Norma de Seguridad: Cláusulas LOPD con acceso a datos, de los que la Diputación Foral de Bizkaia es encargada de tratamiento

1. OBJETO	2. ALCANCE
Cumplimiento del artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, y el artículo 21 del Real Decreto 1720/2007 (LOPD).	Todos los proyectos y servicios prestados por terceras partes que tengan acceso a datos de carácter personal de los que la Diputación Foral de Bizkaia sea encargada de tratamiento. Es decir, cuando un tercero contratado por la Diputación Foral de Bizkaia vaya a acceder a datos de los que la Diputación no sea la propietaria pero sin embargo gestione en sus sistemas (por ejemplo, datos de Gobierno Vasco).

3. DESARROLLO

I. La Diputación Foral de Bizkaia actúa como encargada de tratamiento de los datos de carácter personal propiedad de múltiples organismos (Responsables de Fichero), conforme a la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante LOPD).

II. Dichos ficheros, se encuentran declarados ante el Registro General de la Agencia de Protección de Datos, por cada uno de los organismos con los que la Diputación Foral de Bizkaia colabora.

Todo lo que se estipula a continuación se circunscribe a los datos de carácter personal contenidos que el adjudicatario pudiera tratar con motivo de la prestación del servicio contratado.

III. El adjudicatario, como parte del contrato, se convierte desde su perfección en encargado de tratamiento conforme al Artículo 12 de la LOPD, y el 21c del RD1720/2007. A los efectos de comunicación a la Agencia de Protección de Datos, el adjudicatario consiente en figurar como encargado de tratamiento en cuantos ficheros sean objeto del contrato.

IV. El adjudicatario, no podrá utilizar dichos datos para otro fin distinto del indicado en los acuerdos adoptados en el contrato.

V. El adjudicatario se compromete a tratar los datos conforme a las instrucciones que le marque el Responsable de Fichero.

VI. El adjudicatario en ningún caso comunicará, mostrará, cederá ni revelará datos, ni siquiera para su conservación, a terceras personas ajenas a la relación contractual que se establece en el contrato, salvo requerimiento judicial específico.

VII. Se prohíbe expresamente la subcontratación de terceros para el tratamiento de datos personales en todo o en parte del servicio objeto de contratación, salvo que se cumplan los siguientes requisitos:

a. Que dicho tratamiento se haya especificado en el contrato firmado por la Diputación Foral de Bizkaia y el adjudicatario.

b. Que el tratamiento de datos de carácter personal se ajuste a las instrucciones del Responsable del Fichero.

c. Que el adjudicatario y el tercero formalicen el contrato en los términos previstos en el artículo 12.2 de la Ley Orgánica 15/1999, de 13 de diciembre.

En estos casos, el tercero tendrá también la consideración de encargado del tratamiento.

VIII. El adjudicatario se compromete a cumplir todo lo dispuesto en la legislación vigente sobre protección de datos que le sea de aplicación. Así, todo dato que conozca cualquiera de sus subordinados, como consecuencia de la realización del presente contrato, debe mantenerse en la más estricta confidencialidad, no pudiendo comunicarse a terceros ni emplearse en uso propio, respondiendo de los posibles perjuicios que se pudieran derivar para el Responsable de Fichero, la Diputación Foral de Bizkaia y para los afectados.

IX. El adjudicatario certifica que el personal a su cargo ha firmado una cláusula de confidencialidad por la que se compromete a no revelar la información que pudiera conocer en función de su cargo o cometido durante la prestación del contrato y posteriormente al mismo.

X. En el supuesto de que el adjudicatario haya sido autorizado a mantener algún dato proveniente del contrato, se obliga a devolverlo a la Diputación Foral de Bizkaia una vez cumplida la prestación contractual. En caso de que exista legislación que ampare al mantenimiento de los datos, estos deberán mantenerse debidamente bloqueados en tanto pudieran derivarse posibles responsabilidades jurídicas.

XI. El adjudicatario quedará sujeto al régimen de responsabilidad que instaura la normativa de protección de datos y responderá personalmente siempre que destine los datos a una finalidad diferente a la estipulada en el presente contrato, los comunique a terceros, o los utilice incumpliendo alguna de las cláusulas del contrato.

XII. El adjudicatario deberá implantar las medidas de seguridad precisas de tipo técnico y organizativo que, en función del nivel de protección correspondiente a los datos de carácter personal a los que tenga acceso durante la prestación de los servicios, impone la normativa vigente de protección de datos. Las medidas mínimas de seguridad obligatorias para este contrato se contienen en el Anexo I.

XIII. En caso de que el adjudicatario preste sus servicios en locales propios, ajenos a los del responsable de tratamiento, se deberá reflejar dicha circunstancia en su propio documento de seguridad, indicando el fichero o tratamiento y el responsable del mismo, así como las medidas de seguridad a implantar en relación con dicho tratamiento.

XIV. El Responsable del Fichero, o la Diputación Foral de Bizkaia podrán, si lo estiman conveniente, solicitar bienalmente el informe de auditoría de

protección de datos. En dicho informe se desglosarán los servicios contratados y el grado de cumplimiento conforme a la Ley Orgánica 15/1999 de Protección de datos Personales y de su reglamento de desarrollo. La auditoría será realizada por expertos independientes, aceptados previamente por la Diputación Foral de Bizkaia y el adjudicatario.

XV. El adjudicatario se compromete a implantar las aplicaciones y sistemas de Información de forma que sea posible la realización de auditorías periódicas de protección de datos.

XVI. Serán motivos de resolución del presente contrato la vulneración del deber de secreto por el adjudicatario o su personal, así como el incumplimiento de la normativa sobre protección de datos de carácter personal.

ANEXO I - MEDIDAS DE SEGURIDAD

Las medidas de seguridad que el adjudicatario deberá implantar son las siguientes:

- Medidas para datos de nivel **BÁSICO**: Se deberán aplicar las medidas de los párrafos 1 al 20.
- Medidas para datos de nivel **MEDIO**: Se deberán aplicar las medidas de los párrafos 1 al 27.
- Medidas para datos de nivel **ALTO**: Se deberán aplicar las medidas de los párrafos 1 al 33.

La clasificación de los datos, se realizará en base al artículo 81 del RD 1720/2007, que a modo de resumen, indica lo siguiente:

- Nivel básico: Todos los ficheros o tratamientos de datos de carácter personal deberán adoptar las medidas de seguridad calificadas de nivel básico.
- Nivel medio: Cumplirán con todas las medidas de nivel básico y además las de este nivel los siguientes ficheros o tratamientos de datos:
    - Relativos a comisión de infracción administrativas o penales
    - Relativos a la prestación de servicios de información sobre solvencia patrimonial.
    - Aquellos de los que sean responsables Administraciones Tributarias y se relacionen con el ejercicio de sus potestades tributarias.
    - Aquellos que contengan un conjunto de datos de carácter personal que ofrezcan una definición de las características o de la personalidad de los ciudadanos y que permitan evaluar

determinados aspectos de la personalidad o del comportamiento de los mismos.

- Otros datos de los que sean responsables las entidades financieras, las entidades gestoras de y servicios comunes de la seguridad social, las mutuas de accidentes de trabajo y enfermedades profesionales de la seguridad social para el ejercicio de sus competencias.

- Nivel alto: Además de las medidas de nivel básico y medio, habrá que aplicar estas medidas cuando:
  - Se refieran a datos de ideología, afiliación sindical, religión, creencias, origen racial, salud, o vida sexual.
  - Los que contengan o se refieran a datos recabados para fines policiales sin el consentimiento de las personas afectadas.
  - Aquellos que contengan datos derivados de actos de violencia de género.

En caso de duda, póngase en contacto con el Comité de Seguridad LOPD de la Diputación Foral de Bizkaia.

MEDIDAS DE NIVEL BÁSICO

- **Acceso a través de redes de comunicaciones.**

  1. El adjudicatario se compromete a que las medidas de seguridad exigibles a los accesos a datos de carácter personal a través de redes de comunicaciones garantizarán un nivel de seguridad equivalente al correspondiente a los accesos en modo local.

- **Régimen de trabajo fuera de los locales de ubicación del fichero**

  2. La ejecución de tratamientos de datos de carácter personal fuera de los locales de la ubicación del fichero es autorizada expresamente por el responsable del fichero. El adjudicatario se compromete a garantizar el nivel de seguridad correspondiente al tipo de fichero tratado fuera de los locales. Esta autorización abarca las ejecuciones de tratamientos fuera de la ubicación del fichero en los siguientes supuestos:

     1. Para albergar copias de seguridad
     2. Recuperaciones de datos
     3. Contingencias
     4. Simulacros de planes de contingencias
     5. Mantenimientos de equipos.

- **Ficheros temporales.**

  3. El adjudicatario se compromete a que los ficheros temporales cumplirán el nivel de seguridad que les corresponda dependiendo de la naturaleza de los datos de carácter personal manifestados por el Responsable del Fichero.

4. El adjudicatario se compromete a borrar todo fichero temporal una vez que haya dejado de ser necesario para los fines que motivaron su creación.

- **Registro de Incidencias.**

5. El adjudicatario dispondrá de un procedimiento de notificación y gestión de incidencias, el cual contendrá necesariamente un registro en el que se haga constar el fichero de datos personales implicado, el tipo de incidencia, el momento en que se ha producido, la persona que realiza la notificación, a quién se le comunica, los efectos que se hubieran derivado de la misma y las medidas correctoras aplicadas.

6. El adjudicatario considerará como incidencia de seguridad las recuperaciones de datos y, por tanto, las consigna indicando la persona que ejecutó el proceso, los datos restaurados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación.

- **Identificación y autenticación.**

7. El adjudicatario establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado.

8. Cuando el mecanismo de autenticación se base en la existencia de contraseñas, el adjudicatario dispondrá de una herramienta de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad.

9. El adjudicatario se compromete a que los mecanismos que controlan las contraseñas obligarán al usuario a cambiarlas con la periodicidad no superior a 1 año y mientras estén vigentes se almacenarán de forma ininteligible.

- **Control de acceso**

10. Los usuarios del adjudicatario tendrán acceso autorizado únicamente a aquellas aplicaciones con el perfil que precisen para el desarrollo de sus funciones, tal y como se establece en la descripción del servicio de administración de usuarios.
11. El adjudicatario establecerá mecanismos para evitar que un usuario pueda acceder a aplicaciones con derechos distintos de los autorizados.
12. Exclusivamente usuarios autorizados podrán conceder, alterar o anular el acceso autorizado sobre las aplicaciones.

- **Gestión de Soportes**

13. El adjudicatario se compromete a disponer de un catálogo con el inventario de los soportes informáticos que contengan datos de carácter personal, identificando el tipo de información que contienen, y a almacenarlos en un lugar de acceso restringido al personal autorizado.
14. La salida de soportes informáticos que contengan datos de carácter personal, fuera de los locales en los que esté ubicado el fichero, únicamente podrá ser autorizada por el responsable del fichero.
15. El adjudicatario se compromete a que cuando el soporte vaya a ser desechado o reutilizado, se adoptarán las medidas necesarias para impedir cualquier recuperación posterior de la información almacenada en él.
16. El adjudicatario se compromete a que cuando los soportes vayan a salir fuera de los locales en que se encuentran ubicados los ficheros, se adoptarán las medidas necesarias para impedir cualquier recuperación indebida de la información almacenada en ellos.

- **Copias de Respaldo y Recuperación.**

17. El adjudicatario se compromete a que los procedimientos establecidos para la realización de copias de respaldo y para la recuperación de los datos garantizarán su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción, tal y como se indica en el correspondiente manual de explotación.

18. El adjudicatario se compromete a realizar copias de respaldo, al menos semanalmente, salvo que en dicho periodo no se hubiera producido ninguna actualización de los datos.

- **Pruebas con datos reales**

19. El adjudicatario se compromete a que las pruebas anteriores a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tipo de fichero tratado, aplicando medidas de seguridad equivalentes a las que se aplican al fichero original y realizando previamente una copia de seguridad.

- **Ficheros en soporte no automatizado**

20. El adjudicatario deberá implantar las siguientes medidas específicas para el tratamiento de ficheros en soporte no automatizado que contengan datos de carácter personal:

    - Establecerá los criterios y procedimientos de archivo de soportes y documentos con el fin de garantizar la correcta conservación, localización y consulta y de ejercicio de los derechos de oposición, acceso, rectificación y cancelación. En todo caso, se atenderá a los criterios dispuestos en la norma sectorial que le sea aplicable.

- Los dispositivos de almacenamiento de los documentos que contengan datos de carácter personal deberán disponer de mecanismos que obstaculicen su apertura y en cualquier caso, se adoptarán medidas que impidan el acceso de personas no autorizadas.
- Implantar medidas con el objetivo de que durante los procesos de revisión o tramitación de la documentación se impida el acceso a personas no autorizadas.

MEDIDAS DE NIVEL MEDIO

- **Responsable de Seguridad**

21. El adjudicatario se compromete a designar uno o varios responsables de seguridad que se encargarán de coordinar y controlar la efectiva aplicación de las medidas de seguridad aplicables al tratamiento de datos de carácter personal.

- **Auditoría**

22. El adjudicatario se compromete a que los sistemas de información e instalaciones de tratamiento de datos se someterán a una auditoría que verifique el cumplimiento del reglamento, de los procedimientos e instrucciones vigentes en materia de seguridad de datos, al menos, cada dos años. Se excluye del ámbito de la auditoría los sistemas de información propiedad del Responsable del Fichero.

23. El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles al **Título VIII del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal**, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias. Deberá,

igualmente, incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y recomendaciones propuestas.

24. Los informes de auditoría serán analizados por el responsable de seguridad competente, que elevará las conclusiones al responsable del fichero para que adopte las medidas correctoras adecuadas y quedarán a disposición de la Agencia de Protección de Datos.

- **Identificación y autenticación.**

25. El adjudicatario limitará la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información a un máximo de 5.

- **Gestión de soportes.**

26. El adjudicatario establecerá un sistema de registro de entrada de soportes que permita, directa o indirectamente, conocer el tipo de soporte, la fecha y hora, el emisor, el número de soportes, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción que deberá estar debidamente autorizada.

27. El adjudicatario establecerá un sistema de registro de salida de soportes que permita, directa o indirectamente, conocer el tipo de soporte, la fecha y hora, el destinatario, el número de soportes, el tipo de información que contienen, la forma de envío y la persona responsable de la entrega que deberá estar debidamente autorizada.

MEDIDAS DE NIVEL ALTO

- **Distribución de soportes**

28. El adjudicatario se compromete a que la distribución de los soportes que contengan datos de carácter personal se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que dicha información no sea inteligible ni manipulada durante su transporte.

- **Registro de accesos**

29. El adjudicatario dispondrá de un mecanismo que de cada intento de acceso a los ficheros de datos de nivel alto:

    - Guardará como mínimo, la identificación del usuario, la fecha y hora en que se realizó el acceso, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado.
    - En el caso de que el acceso hubiera sido autorizado, se guardará la información que permita identificar el registro accedido.
    - Los mecanismos que permitan el registro de los datos de acceso estarán bajo el control directo del personal competente del adjudicatario sin que se deba permitir, en ningún caso, la desactivación de los mismos.
    - El periodo mínimo de conservación de los datos registrados es de dos años.

- **Copias de Respaldo y Recuperación**

30. El adjudicatario conservará una copia respaldo y de los procedimientos de recuperación de los datos en un lugar diferente de aquél en que se encuentren los equipos informáticos que los tratan cumpliendo, en todo caso, las medidas de seguridad exigidas.

- **Telecomunicaciones**

31. El adjudicatario se compromete a que la transmisión de datos de carácter personal a través de redes públicas o redes inalámbricas de telecomunicaciones la realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

- **Cifrado**

  32. El adjudicatario asegura que los datos que proporcionan la calificación de Nivel Alto al fichero permanecerán cifrados en los soportes y equipos informáticos que los contengan.

- **Tratamientos en soporte no automatizado**

  33. El adjudicatario deberá implantar los siguientes procedimientos y medidas ante el tratamiento de ficheros no automatizados de nivel alto:

  - Los armarios, archivadores u otros elementos en los que se almacenen los ficheros no automatizados con datos de carácter personal deberán encontrarse en áreas con acceso protegido mediante puertas dotadas de sistemas de apertura con llave o dispositivo equivalente. Si no fuera posible por las características de los mismos, se adoptarán medidas alternativas y se motivarán en su Documento de Seguridad.
  - La generación de copias o la reproducción de los documentos únicamente podrá ser realizada bajo el control del personal autorizado en el documento de seguridad. Deberá procederse a la destrucción de las copias o reproducciones desechadas de forma que se evite el acceso a la información o su recuperación posterior.
  - El acceso a la documentación se limitará exclusivamente al personal autorizado y se establecerán mecanismos que permitan identificar los accesos realizados por múltiples usuarios. También se registrarán los accesos de personal no autorizado de acuerdo con el procedimiento establecido al efecto en el documento de seguridad.
  - Deberán adoptarse medidas dirigidas a impedir el acceso o manipulación de la información objeto de traslado físico.

4. HISTORIAL DE REVISIONES		
Revisión	**Fecha**	**Modificaciones**
00	14/10/2013	Primera versión