ACUERDO de 26 de septiembre de 2018 por el que se modifica el Acuerdo de 24 de junio de 2016, por el que se dispone la publicación de las cláusulas específicas de seguridad de la información que deben incluirse en determinados contratos celebrados por la Consejería de Medio Ambiente y Rural, Políticas Agrarias y Territorio como organismo pagador de los gastos financiados por el Fondo Europeo Agrícola de Garantía (FEAGA) y por el Fondo Europeo Agrícola de Desarrollo Rural (FEADER).

(2018AC0034)

La Consejería con competencias en materia de agricultura, como organismo pagador de los fondos europeo agrícolas, Fondo Europeo Agrícola de Garantía (FEAGA) y al Fondo Europeo Agrícola de Desarrollo Rural (FEADER) y de acuerdo con lo establecido en el Decreto 299/2015, de 27 de noviembre, por el que se designa y establece la organización y funcionamiento del Organismo Pagador de los gastos financiados por el Fondo Europeo Agrícola de Garantía (FEAGA) y al Fondo Europeo Agrícola de Desarrollo Rural (FEADER) en la Comunidad Autónoma de Extremadura, debe cumplir unas condiciones mínimas de autorización en materia de entorno interior, actividades de control, información, comunicación y seguimiento.

El Reglamento Delegado (UE) n.º 907/2014 de la Comisión, de 11 de marzo de 2014, que completa el Reglamento (UE) n.º 1306/2013 del Parlamento Europeo y del Consejo, en lo relativo a los organismos pagadores y otros órganos, la gestión financiera, la liquidación de cuentas, las garantías y el uso del euro, establece en su anexo I punto 3 B) ii) la obligación de que la seguridad de los sistemas de información esté certificada de conformidad con la norma ISO /IEC 27001: Information Security management systems-Requeriments (ISO) (Sistema de gestión de la seguridad de la información-Requisitos) (ISO).

La ISO/IEC 27001 dispone que la organización del organismo pagador ha de establecer las medidas de seguridad en todas aquellas relaciones que mantenga con terceros, independientemente de la naturaleza y objeto de éstas.

Para dar cumplimiento a dichas obligaciones se publicó, en el Diario Oficial de Extremadura el Acuerdo de 24 de junio de 2016 por el que se dispone la publicación de las cláusulas específicas de seguridad de la información que deben incluirse en determinados contratos celebrados por la Consejería de Medio Ambiente y Rural, Políticas Agrarias y Territorio, como organismo pagador de los gastos financiados por el Fondo Europeo Agrícola de Garantía (FEAGA) y al Fondo Europeo Agrícola de Desarrollo Rural (FEADER).

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 sus datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE

(Reglamento General de Protección de Datos), es de aplicación directa en todos los países de la Unión Europea desde el 25 de mayo de 2018.

El Reglamento General de Protección de Datos supone una profunda modificación del régimen vigente en materia de protección de datos personales, no sólo desde el punto de vista sustantivo y de cumplimiento por los sujetos obligados, sino particularmente en lo que afecta a la actividad de supervisión por parte de las autoridades de control que el mismo regula.

El citado reglamento extiende su protección a los derechos y libertades fundamentales de las personas físicas y en particular, su derecho a la protección de los datos personales.

La cláusula segunda del Acuerdo de 24 de junio de 2016 antes citado, se refiere a la protección de datos de carácter personal, siendo necesaria una nueva regulación de su contenido, acorde con las nuevas exigencias del Reglamento General de Protección de Datos.

Asimismo, se ha considerado necesaria la ampliación de su ámbito de aplicación, de manera que queden incluidos la totalidad de los contratos de servicios y aquellos contratos de obras que se ejecuten en las dependencias de la Consejería con competencia en materia de agricultura, con independencia de su fuente de financiación. De esta forma, dichos contratos contendrán unas cláusulas específicas de seguridad de la información que se deberán aplicar como un requisito adicional al cumplimiento del resto de obligaciones contractuales.

Por consiguiente, en virtud de las atribuciones que me confiere la legislación vigente

A C U E R D O :

Único. Disponer la publicación de la modificación del Acuerdo de 24 de junio de 2016 por el que se dispone la publicación de las cláusulas específicas de seguridad de la información que deben incluirse en determinados contratos celebrados por la Consejería de Medio Ambiente y Rural, Políticas Agrarias y Territorio como organismo pagador de los gastos financiados por el Fondo Europeo Agrícola de Garantía (FEAGA) y al Fondo Europeo Agrícola de Desarrollo Rural (FEADER), de acuerdo con lo siguiente:

Primero. Se modifica el título del Acuerdo de 24 de junio de 2016 por el que se dispone la publicación de las cláusulas específicas de seguridad de la información que deben incluirse en determinados contratos celebrados por la Consejería de Medio Ambiente y Rural, Políticas Agrarias y Territorio como organismo pagador de los gastos financiados por el Fondo Europeo Agrícola de Garantía (FEAGA) y por el Fondo Europeo Agrícola de Desarrollo Rural (FEADER), que pasa a denominarse Acuerdo de 24 de junio de 2016 por el que se dispone la publicación de las cláusulas específicas de seguridad de la información que deben incluirse en determinados contratos celebrados por la Consejería de Medio Ambiente y Rural, Políticas Agrarias y Territorio.

Segundo. Se modifica la cláusula segunda: protección de datos de carácter personal, que queda redactada en la siguiente forma:

"Segunda. Protección de datos.

A. BASE NORMATIVA.

El prestador de servicios quedará obligado al cumplimiento del ----- 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 y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos) (En adelante RGPD).

La Consejería de Medio Ambiente y Rural, Políticas Agrarias y Territorio ostenta la posición de Responsable del tratamiento con las funciones, derechos y obligaciones que le son propias.

El prestador de servicios trata datos de carácter personal por cuenta del Responsable del tratamiento, asume la responsabilidad de Encargado del tratamiento (artículo28 del RGPD).

B. OBLIGACIONES DERIVADAS DEL CONTRATO.

B.1. Obligaciones derivadas del contrato.

El Encargado y todo el personal bajo su control se obliga a:

a. Utilizar los datos personales objeto de tratamiento, o los que recoja para su inclusión, sólo para la finalidad objeto de este encargo. En ningún caso podrá utilizar los datos para fines propios.

b. Tratar los datos de acuerdo con las instrucciones documentadas del Responsable. Inclusive con respecto a las transferencias internacionales de datos; si el Encargado debe transferir datos personales a un tercer país o a una organización internacional, en virtud del Derecho de la Unión o de los Estados miembros que le sea aplicable, informará al Responsable de esa exigencia legal de manera previa, salvo que tal Derecho lo prohíba por razones importantes de interés público.

c. Llevar, por escrito, salvo que pueda acogerse a alguna de las excepciones del artículo 30.5 del RGPD, un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta del Responsable, que contenga, conforme al artículo 30.2 del RGPD:

1. El nombre y los datos de contacto del Encargado y de cada responsable por cuenta del cual actúe el Encargado.

2. Las categorías de tratamientos efectuados por cuenta de cada responsable.

3. Una descripción general de las medidas técnicas y organizativas de seguridad apropiadas que esté aplicando al tratamiento de los datos.

d. No comunicar los datos a terceras personas, salvo que cuente con la autorización expresa del Responsable, en los supuestos legalmente admisibles.

e. Si el Encargado quiere subcontratar total o parcialmente el tratamiento, tiene que informar al Responsable y solicitar su autorización previa. En caso de autorización positiva deberá cumplir las siguientes condiciones:

1. El subencargado quedará sujeto a las mismas condiciones (instrucciones, obligaciones, medidas de seguridad …) y con los mismos requisitos formales que el Encargado, en lo referente al adecuado tratamiento de los datos personales y a la garantía de los derechos de las personas afectadas.

2. El Encargado pondrá a disposición un listado en el que se identifiquen los servicios subcontratados y la identidad de los subencargos.

3. En caso de incumplimiento por parte del subencargado, el Encargado continuará siendo plenamente responsable.

f. Mantener el deber de secreto respecto a los datos de carácter personal a los que haya tenido acceso en virtud del presente encargo, incluso después de que finalice el contrato.

g. Garantizar que las personas autorizadas para tratar datos personales se comprometan de forma expresa y por escrito, a respetar la confidencialidad a cumplir las medidas de seguridad correspondientes, de las que el encargado les informará convenientemente. El Encargado mantendrá a disposición del Responsable la documentación acreditativa del cumplimiento de esta obligación.

h. Garantizar la formación necesaria en materia de protección de datos personales de las personas autorizadas para tratar datos personales.

i. Cuando las personas afectadas ejerzan los derechos de acceso, rectificación, supresión y oposición, limitación del tratamiento y portabilidad de datos ante el Encargado, éste debe comunicarlo por correo electrónico a la dirección que indique el Responsable. La comunicación debe hacerse de forma inmediata y en ningún caso más allá del día laborable siguiente al de la recepción de la solicitud, juntamente, en su caso, con otras informaciones que puedan ser relevantes para resolver la solicitud.

j. Notificación de violaciones de la seguridad de los datos. El encaragado notificará al Responsable, sin dilación indebida y a través de la dirección de correo electrónico que le indique el Responsable, las violaciones de la seguridad de los datos personales a su cargo de las que tenga conocimiento, juntamente con toda la informa-

ción relevante para la documentación y comunicación de la incidencia. Se facilitará, como mínimo, la información siguiente:

— Descripción de la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados.

— Datos de la persona de contacto del Encargado para obtener más información.

— Descripción de las posibles consecuencias de la violación de la seguridad de los datos personales.

— Descripción de las medidas adoptadas o propuestas parta poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos. Si no es posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.

k. El Encargado asistirá al responsable con toda la información de la que disponga, a realizar la comunicación de las violaciones de la seguridad a los interesados, cuando sea probable que dicha violación suponga un alto riesgo para sus derechos y libertades.

l. El Encargado, a petición del Responsable, comunicará en el menor tiempo posible, con toda la información de la que disponga, la violación de la seguridad de los datos a los interesados, cuando sea probable que la violación suponga un alto riesgo para los derechos y las libertades de las personas físicas. La comunicación debe realizarse en un lenguaje claro y sencillo y deberá incluir los elementos que en cado caso señale el Responsable y, como mínimo:

— La naturaleza de la violación de datos.

— Indicación de contacto del Responsable o del Encargado donde se pueda obtener más información.

— Posibles consecuencias de la violación de la seguridad de los datos personales.

— Medidas adoptadas o propuestas por el Responsable para poner remedio a la violación de la seguridad, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

m. Poner a disposición del Responsable toda la información necesaria para demostrar el cumplimiento de sus obligaciones, así como para la realización de las auditorías o las inspecciones que realicen el Responsable u otro auditor autorizado por él.

n. Implantar las medidas de seguridad técnicas y organizativas necesarias para garantizar la confidencialidad, integridad, disponibilidad y resilencia permanentes de los sistemas y servicios de tratamiento. Las medidas de seguridad mínimas se recogen en el apartado "Medidas de seguridad mínimas a aplicar por el Encargado.

B.2. Obligaciones del responsable.

Corresponde al Responsable:

— Proporcionar al Encargado los datos necesarios para que pueda prestar el servicio.

— Velar, de forma previa y durante todo el tratamiento, por el cumplimiento del RGPD por parte del Encargado.

— Supervisar el tratamiento, incluida la realización de inspecciones y auditorías.

C. MEDIDAS DE SEGURIDAD MÍNIMAS A APLICAR POR EL ENCARGADO.

C.1. Ámbito de aplicación.

Los ámbitos de aplicación de estas medidas serán:

— Los recursos bajo el control del Encargado (como sistemas informáticos y/o de archivo, centros de trabajo y trabajadores) y que éste destine al tratamiento de los datos.

— Los recursos bajo el control del Responsable cuanto éste haya encomendado al Encargado la seguridad de los mismos.

— Los sistemas de información que el Encargado desarrolle o implante por cuenta del Responsable.

C.2. Medidas organizativas.

Todo el personal al que el Encargado proporcione acceso a los datos personales deberá ser informado de las siguientes medidas organizativas:

1. Deber de confidencialidad y secreto, este deber persiste incluso cuando finalice la relación laboral o de prestación de servicios.

2. Se deberá evitar el acceso de personas no autorizadas a los datos personales, a tal fin se evitará: dejar los datos personales expuestos a terceros (pantallas electrónicas desatendidas, documentos en papel en zonas de acceso público, soportes con datos personales, etc.), esta consideración incluye las pantallas que se utilicen para la visualización de imágenes del sistema de videovigilancia si lo hubiera. Cuando la persona se ausente del puesto de trabajo, procederá al bloqueo de la pantalla o al cierre de la sesión.

3. Los documentos en papel y soportes electrónicos se almacenarán en lugar seguro (armarios o estancias de acceso restringido) durante las 24 horas del día, y serán custodiados cuando, con motivo de su tramitación, se encuentren fuera de los dispositivos o salas de archivo.

4. No se desecharán documentos (papel) o soportes electrónicos (cd, pendrives, discos duros, etc.) con datos personales sin garantizar su destrucción, de forma que la información no sea recuperable.

5. No se comunicarán datos personales o cualquier información personal a terceros, prestando atención especial en no divulgar datos personales protegidos durante las consultas telefónicas, correos electrónicos, etc.

6. Derechos de los titulares de los datos. Se informará a todo el personal del Encargado acerca del procedimiento, si procede, para atender los derechos de los interesados, definiendo de forma clara los mecanismos por los que pueden ejercerse los mismos y teniendo en cuenta lo siguiente:

   6.1. Los interesados podrán ejercer, en los términos establecidos por la legislación vigente, los derechos de acceso, rectificación y supresión de datos, así como solicitar que se limite el tratamiento de sus datos personales, oponerse al mismo, o solicitar la portabilidad de sus datos dirigiendo una comunicación por escrito al Responsable, a través de direcciones especificadas.

   6.2. Asimismo, podrán ponerse en contacto con los respectivos delegados de protección de datos en la dirección dpd@juntaex.es, o presentar una reclamación ante la Agencia Española de Protección de Datos u otra autoridad competente.

   6.3. La obligación de atender estos derechos corresponde al Responsable.

   6.4. Si la petición la recibe el Encargado, en relación a los tratamientos por cuenta del Responsable, éste tiene la obligación de comunicarle dicha solicitud en un periodo inferior a 24 horas, acompañándola de la información pertinente de la que disponga.

   6.5. El Responsable identificará las acciones que deben realizarse en base a la petición de los interesados, que serán comunicadas al Encargado.

      a) Para el derecho de acceso se procederá a facilitar al Responsable los datos de los interesados que obren en su poder.

      b) Para el derecho de rectificación se procederá a modificar los datos de los interesados que fueran inexactos o incompletos atendiendo a los fines del tratamiento.

c) Para el derecho de supresión se suprimirán los datos de los interesados cuando estos manifiesten su negativa u oposición para el tratamiento de los mismos y no exista base legal que lo impida.

6.6. Violaciones de seguridad de datos de carácter personal. Cuando se produzcan violaciones de seguridad de datos de carácter personal, como, por ejemplo, el robo o acceso indebido a los mismos se notificará al Responsable de forma inmediata acerca de tal circunstancia, incluyendo toda la información necesaria para el esclarecimiento de los hechos. Asimismo, se apoyará al Responsable para realizar la notificación de la violación de la seguridad a la Agencia Española de Protección de Datos teniendo en cuenta la información a disposición del Encargado.

6.7. El ejercicio de derechos requerirá la previa presentación por parte del interesado de copia de su DNI o documento identificativo.

6.8. No obstante el Encargado tiene la obligación de informar a cualquier interesado de las siguientes circunstancias:

a) Lista de tipologías de datos personales tratados.

b) Finalidad para la que han sido recogidos.

c) Identidad de los destinatarios de los datos.

d) Plazo de conservación de los datos.

e) Identidad del Responsable ante el que pueden solicitar la rectificación, supresión y oposición al tratamiento.

f) Datos de contacto del Delegado de Protección de Datos.

C.3. Medidas de seguridad técnicas para la identificación

El Encargado implantará como mínimo las siguientes medidas técnicas para garantizar la identificación y autenticación de los usuarios con acceso a los datos:

1. No se permitirá el uso para fines particulares de aquellos ordenadores y dispositivos destinados al tratamiento de los datos personales.

2. Se recomienda disponer de perfiles con derechos de administración para la instalación y configuración del sistema y usuarios sin privilegios o derechos de administración para el acceso a los datos personales. Esta medida evitará que en caso de ataque de ciberseguridad puedan obtenerse privilegios de acceso o modificar el sistema operativo.

3. Se garantizará la existencia de contraseñas (o mecanismos equivalentes) para el acceso a los datos personales almacenados en sistemas electrónicos. La contrase-

ña tendrá la menos 8 caracteres, mezcla de números y letras, frases complejas, etc y se renovarán periódicamente.

4. Cuando a los datos personales accedan distintas personas, para cada una de ellas, se dispondrá de un usuario y contraseña específicos (identificación inequívoca).

5. Se debe garantizar la confidencialidad de las contraseñas, evitando que queden expuestas a terceros. En ningún caso se compartirán las contraseñas ni se dejarán anotadas en lugar común y el acceso de personas distintas del usuario.

C.4. Medidas de seguridad técnicas para salvaguardar los datos.

A continuación, se exponen las medidas técnicas mínimas para garantizar la salvaguarda de los datos personales:

1. Actualización de ordenadores y dispositivos. Los dispositivos y ordenadores utilizados para el almacenamiento y el tratamiento de los datos personales deberán mantenerse actualizados.

2. Malware. En los ordenadores y dispositivos donde se realice el tratamiento de los datos personales se dispondrá de un sistema de antivirus que garantice en la medida de lo posible el robo y destrucción de la información y tales datos personales. El sistema de antivirus deberá estar actualizado permanentemente y gestionado de forma central.

3. Cortafuegos. Para evitar accesos remotos indebidos a los datos personales se velará para garantizar la existencia de un cortafuegos activado en aquellos sistemas en los que se realice el almacenamiento y/o tratamiento de los mismos.

4. Cifrado de datos. Cuando se precise realizar la extracción de datos personales fuera del recinto donde se realiza su tratamiento, ya sea por medios físicos o por medios electrónicos, se deberá valorar la posibilidad de utilizar un método de cifrado para garantizar su confidencialidad.

5. Copia de seguridad. Periódicamente se realizará una copia de seguridad en un segundo soporte distinto del que se utiliza para el trabajo diario. La copia se almacenará en un lugar seguro, distinto de aquél en que esté ubicado el equipo con los ficheros originales, con el fin de permitir la recuperación de los datos personales en caso de pérdida de la información.

C.5. Verificación, evaluación y valoración periódica de las medidas de seguridad.

El Encargado implantará un procedimiento a periódico que le permita verificar, evaluar y valorar, la eficacia de las medidas técnicas y organizativas implantadas en los sistemas de tratamiento, centros de trabajo y usuarios bajo su control.

De ese procedimiento periódico se derivarán la implantación de mecanismos adicionales para:

— Garantizar la confidencialidad, integridad, disponibilidad y resilencia permanentes de los sistemas y servicios de tratamiento.

— Restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.

— Seudonimizar y cifrar los datos personales, en su caso.

Las medidas de seguridad abarcarán la protección de los sistemas de información así como de los sistemas de tratamiento manual y el archivo de la documentación.

La revisión podrá realizarse por mecanismos automáticos (software o programas informáticos) o de forma manual.

C.6. Medidas de seguridad.

El Encargado dispondrá en todo momento de información actualizada sobre las medidas de seguridad aplicadas en el encargo de tratamiento y deberá proporcionarlas al Responsable cuando éste las solicite y en todo caso siempre que haya cambios relevantes en su arquitectura de seguridad de la información".

La presente modificación entrará en vigor al día siguiente de su publicación en el Diario Oficial de Extremadura.

Mérida, 26 de septiembre de 2018.

El Secretario General,

F. JAVIER GASPAR NIETO