DISPOSICIONES GENERALES

OSAKIDETZA-SERVICIO VASCO DE SALUD

3609

ACUERDO de 26 de junio de 2017, del Consejo de Administración del Ente Público Osakidetza-Servicio vasco de salud, por el que se regulan Cláusulas de Protección de Datos de Carácter Personal cuya inclusión debe considerarse en supuestos de Contratación Administrativa por Osakidetza-Servicio vasco de salud.

El artículo 12 de la Ley Orgánica 15/1999 de Protección de Datos de carácter personal (en adelante, LOPD) establece lo siguiente:

1.– No se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento.

2.– La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas. En el contrato se estipularán, asimismo, las medidas de seguridad a que se refiere el artículo 9 de esta Ley que el encargado del tratamiento está obligado a implementar.

3.– Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.

4.– En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado, también, responsable del tratamiento, respondiendo de las infracciones.

Por otra parte, se ha de considerar que Osakidetza-Servicio vasco de salud en todos los procedimientos de Contratación administrativa se encuentra obligada a respetar los modelos de Pliegos de Contratación previamente aprobados por los órganos competentes.

Es por ello que, al objeto de dar cumplimiento a los requisitos señalados precedentemente, Osakidetza-servicio vasco de salud ha de establecer para el momento de la firma del contrato, o en posterior adenda al mismo, que toda prestación de servicios que implique el tratamiento de datos de carácter personal, independientemente de la cuantía de la misma, se realice mediante la firma de un contrato de acceso a datos que refleje el contenido mínimo establecido en dicho artículo 12 de la LOPD; es decir:

- Que el encargado de tratamiento tratará los datos de carácter personal conforme a las instrucciones del responsable del fichero.
- Que no los utilizará con fin diferente al que figure en el contrato.
- Que no los comunicará, ni siquiera para su conservación, a otras personas.

● Que una vez terminada la prestación del servicio se deberá, o bien destruir los datos, o bien devolverlos, haciendo indicación precisa de aspectos como el plazo, el modo, etc., establecidos para cumplir dicho requisito.

● Las concretas medidas de seguridad que debe implementar el encargado del tratamiento.

En su virtud, de conformidad con las facultades otorgadas por las disposiciones legales,

ACUERDO:

Primero.– Las cláusulas I a XIII siguientes se incorporarán íntegras, para el momento de firma del contrato con la empresa adjudicataria, sustituyendo las equis (XXX) con la identificación del prestador del servicio (en general, la empresa contratada):

I.– Osakidetza-Servicio vasco de salud es responsable de los ficheros que se tratan con motivo del servicio objeto de la contratación, conforme la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante LOPD).

Dichos ficheros, declarados, en su caso, ante el Registro General de la Agencia Vasca de Protección de Datos recogen, según corresponda, información de los empleados, de pacientes o de quienes sean contratistas de este Ente Público.

Todo lo que se estipula a continuación se circunscribe a los datos de carácter personal contenidos en los ficheros arriba enunciados que XXX pudiera tratar con motivo de la prestación del servicio contratado.

II.– XXX, como parte del presente contrato, se convierte desde su perfección en encargado de tratamiento conforme al Artículo 12 de la LOPD.

A los efectos de comunicación a la Agencia Vasca de Protección de Datos, XXX consiente en figurar como encargado de tratamiento en cuantos ficheros sean objeto del presente contrato.

III.– XXX, no podrá utilizar dichos datos para otro fin distinto de aquel que constituya el objeto del presente contrato.

IV.– XXX se compromete a tratar los datos conforme a las instrucciones que le marque Osakidetza-Servicio vasco de salud, las cuales provendrán de (citar el cargo de la persona responsable de Osakidetza-servicio vasco de salud).

V.– XXX 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 presente contrato, o a los procedimientos de subcontratación que, en su caso, pudieran establecerse, salvo requerimiento judicial específico.

VI.– XXX 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 Osakidetza-Servicio vasco de salud y para los afectados.

VII- XXX se obliga a realizar cuantas gestiones correspondan para que el personal a su cargo firme una cláusula de confidencialidad por la que se comprometa a no revelar la información que pudiera conocer en función de su cargo o cometido durante la prestación del presente contrato y posteriormente al mismo.

VIII.– En el supuesto de que XXX haya sido autorizado a mantener algún dato proveniente del presente contrato, se obliga a devolverlo a Osakidetza-Servicio vasco de salud una vez cumplida la prestación contractual, en el plazo de tres meses, o en su caso, a destruirlo, al igual que el soporte o documento en el que conste aquél.

IX.– XXX quedará sujeto al régimen de responsabilidad que instaura la LOPD y responderá 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 de este contrato, conforme a cuantas acciones penales o civiles pudiera corresponder.

X.– XXX 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 adjunto.

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

XIII. En caso de subcontratación, la empresa contratista y la subcontratada deberán cumplir cuantas obligaciones legales corresponda en aplicación de las previsiones de contratación administrativa.

En lo referente al régimen de Protección de Datos Personales, la contratista exigirá a la subcontratada el cumplimiento de las mismas medidas de seguridad que las que a ella correspondieran en cumplimiento y ejecución de las previsiones del contrato administrativo.

La identidad del subcontratista deberá ser comunicada a Osakidetza, sin que resulte, ello no obstante, obligada la comunicación de la condición de nuevo encargado de tratamiento a la Agencia Vasca de Protección de datos.

Segundo.– Del anexo de Medidas de Seguridad, que se inserta a continuación, se ha de realizar un análisis pormenorizado en cada caso, de modo que sólo deberán incorporarse las medidas adecuadas al objeto del servicio contratado y a la naturaleza y nivel de seguridad de los datos de carácter personal accedidos; pudiéndose añadir cuantas medidas de seguridad y protección de datos se consideren pertinentes, siempre y cuando no contradigan lo dispuesto legalmente ni lo previsto en el Documento de Seguridad de Osakidetza.

ANEXO

MEDIDAS DE SEGURIDAD

Medidas de nivel básico.

Para los tratamientos que contengan datos de nivel básico, la entidad adjudicataria adoptará las siguientes medidas:

● Con carácter general, las personas usuarias y/o personal de la entidad adjudicataria deberán disponer y conocer de unas funciones y obligaciones definidas, difundidas y documentadas respecto a la seguridad de los Datos de Carácter Personal. En todo caso, deberán atenerse a las instrucciones que en la materia les aporte la responsable de ficheros Osakidetza-Servicio vasco de salud.

● En caso de que la entidad adjudicataria precise acceder a datos a través de redes de comunicaciones deberá garantizar un nivel de seguridad equivalente al correspondiente al acceso en modo local.

● La entidad adjudicataria se compromete a no realizar tratamientos de datos fuera de los locales de ubicación del fichero sin la autorización previa de Osakidetza-Servicio vasco de salud.

● La entidad adjudicataria se compromete a que los ficheros temporales y/o copia de documentos generados a partir de un fichero maestro cumplirán con el nivel de seguridad correspondiente a este último y que los eliminará una vez hayan dejado de ser necesarios.

● Cualquier incidencia que afecte a la integridad, confidencialidad, autenticidad y disponibilidad del tratamiento de los datos de carácter personal llevada a cabo por la entidad adjudicataria será comunicada de inmediato a Osakidetza-Servicio vasco de salud.

● La entidad adjudicataria se encargará de que exista una relación actualizada de su personal con acceso a los datos de carácter personal de Osakidetza-Servicio vasco de salud y de establecer los procedimientos de identificación y autenticación para dicho acceso cuando se encuentren bajo su control y/o deba implementarlo de acuerdo al objeto del contrato.

● Cuando el mecanismo de identificación y autenticación de las personas usuarias de la entidad adjudicataria se encuentre bajo su control y/o deba implementarlo de acuerdo al objeto del contrato garantizará la identificación de modo inequívoco y personalizado. Si la autenticación se basa en contraseñas, existirá un procedimiento de distribución y almacenamiento que garantice su confidencialidad, integridad e ininteligibilidad. Las contraseñas deberán cambiarse periódicamente al menos una vez al año.

● Las personas usuarios de la entidad adjudicataria tendrán acceso únicamente a los datos de carácter personal estrictamente necesarios para la realización de sus funciones y, en todo caso, durante el tiempo que duren los servicios. La entidad adjudicataria establecerá mecanismos para disponer de una relación actualizada de perfiles de sus personas usuarias y, si es preciso, para evitar que dichas personas accedan a aplicaciones con derechos distintos de los autorizados. Una vez finalizadas las funciones de sus personas usuarias, los accesos a los datos de carácter personal serán eliminados. En todo caso, solamente las personas autorizadas por Osakidetza-Servicio vasco de salud podrán gestionar las autorizaciones de acceso a los recursos.

● Cuando el tratamiento de datos de carácter personal de Osakidetza-Servicio vasco de salud conlleve la utilización de cualquier tipo de soporte, la adjudicataria se encargará de mantenerlos etiquetados e inventariados y restringirá el acceso a los mismos a su personal previamente autorizado.

● Con carácter general, la salida de soportes con datos personales fuera de las instalaciones de Osakidetza-Servicio vasco de salud debe ser previamente autorizada por la misma. En caso de disponer de autorización, la entidad adjudicataria adoptará las medidas necesarias para impedir cualquier recuperación indebida de la información almacenada en el soporte y establecerá un registro de salida de soportes informáticos que permita conocer el tipo de soporte, fecha y hora de entrada o salida, forma de envío y persona encargada del envío o recepción del mismo en cada caso.

● La entidad adjudicataria adoptará las medidas necesarias para garantizar la imposibilidad de recuperación de datos cuando un soporte sea desechado o reutilizado.

● En caso de que la entidad adjudicataria deba realizar copias de respaldo de los datos personales de acuerdo al objeto del contrato, deberá realizar copias de seguridad al menos semanalmente

a fin de que garanticen la reconstrucción de los datos en caso de pérdida o destrucción y además, verificar el correcto funcionamiento de dichas copias al menos cada seis meses. Será necesaria la autorización por escrito de la responsable del fichero para la ejecución de los procedimientos de recuperación de los datos.

● La entidad adjudicataria, previamente a la implantación y/o modificación de sistemas de información, no podrá realizar pruebas con datos reales salvo que, disponga de autorización previa de Osakidetza-Servicio vasco de salud, se asegure el nivel de seguridad correspondiente al tipo de fichero tratado, se anote su realización en el Documento de Seguridad de Osakidetza-Servicio vasco de salud y se realice una copia de seguridad previa de los Sistemas de Información.

● En caso de que la entidad adjudicataria trate datos personales no automatizados de acuerdo al objeto del contrato, 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. Especialmente, se estará a lo dispuesto en la normativa sanitaria en caso de tratamientos de datos y ficheros afectados por dicha legislación.

● Los dispositivos de almacenamiento de los documentos bajo control de la entidad adjudicataria 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 y de igual modo, durante los procesos de revisión o tramitación de la documentación.

Medidas de nivel medio.

● En caso de que la entidad adjudicataria controle y/o deba implantar el mecanismo de identificación y autenticación de personas usuarias de acuerdo al objeto del contrato, se deberá de restringir el número de intentos de acceso erróneos a un máximo de cinco (5).

● En caso de que el acceso físico a los locales donde se encuentren los Sistemas de Información con datos de carácter personal de Osakidetza-Servicio vasco de salud se encuentren bajo control y/o dependan de la entidad adjudicataria de acuerdo al objeto del contrato, se deberá establecer un control del acceso físico de acuerdo a las instrucciones del responsable de fichero.

● En caso de que la entidad adjudicataria deba remitir o enviar datos personales de nivel medio mediante soportes físicos con capacidad de almacenamiento, deberá registrar las entradas indicando el tipo de documento o soporte, la fecha y hora, la persona emisora, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción que deberá estar debidamente autorizada.

● En caso de que se produzca alguna incidencia que afecte a la seguridad de los datos de nivel medio, la entidad adjudicataria deberá comunicar, además de lo indicado en el nivel básico, los procedimientos realizados de recuperación de los datos, 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. En todo caso, será necesaria la autorización de Osakidetza-Servicio vasco de salud para la ejecución de los procedimientos de recuperación de los datos.

Medidas de nivel alto.

Para la prestación de servicios que conlleven tratamientos de datos de carácter personal de nivel alto, la entidad adjudicataria deberá adoptar además de las de nivel básico y medio, las siguientes medidas:

● La entidad adjudicataria deberá adoptar las medidas necesarias para que la distribución de soportes con datos de carácter personal de nivel alto se realice cifrando su contenido o garantizando que la información no sea inteligible ni manipulada durante su transporte.

● Cualquier transmisión de datos de nivel alto a través de redes de telecomunicaciones deberá contar con medios de cifrado o análogos que no permitan la lectura y manipulación de la información por terceros.

● En caso de que la entidad adjudicataria deba realizar copias de respaldo de los datos de carácter personal de nivel alto conservará una copia de seguridad y de los procedimientos de recuperación de los datos en un lugar diferente de aquel en que se encuentren los equipos que los tratan.

● En caso de que la entidad adjudicataria deba implantar y/o controlar los mecanismos de identificación/autenticación de personas usuarias y/o de su personal deberá implantar un sistema de registro de cada acceso a los datos de carácter personal que deberá conservar al menos durante dos años, a disposición de Osakidetza-Servicio vasco de salud. En concreto, el mencionado registro de accesos deberá guardar la identificación de la persona usuaria, fecha y hora, fichero accedido, tipo de acceso, y si ha sido autorizado o denegado. En caso de ser autorizado, se anotará también a qué registros se ha accedido. La entidad adjudicataria deberá revisar al menos una vez al mes la información del registro de accesos y emitir un informe con las acciones realizadas y los problemas detectados que quedará a disposición de Osakidetza-Servicio vasco de salud.

● En caso de que la entidad /adjudicataria deba tratar datos de nivel alto no automatizados por cuenta de Osakidetza-Servicio vasco de salud, tanto en lugares físicos propios como del responsable de ficheros deberá proteger mediante puertas dotadas de sistemas de apertura con llave o dispositivo equivalente los armarios, archivadores u otros elementos en los que se almacenen los datos personales no automatizados. En su defecto, si dicha medida no fuera posible se adoptarán medidas alternativas y se motivarán en el Documento de Seguridad.

● La entidad adjudicataria y su personal podrá generar copias y reproducir documentos en papel con datos de nivel alto previa autorización de Osakidetza-Servicio vasco de salud. En caso de autorización deberá: disponer de un listado de personal y personas usuarias autorizadas a tratar con datos no automatizados de nivel alto; garantizar la confidencialidad de la información cuando se destruya o deseche, con el fin de impedir su recuperación posterior, ante el traslado de documentos; adoptar medidas que impidan el acceso o la manipulación por terceras personas ajenas no autorizadas; Implantar un mecanismo que registre los accesos a datos no automatizados realizados por múltiples personas usuarias.

Tercero.– Las áreas responsables de incorporar estas cláusulas y medidas serán aquellos Servicios y Unidades que requieran la prestación de los servicios de terceros y que, en consecuencia, participen en la confección de contratos administrativos o bien en la definición de los requisitos del servicio demandado.

Este Acuerdo entrará en vigor al día siguiente de su publicación en el Boletín Oficial del País Vasco.

En Vitoria-Gasteiz, a 26 de junio de 2017.

El Presidente del Consejo de Administración de Osakidetza-Servicio vasco de salud,
JON DARPÓN SIERRA.