ANEXO VII – EVALUACIÓN DE PRESTADORES DE SERVICIOS CON ACCESO A DATOS

**(A cumplimentar exclusivamente por la empresa adjudicataria. Su representante, lo cumplimentará, fechará, firmará y remitirá a** [**ucpd@enaire.es**](mailto:ucpd@enaire.es)**. En el campo asunto del correo debe hacerse constar lo siguiente: EET/NUM EXPTE/NOMBRE EXPTE.)**

RESPONSABILIDAD ACTIVA

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), así como en la DA1ª de la LO 3/2018, de 5 de diciembre, ENAIRE precisa conocer su grado de adaptación a esta normativa.

ENAIRE se reserva el derecho de solicitar la información complementaria que acredite el cumplimiento de las obligaciones establecidas por el RGPD así como la documentación que estime pertinente.

Le rogamos cumplimente este cuestionario y lo envíe fechado y firmado, urgentemente, a ucpd@enaire.es.

Si alguna de las preguntas realizas en el cuestionario no es de aplicación según los servicios prestados debe consignar: “No aplica”.

Por último, facilite mediante Anexo cualquier información o documento relevante en términos de cumplimiento normativo.

1. Identificación de la empresa prestadora de servicios
   1. Razón social / nombre:
   2. NIF
   3. Dirección
   4. Persona de contacto
2. Relación con ENAIRE
   1. Indique la referencia del contrato existente en entre su empresa y ENAIRE
   2. Describa brevemente los servicios que presta su empresa a ENAIRE:
3. Tratamiento de datos personales
   1. ¿Para la ejecución del contrato su empresa procede al tratamiento de datos de carácter personal cuya responsabilidad corresponde a ENAIRE actuando como Encargado del Tratamiento?

Sí  No

**SI HA CONTESTADO NEGATIVAMENTE NO ES NECESARIO QUE SIGA RESPONDIENDO EL CUESTIONARIO. GUÁRDELO Y REMÍTALO FIRMADO A ENAIRE A TRAVÉS DEL CORREO-E: UCPD@ENAIRE.ES**

* 1. ¿Cómo se regula el tratamiento de datos de carácter personal entre su entidad y ENAIRE?

Cláusula en Pliego de Contratación  Contrato de Encargado del Tratamiento

* 1. Descripción de la tipología de datos personales tratados para la prestación del servicio (nombre y apellidos, NIF, dirección, datos ecónomicos, etc.):
  2. ¿Se tratan categorías especiales de datos (salud, afiliación sindical, datos biométricos, etc.) en la prestación del servicio?

1. Política de seguridad y de protección de datos personales
   1. ¿Dispone su empresa de una Política de Seguridad y de Protección de Datos (Privacidad) adaptada a la legislación vigente?  Sí  No

En caso negativo, le rogamos facilite detalles sobre otros procedimientos internos de su organización para la protección de los datos personales:

* 1. ¿Su empresa informa y facilita a sus empleados los procedimientos y políticas internas de protección de datos, así como sus actualizaciones y les requiere la confirmación de su cumplimiento?

Sí  No

En caso negativo, le rogamos facilite explicación del motivo:

* 1. ¿Se han establecido planes formativos en materia de protección de datos y seguridad en su empresa para empleados o cualquier otro miembro involucrado en la prestación de los servicios a ENAIRE??

Sí  No

Si ha contestado, afirmativamente, especifique 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.
  1. ¿Cuándo y por quién han sido revisados por última vez los procedimientos internos de protección de datos?
  2. ¿Dispone su empresa de certificaciones en materia de seguridad (ISO-27001, ENS, etc.)?

Sí  No

En caso afirmativo, indique cuales:

* 1. ¿El ET cumple con la normativa vigente de protección de datos?

Sí  No

* 1. ¿El ET ha elaborado e implantado un programa de cumplimiento de protección de datos y seguridad de la información?

Sí  No

* 1. ¿El ET posee la documentación necesaria para evidenciar el cumplimiento de este   apartado?

Sí  No

* 1. ¿Existe un proceso de verificación, evaluación y valoración regular de la eficacia de estas medidas técnicas y organizativas para garantizar la seguridad del tratamiento?

Sí  No

* 1. ¿El ET está adherido a algún Código de Conducta en materia de protección de datos o está certificado en alguna norma internacional?

Sí  No

* 1. ¿El ET se somete a auditorías periódicas de protección de datos?

Sí  No

1. Subcontratación de servicios y tratamientos fuera del Espacio Económico Europeo (EEE)
   1. ¿Existen subcontratistas/subencargados (incluyendo prestadores de servicios, otras empresas del grupo, etc…) que intervendrán en la prestación del servicio contratado con ENAIRE?:

Sí  No

En caso afirmativo, indique los subcontratistas/encargados y tratamientos de datos realizados en cada caso:

En caso afirmativo, Indique si existe contrato firmado acorde al Reglamento Europeo de Protección de Datos (RGPD) con estos subcontratistas/subencargados.

Sí  No

Observaciones:

* 1. ¿Se tratan los datos personales de los cuales es responsable ENAIRE fuera del Espacio Económico Europeo?  Sí  No

En caso afirmativo, indique el país, la tipología de datos tratados, los motivos por los cuales se tratan fuera del EEE y las garantías de seguridad en dichos tratamientos:

1. Delegado de protección de datos
   1. Señale si es obligatorio el nombramiento de DPD en su empresa.

Sí  No

Si ha contestado afirmativamente, indique si se ha nombrado (identificación y canal de comunicación) o el plazo en el cual se procederá a su nombramiento.

* 1. En caso afirmativo, indicar datos de contacto del mismo (teléfono y e-mail):..…………………………..
  2. A la hora de nombrar al DPO, ¿ha tenido en cuenta sus cualificaciones profesionales y sus conocimientos?

Sí  No

* 1. El ET permite al DPO actuar con independencia y le proporciona los recursos necesarios para realizar sus funciones de acuerdo al RGPD?

Sí  No

* 1. ¿El ET posee la documentación necesaria para evidenciar el cumplimiento de este apartado?

Sí  No

1. Análisis de riesgos
   1. ¿Se ha procedido a la realización de un análisis de riesgos en su empresa con el fin de establecer medidas de seguridad y control para garantizar la seguridad de los datos personales tratados en la prestación de los servicios a ENAIRE?  Sí  No

Si ha contestado afirmativamente, indique cuando ha sido realizado/revisado el análisis de riesgos por última vez:

1. Notificación de brechas de seguridad (violaciones de seguridad)
   1. ¿Se ha establecido un procedimiento de notificación de brechas de seguridad en su empresa de acuerdo con lo previsto en el RGPD, incluyendo la comunicación a ENAIRE?

Sí  No

En caso afirmativo, indique los plazos y los medios por los cuales va a comunicar las brechas de seguridad a ENAIRE:

1. Medidas de seguridad

Medidas de seguridad que afectan a los sistemas de información de su empresa en los cuales se tratan los datos personales relacionados con la prestación de servicios a ENAIRE.

**Protección de sistemas**

* 1. ¿Disponen los sistemas de su empresa en los que se tratan los datos personales cuya responsabilidad corresponde a ENAIRE de medidas de protección ante software malicioso (virus, ransomware, spyware, etc.)?  Sí  No

Si ha contactado afirmativamente, indique las medidas aplicadas:

* 1. ¿Dispone de un programa de evaluación de vulnerabilidades proactivo que monitoriza las brechas y asegura un tiempo de actualización de los parches de seguridad críticos, vulnerabilidades conocidas?

Sí 🗆 No

* 1. ¿Su empresa dispone de sistemas de protección con el fin de evitar accesos no autorizados o daños a sus sistemas informáticos, redes, o sistemas de almacenamiento de datos e información (IPS, Cortafuegos, NGFW, anti-DDoS, etc.)?  Sí  No
  2. ¿Dispone su empresa de sistemas para la monitorización de sus redes y sistemas informáticos para la detección de violaciones de seguridad?  Sí  No

**Dispositivos portátiles**

* 1. ¿Se utilizan dispositivos portátiles o soportes móviles para el tratamiento de datos en la prestación de los servicios a ENAIRE?  Sí  No

Si ha contestado afirmativamente conteste las siguientes preguntas:

¿Se adoptan medidas en dichos dispositivos portátiles para evitar accesos no autorizados?

Sí  No

Si ha contestado afirmativamente, indique las medidas adoptadas:

**Continuidad**

* 1. ¿Se han establecido en su empresa procedimientos y mecanismos que garanticen la realización de copias de seguridad de los datos personales?

Sí  No

Si ha contestado afirmativamente, indique si dispone de copias de los datos en una segunda ubicación:

Sí  No

* 1. ¿Dispone su empresa de un plan de continuidad del negocio (BCP) y plan de recuperación ante desastres (DRP) de trabajo para evitar la interrupción de los servicios a causa de problemas informáticos o acelerar su recuperación?

Sí  No

**Confidencialidad**

* 1. ¿El ET aplica medidas adecuadas para evitar que personas no autorizadas accedan a datos personales o a los sistemas y equipos que almacenan y procesan datos personales?

Sí  No

* 1. ¿El ET controla el acceso del personal a áreas restringidas (por ejemplo, a través de tarjetas magnéticas, control biométrico, códigos de acceso, llaves entregadas sólo al personal autorizado, alarmas, etc.)?

Sí  No

* 1. ¿Se conceden a los usuarios los mínimos permisos en el acceso (lectura, modificación, borrado) en función de las necesidades de su puesto?

Sí  No

* 1. ¿El ET dispone de procedimientos de seudonimización de la información?

Sí  No

* 1. ¿Se revisa periódicamente la correcta implantación y la eficacia de estas medidas?

Sí  No

**Trazabilidad**

* 1. ¿Dispone su empresa de mecanismos destinados a identificar los accesos realizados a las aplicaciones y bases de datos en las que se tratan datos personales para la prestación de los servicios a ENAIRE?

Sí  No

* 1. ¿El acceso a los datos personales queda registrado de forma que permita identificar al usuario que ha accedido, la fecha del acceso, a qué ha accedido y qué acciones ha realizado?

Sí  No

**Seguridad física**

* 1. ¿Se han establecido en su empresa controles físicos de seguridad para la detección y detención de accesos no autorizados a los sistemas informáticos y centro de proceso de datos (CPD)?

Sí  No

Si ha contestado afirmativamente, describa las medidas implantadas:

**Auditoría Técnica de Sistemas**

* 1. ¿Se realizan auditorías técnicas de los sistemas y Pentesting de los sistemas que tratan los datos personales relacionados con la prestación de servicios a ENAIRE?  Sí  No

**Otras medidas de seguridad**

* 1. Si lo considera necesario indique otras medidas de seguridad que son aplicadas en el tratamiento de los datos personales de ENAIRE en la prestación del servicio:

1. Observaciones

Observaciones o comentarios

Declaro que la información facilitada a través del presente, así como la información facilitada a través de la documentación adjunta, es verdadera y que no se ha omitido ningún dato o información relevante en el ámbito de la normativa de protección de datos.

En \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, a \_\_de \_\_\_\_\_\_ de 20\_\_

D. /Dña.

Firmado