsable del tratamiento o Tercero (artículo 6.1.f GDPR)
Origen de los datos	El mismo interesado o su representante legal
Categorías de interesados	Empleados, Proveedores, Personas de contacto, Clientes y usuarios
Criterios de conservación	Conservados durante un máximo de 30 días
Sistema de tratamiento	Automatizado
<b>Categorías de datos</b>	
Datos identificativos	Imagen
Categorías de datos especiales o penales	No existen
Otro tipo de datos	Características personales
<b>Categorías de destinatarios</b>	
Cesiones	
Transferencias internacionales	No existen



## 7. REGISTRO JORNADA LABORAL

<b>Tratamiento</b>	
Descripción	Registro horario de la jornada laboral para dar cumplimiento al RDL 8/2019, de medidas urgentes de protección social y de lucha contra la precariedad laboral en la jornada de trabajo
Finalidades	Recursos humanos, Gestión de nóminas
Legitimación	• Por una OBLIGACIÓN LEGAL del Responsable del tratamiento (artículo 6.1.c GDPR)
Origen de los datos	El mismo interesado o su representante legal
Categorías de interesados	Empleados
Criterios de conservación	Conservados durante 4 años para el registro horario de jornada laboral
Sistema de tratamiento	Parcialmente Automatizado
<b>Categorías de datos</b>	
Datos identificativos	DNI/NIF/NIE/Pasaporte, Nombre y apellidos, Identificador de usuario
Categorías de datos especiales o penales	No existen
Otro tipo de datos	No existen
<b>Categorías de destinatarios</b>	
Cesiones	• Interesados legítimos • Organismos de la Seguridad Social
Transferencias internacionales	No existen

## 8. IMÁGENES

<b>Tratamiento</b>	
Descripción	Gestión de audiovisuales para su publicación en los medios de comunicación
Finalidades	Gestión de actividades asociativas, culturales, recreativas, deportivas y sociales
Legitimación	• Consentimiento EXPLÍCITO para fines determinados (artículo 6.1.a GDPR)
Origen de los datos	Fuentes accesibles al público, El mismo interesado o su representante legal
Categorías de interesados	Asociados y miembros, Padres o tutores
Criterios de conservación	Conservados durante no más tiempo del necesario para mantener el fin del tratamiento o mientras existan prescripciones legales que dictaminen su custodia
Sistema de tratamiento	Parcialmente Automatizado
<b>Categorías de datos</b>	
Datos identificativos	Imagen
Categorías de datos especiales o penales	No existen
Otro tipo de datos	No existen
<b>Categorías de destinatarios</b>	
Cesiones	• Organizaciones o personas directamente relacionadas con el responsable
Transferencias internacionales	No existen

## 9. VOLUNTARIOS

<b>Tratamiento</b>	
Descripción	Organización de actividades sociales. Personas, socias o no, que colaboran en la organización de las actividades de la asociación
Finalidades	Recursos humanos
Legitimación	• Consentimiento EXPLÍCITO para fines determinados (artículo 6.1.a GDPR)
Origen de los datos	El mismo interesado o su representante legal
Categorías de interesados	Asociados y miembros, Solicitantes
Criterios de conservación	Conservados durante NO MÁS TIEMPO DEL NECESARIO para alcanzar los fines
Sistema de tratamiento	Parcialmente Automatizado
<b>Categorías de datos</b>	
Datos identificativos	DNI/NIF/NIE/Pasaporte, Nombre y apellidos, Dirección postal o electrónica, Teléfono, Imagen, Firma manual, Núm. de SS o mutualidad
Categorías de datos especiales o penales	No existen
Otro tipo de datos	Características personales, Circunstancias sociales, Académicos y profesionales, Detalles de empleo
<b>Categorías de destinatarios</b>	
Cesiones	
Transferencias internacionales	No existen

## 10. USUARIOS

<b>Tratamiento</b>	
Descripción	Gestión de usuarios de la entidad. Incluye datos relacionados con el usuario (representante legal, familiares, características personales y sociales, etc.)
Finalidades	Gestión de asistencia social, Gestión de actividades asociativas, culturales, recreativas, deportivas y sociales, Gestión contable, fiscal y administrativa
Legitimación	• Consentimiento EXPLÍCITO para fines determinados (artículo 6.1.a GDPR)
Origen de los datos	El mismo interesado o su representante legal
Categorías de interesados	Clientes y usuarios
Criterios de conservación	Conservados durante no más tiempo del necesario para mantener el fin del tratamiento o mientras existan prescripciones legales que dictaminen su custodia
Sistema de tratamiento	Parcialmente Automatizado
<b>Categorías de datos</b>	
Datos identificativos	DNI/NIF/NIE/Pasaporte, Nombre y apellidos, Dirección postal o electrónica, Teléfono, Imagen, Firma manual
Categorías de datos especiales o penales	No existen
Otro tipo de datos	Características personales (personalidad o comportamiento), Características personales, Circunstancias sociales, Académicos y profesionales, Detalles de empleo, Económicos, financieros y de seguro
<b>Categorías de destinatarios</b>	
Cesiones	• Administración pública con competencia en la materia
Transferencias internacionales	No existen

## 11. USUARIOS SALUD

<b>Tratamiento</b>	
Descripción	Gestión administrativa de datos de salud de los usuarios. Incluye el historial clínico y el control sanitario
Finalidades	Historial clínico, Gestión y control sanitario
Legitimación	• Para la ejecución de un CONTRATO o precontrato con el interesado (artículo 6.1.b GDPR)
Origen de los datos	El mismo interesado o su representante legal
Categorías de interesados	Empleados, Asociados y miembros, Pacientes
Criterios de conservación	Conservados durante no más tiempo del necesario para mantener el fin del tratamiento o mientras existan prescripciones legales que dictaminen su custodia
Sistema de tratamiento	Parcialmente Automatizado
<b>Categorías de datos</b>	
Datos identificativos	DNI/NIF/NIE/Pasaporte, Nombre y apellidos, Dirección postal o electrónica, Teléfono, Imagen, Tarjeta sanitaria
Categorías de datos especiales o penales	Salud
Otro tipo de datos	No existen
<b>Categorías de destinatarios</b>	
Cesiones	• Entidades sanitarias
Transferencias internacionales	No existen

## MEDIDAS TÉCNICAS Y ORGANIZATIVAS DE SEGURIDAD

### Locales o delegaciones

SEDE PRINCIPAL	Medidas	Riesgo
<b>Tipo de acceso al local</b>	Entrada libre con control de acceso (personal de recepción, vigilantes, etc.).	Bajo
<b>Sistema general de control de llaves</b>	Las llaves se guardan en un lugar seguro y con acceso autorizado a las mismas	Bajo
<b>Otras medidas de seguridad</b>	NO EXISTEN medidas de seguridad.	Bajo

### Departamentos

OFICINA	Medidas	Riesgo
<b>Permiso:</b>	Limitado a personal autorizado en todo el Departamento.	Bajo
<b>Acceso:</b>	Acceso al Departamento regido por las medidas de seguridad del Local.	Bajo
<b>Control de llaves:</b>	Las llaves se guardan en un lugar seguro y con acceso autorizado a las mismas.	Bajo
<b>Otras medidas de seguridad:</b>	NO EXISTEN otras medidas de seguridad.	Bajo

### Confidencialidad de la información

Información del tratamiento al interesado	Medidas	Riesgo
<b>¿Se informa al interesado de los detalles del tratamiento?</b>	Sí, con cláusulas personalizadas de protección de datos.	Bajo
<b>¿Se informa al interesado de los derechos que le asisten?</b>	Sí, con cláusulas personalizadas de protección de datos.	Bajo
Transporte y transmisión de datos	Medidas	Riesgo
<b>Transporte de los soportes dentro de la empresa</b>	NO SE TRANSPORTAN soportes dentro de la Empresa.	Muy bajo
<b>Transporte de los soportes fuera de la empresa</b>	Por personal autorizado por el Responsable del tratamiento con medidas de seguridad.	Bajo
Procedimientos con datos automatizados (digital)	Medidas	Riesgo
<b>Acceso durante el tratamiento digital (pantallas)</b>	Se tratan impidiendo la visión de los datos a personas no autorizadas.	Bajo
<b>Almacenamiento de los soportes digitales</b>	Se guardan en un Mobiliario y/o Departamento con medidas de seguridad.	Bajo
<b>Destrucción de soportes digitales</b>	Destructora de soportes digitales.	Bajo
Procedimientos con datos no automatizados (documentos)	Medidas	Riesgo
<b>Acceso durante el tratamiento manual (documentos)</b>	Se tratan impidiendo el acceso a los datos a personas no autorizadas.	Bajo

<b>Almacenamiento de documentos</b>	Se guardan en un Mobiliario y/o Departamento con medidas de seguridad.	Bajo
<b>Destrucción de documentos</b>	Destructor de papel.	Bajo
Otras medidas de seguridad	Medidas	Riesgo
<b>¿Se lleva un registro de accesos a categorías especiales de datos?</b>	Sí, mediante una aplicación informática.	Bajo

### Sistemas de información

Acceso a equipos informáticos	Medidas	Riesgo
<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	Muy bajo
Acceso a redes informáticas	Medidas	Riesgo
<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	Medidas	Riesgo
<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>	La contraseña se compone al menos de 8 caracteres, con algún número, mayúscula, minúscula y símbolo o carácter especial	Bajo
<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	Medidas	Riesgo
<b>Ubicación de las copias</b>	Se guardan en un Hardware 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>	Como máximo, 6 meses desde la creación.	Bajo
<b>Método de comprobación de datos</b>	Aplicación informática de verificación de copias.	Bajo
Copias de respaldo externas	Medidas	Riesgo
<b>Ubicación de las copias externas</b>	Local o departamento distinto de donde se creó.	Bajo

<b>Periodicidad de programación de las copias externas</b>	Semanalmente, como mínimo.	Bajo
<b>Cifrado de los datos de las copias externas</b>	Sí.	Bajo
Disponibilidad de los datos	Medidas	Riesgo
<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 firewall, antivirus, antispam, antiphishing, antimalware, antiransomware, etc.	Bajo
<b>Disponibilidad de los servicios de información</b>	EXISTEN medidas para garantizar la disponibilidad de los datos	Bajo
<b>Restauración de los servicios de información</b>	EXISTEN medidas para restaurar rápidamente la disponibilidad y el acceso a los datos	Bajo
<b>Resiliencia de los servicios de información</b>	EXISTEN medidas para anticiparse y adaptarse a cambios imprevistos en los servicios de información	Bajo
<b>Procesos de verificación, evaluación y valoración de las medidas de seguridad</b>	SE HAN ESTABLECIDO procesos para verificar, evaluar y valorar la eficacia de las medidas de seguridad	Bajo

### Tratamientos específicos

Tratamientos específicos	Medidas	Riesgo
<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 OCASIONALMENTE de personas en situación de vulnerabilidad	Bajo
<b>Tratamiento de datos que puede invadir la intimidad de las personas</b>	Se tratan datos OCASIONALMENTE que pueden invadir la intimidad de las personas	Bajo
<b>Vulneración de los derechos y libertades fundamentales</b>	NO SE REALIZAN tratamientos que vulneren los derechos o libertades fundamentales	Muy bajo

### Internet

Comunicaciones electrónicas	Medidas	Riesgo
<b>Correo electrónico</b>	SE UTILIZA correo electrónico seguro mediante cifrado punto a punto.	Muy bajo
<b>Cláusula de protección de datos</b>	SE HA PUBLICADO una cláusula de protección de datos con información adecuada del tratamiento.	Muy bajo

### Organización

Organización	Medidas	Riesgo
<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 y su protección desde el DISEÑO Y POR DEFECTO	Bajo



<b>Formación en protección de datos</b>	[Se facilita suficiente formación al personal autorizado para tratar datos] mediante la entrega de la política de seguridad	Bajo
<b>Violaciones de la seguridad</b>	EXISTE un protocolo documentado para gestionar y registrar las violaciones de la seguridad	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
<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