RESPONSABILIDAD ACTIVA - RGPD

EVALUACIÓN PRESTADORES DE SERVICIOS CON ACCESO A DATOS

En cumplimento del principio de responsabilidad activa y diligencia en la elección de proveedores con acceso a datos de carácter personal (encargados del tratamiento) establecido en 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 – Reglamento General de Protección de Datos (RGPD), Enaire precisa conocer su grado de adaptación a esta normativa.

Así mismo, Enaire se reserva el derecho de poder solicitar información complementaria para acreditar el cumplimiento de las exigencias establecidas en el RGPD.

Por ello, le rogamos que cumplimente el siguiente cuestionario y lo envíe ucpd@enaire.es, antes del (_ _/ _ _ /_ _ _ _).

Si alguna de las preguntas realizas en el cuestionario no es de aplicación según los servicios prestados por su entidad especifique: "No aplica".

1. Datos de contacto

1.1 Identificación del prestador de servicios (Encargado del Tratamiento)

Denominación social, nombre(s) comercial(es), CIF y domicilio social del prestador de servicios:

1.2 Datos de contacto (Interlocutor y/Delegado de Protección de Datos)

Nombre, apellidos, número de teléfono y dirección de correo electrónico de la persona designada por el prestador de servicios para la resolución de las consultas y/o cuestiones en materia de protección de datos y/o del Delegado de Protección de Datos (indicar si la persona de contacto ha sido designada formalmente como DPD o no). En caso de ser dos personas diferentes, indicar los datos de ambos.

2. SITUACIÓN ACTUAL DE REGULACIÓN

2.1 Nivel de Cumplimiento Actual

Indique si actualmente existe un contrato entre Enaire y su entidad en el que se regule el tratamiento de datos personales realizado por el Encargado en la prestación de servicios.

En caso afirmativo, indique si el citado contrato está adecuado a las nuevas exigencias del RGPD.

3. INFORMACIÓN SOBRE EL TRATAMIENTO DE DATOS EN LOS SERVICIOS PRESTADOS

3.1 Servicios Prestados

Exponga los siguientes aspectos:

a) Servicios prestados por el Encargado a Enaire (breve descripción y referencia al contrato/s):

b) Categorías de datos personales a los que tiene acceso para realizar la prestación de servicios:

3.2 Localización y ubicación de los tratamientos de datos

Indique la totalidad de las ubicaciones en las que realizará tratamiento (incluyendo almacenamiento y conservación) de datos para la prestación de servicios a Enaire:

3.3 Subcontratistas/subencargados del Encargado del Tratamiento

Indique todos los subcontratistas (incluyendo prestadores de servicios, otras empresas del grupo, etc…) que intervendrán en la prestación del servicio a Enaire:

4. ACTUACIONES DE ADECUACIÓN AL RGPD REALIZADAS POR EL PRESTADOR DE SERVICIOS

4.1 Modificación en los servicios prestados

Indicar si el RGPD exige modificaciones en los servicios prestados o en el tratamiento de datos por parte de su entidad como encargado del tratamiento de Enaire. En caso afirmativo, indique y justifique las modificaciones requeridas.

4.2 Nombramiento del DPD

Señale si es obligatorio el nombramiento de DPD en su entidad. Si fuera necesario, indicar si se ha nombrado o el plazo en el cual se procederá a su nombramiento.

4.3 Principio de responsabilidad Proactiva

Detallar las acciones llevadas a cabo por el prestador de servicios para el cumplimiento del principio de Responsabilidad Proactiva del RGPD.

4.4 Políticas y procedimientos de cumplimiento RGPD

Describa brevemente las políticas aplicadas y planes de actuación para dar cumplimiento al RGPD. En el supuesto de que las mismas no estén implantadas, indique el plazo o fecha en que serán efectivas y el medio por el cual se comunicarán a Enaire.

4.5 Códigos de conducta y certificados de privacidad

Especifique los códigos de conducta o certificados de privacidad o seguridad (Certificación ENS, ISO 27001, ISO 22001, etc.) con los que cuenta su entidad, se encuentra adherido o en proceso de obtención.

4.6 Planes formativos

Indique los planes formativos en materia de protección de datos y seguridad para empleados o cualquier otro miembro de su entidad involucrado en la prestación de los servicios a Enaire. Especificar los siguientes aspectos:

- Frecuencia con la que se revisan los citados planes de formación;
- Asiduidad con la que se imparte formación;
- Si existe documentación y/o reportes que acrediten la realización de esta formación.

4.7 Subcontratistas

Indique todos los subcontratistas (incluyendo prestadores de servicios, empresas del grupo, ...) que intervendrán en la prestación del servicio a Enaire. Indique si existe contrato firmado acorde al Reglamento Europeo de Protección de Datos (RGPD) con estos subcontratistas/subencargados.

5. RELACIONES CON ENAIRE

5.1 Sistemas/ aplicativos utilizados

Indicar los sistemas y/o aplicativos utilizados para la prestación del servicio a Enaire:

5.2 Colaboración con Enaire

Indicar los procedimientos o medidas que aplica o prevé aplicar con el fin de garantizar que en la prestación de los servicios Enaire cumple con el RGPD. Concretamente, exponga los procesos o medidas concernientes a:

- Principio de privacidad por diseño y por defecto.
- Procedimientos para el efectivo ejercicio de los derechos de las personas afectadas.
- Transparencia del tratamiento (deber de informar).

5.3 Notificación de brechas de seguridad (violaciones de seguridad)

Indicar los procedimientos de notificación de brechas de seguridad en la entidad de acuerdo con lo previsto en el RGPD, incluyendo, entre ellos, la comunicación a Enaire:

5.4 Medidas de seguridad

Indique si se han implementado las siguientes medidas de seguridad en los sistemas:

MEDIDA	COMENTARIOS
CONTROL DE ACCESOS FÍSICO AL CPD (describir)	
MEDIDAS DE PROTECCIÓN FÍSICA EN CPD (describir)	
GESTIÓN DE SOPORTES (inventario actualizado de soportes)	
GESTIÓN DE SOPORTES (cifrado de soportes, borrado seguro de soportes,...)	
CONTROL DE ACCESOS LÓGICOS A SISTEMA OPERATIVO Y APLICACIONES (Administradores y usuarios, segregación de funciones)	
CONTROL DE ACCESOS LÓGICOS A SISTEMAS OPERATIVOS Y APLICACIONES (Políticas de contraseñas)	
REGISTROS DE ACCESOS A APLICACIONES Y BASES DE DATOS	
COPIA DE SEGURIDAD (frecuencia y ubicación de las copias)	
PROCEDIMIENTO DE CONTINUIDAD DE NEGOCIO	
GESTIÓN DE INCIDENCIAS (registro y notificación de brechas de seguridad)	
COMUNICACIONES CIFRADAS	

MEDIDA	COMENTARIOS
AUDITORÍA TÉCNICA DE SISTEMAS Y PENTESTING	
GESTIÓN DE VULNERABILIDADES DE SISTEMAS Y APLICACIONES	
CIFRADO EN EQUIPOS Y DISPOSITIVOS MÓVILES	
SEGURIDAD EN ENTORNOS DE DESARROLLO Y TEST	
PSEUDOANONIMIZACIÓN / ANONIMIZACIÓN DE DATOS PERSONALES	
OTRAS MEDIDAS DE SEGURIDAD	

6. Observaciones

Observaciones o comentarios

En , a de mayo de 2018

D. /Dña.

Firmado