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). (2016AC0005)

El Reglamento (UE) n.º 1306/2013, del Parlamento Europeo y del Consejo, de 17 de diciembre de 2013, por el que se derogan los Reglamentos (CE) n.º 352/78, (CE) n.º 165/94, (CE) n.º 2799/98, (CE) n.º 814/2000, (CE) n.º 1290/2005 y (CE) n.º 485/2008, del Consejo, recoge la regulación, en su Título II, Capítulo II de los organismos pagadores, indicando que éstos serán los responsables de la gestión y control y de los gastos financiados en gestión compartida correspondientes al Fondo Europeo Agrícola de Garantía (FEAGA) y al Fondo Europeo Agrícola de Desarrollo Rural (FEADER).

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 Comuniad Autónoma de Extremadura designa, en su artículo 3 a la Consejería competente en materia de agricultura como el Organismo Pagador previsto en el Real Decreto 521/2006, de 28 de abril, por el que se establece el régimen de los organismos pagadores y de coordinación de los fondos europeos agrícolas, en el Reglamento n.º 1306/2013, del Parlamento Europeo y del Consejo de 13 de diciembre, y en sus disposiciones de desarrollo.

De acuerdo con lo anterior corresponde a la Consejería con competencias en materia de agricultura el cumplimiento de unas condiciones mínimas de autorización en materia de entorno interior, actividades de control, información, comunicación y seguimiento.

En este sentido, el Reglamento Delegado (UE) n.º 907/2014 de la Comisión de 11 de marzo de 2014 que completa el Reglamento (UE) núm.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, a partir del 16 de octubre de 2016, 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. Con el fin de dar cumplimiento a dicho mandato el Comité de Gestión y Coordinación de Seguridad de la Información del Organismo Pagador ha aprobado la "Normativa de Seguridad en Servicios de Terceros", que describe las normas de seguridad de la información aplicables a las relaciones con los mismos.

De acuerdo con lo anterior, la contratación que se lleve a cabo por la Consejería con competencias en materia de agricultura deberá contemplar en los contratos que apliquen dicha normativa las medidas de seguridad necesarias para su cumplimento. En este sentido, la totalidad de los contratos de servicios y aquellos contratos de obras que se ejecuten en las dependencias de la Consejería con competencias en materia de agricultura, cuyos gastos estén financiados por el Fondo Europeo Agrícola de Garantía (FEAGA) y por el Fondo Europeo Agrícola de Desarrollo Rural (FEADER), incluirán unas cláusulas específicas de seguridad de la información que se deberán aplicar en el ámbito de dichos contratos 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 en el Diario Oficial de Extremadura del contenido de las cláusulas específicas de seguridad de la información en todos los contratos de servicios y en los contratos de obras que se ejecuten en las dependencias de la Consejería con competencias en materia de agricultura, cuyos gastos estén financiados por el Fondo Europeo Agrícola de Garantía (FEAGA) y por el Fondo Europeo Agrícola de Desarrollo Rural (FEADER).

Mérida, 24 de junio de 2016.

El Secretario General,
F. JAVIER GASPAR NIETO

CLÁUSULAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN EN TODOS LOS CONTRATOS DE SERVICIOS Y EN CONTRATOS DE OBRAS QUE SE EJECUTEN EN LAS DEPENDENCIAS DE LA CONSEJERÍA CON COMPETENCIAS EN MATERIA DE AGRICULTURA, CUYOS GASTOS ESTÉN FINANCIADOS POR EL FONDO EUROPEO AGRÍCOLA DE GARANTÍA (FEAGA) Y POR EL FONDO EUROPEO AGRÍCOLA DE DESARROLLO RURAL (FEADER)

Primera: Confidencialidad de la información.

El tercero vendrá obligado a guardar la más estricta confidencialidad sobre el contenido del encargo, así como sobre los datos o información a la que pueda tener acceso como consecuencia de la ejecución del mismo, y a usar dicha información a los exclusivos fines de la ejecución del contrato y conforme a la Política de Seguridad del Organismo Pagador en los términos en que resulte aplicable. Esta obligación se mantendrá incluso después de la finalización de la relación contractual.

El deber de confidencialidad sobre la información del Organismo Pagador será extensible a todo el personal del tercero o colaborador con éste que participe en la prestación del servicio.

Todo el personal del tercero protegerá, en la medida de sus posibilidades, la información propiedad del Organismo Pagador y los sistemas de información a los que tenga acceso con el fin de evitar revelación, alteración o uso indebido de la información.

El acceso y posesión de información del Organismo Pagador por parte del tercero es estrictamente temporal y vinculado a las atribuciones propias del desempeño del puesto de trabajo o servicio contratado, sin que ello confiera derecho alguno de posesión, de titularidad de copia o de transmisión sobre dicha información.

El tercero, una vez finalizadas las tareas que han originado el acceso a la información, deberá devolver los soportes y documentación que pudiera habérsele facilitado.

El tercero no puede transmitir, enviar, compartir o poner a disposición de otras entidades información propiedad del Organismo Pagador, a no ser que de manera previa haya sido expresamente autorizado para hacerlo, independientemente del medio o formato de la información y de su contenido.

Segunda: Protección de datos de carácter personal.

El acceso del tercero a los datos de carácter personal contenidos en los ficheros titularidad de la Junta de Extremadura para la prestación de servicios objeto del presente pliego, no tendrá la consideración legal de comunicación o cesión de datos a los efectos previstos en el RD 1720/2007 de desarrollo de la LO 15/1999, de 23 de diciembre, de Protección de Datos de Carácter Personal, sino de acceso por cuenta de tercero según lo previsto en la citada ley. Tales datos de carácter personal serán propiedad exclusiva de la Junta de Extremadura.

A los efectos anteriores, el tercero tendrá la condición de encargado del tratamiento y se sujetará al deber de confidencialidad y seguridad de los datos personales a los que tenga

acceso conforme a lo previsto en la normativa que resulte aplicable, obligándose específicamente a lo siguiente:

a) A utilizar y aplicar los datos personales a los exclusivos fines del cumplimiento del objeto del contrato.

b) A adoptar las medidas de índole técnica y organizativa necesarias establecidas en el artículo 9 de la Ley Orgánica 15/1999 y en las normas reglamentarias que la desarrollen, que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, tratamiento o acceso no autorizado habida cuenta del estado de la tecnología, la naturaleza de los datos objeto de tratamiento y los riesgos a que estén expuestos, ya provengan de la acción humana o del medio físico o natural. En todo caso se obliga a aplicar las medidas de seguridad del nivel que corresponda en función de los datos a tratar de conformidad con lo previsto en el RD 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.

c) A mantener la más absoluta confidencialidad sobre los datos personales a los que tenga acceso para la prestación de servicios así como sobre los que resulten de su tratamiento cualquiera que sea el soporte en el que se hubieren obtenido.

d) Cuando se procesen datos de nivel medio o alto, responsabilidad de la Junta de Extremadura, en los sistemas o instalaciones del tercero, éste debe llevar a cabo los procesos de auditoría estipulados en la legislación aplicable. Los informes derivados de estos procesos de auditoría deben ser puestos a disposición del Organismo Pagador mientras dure la relación contractual entre éste y el tercero.

e) El tercero debe garantizar que los datos personales utilizados en el servicio prestado son los proporcionados por la Junta de Extremadura o que han sido recogidos con el consentimiento expreso del afectado (siguiendo lo establecido en la legislación aplicable) y que sólo son tratados y/o cedidos con la expresada finalidad, y siempre con el consentimiento del propietario de los datos.

f) Cuando el tratamiento de datos de carácter personal que sean responsabilidad de la Junta de Extremadura se realice o ejecute fuera de las instalaciones del proveedor, el tratamiento debe ser autorizado y validado previamente y de manera expresa por la Junta de Extremadura, garantizando el nivel de seguridad correspondiente al tipo de información tratada.

El incumplimiento de estos compromisos será responsabilidad exclusiva de la empresa adjudicataria, que responderá frente a terceros y frente a la Administración de la Junta de Extremadura de los daños y perjuicios que pudieran generarse.

Tercera: Propiedad Industrial e intelectual.

Sin perjuicio de lo dispuesto en la legislación vigente, el adjudicatario acepta expresamente que la propiedad de la documentación y los trabajos realizados al amparo del presente encargo, y durante el período de garantía y mantenimiento, corresponde únicamente a la

Junta de Extremadura, con exclusividad y sin más limitaciones que las impuestas por el ordenamiento jurídico.

Sin perjuicio de lo dispuesto por la legislación vigente en materia de propiedad intelectual y de protección jurídica de los programas de ordenador, el adjudicatario acepta expresamente que los derechos de explotación y la propiedad del código fuente de las aplicaciones desarrolladas al amparo del presente contrato corresponden únicamente a la Junta de Extremadura, con exclusividad y a todos los efectos.

El adjudicatario acepta expresamente que los derechos de propiedad sobre los soportes materiales a los que se incorporen los trabajos realizados, en cumplimiento de las obligaciones derivadas del contrato objeto de este pliego, corresponden a la Junta de Extremadura.

El adjudicatario exonerará a la Junta de Extremadura de cualquier tipo de responsabilidad frente a terceros por reclamaciones de cualquier índole dimanante de los suministros, materiales, procedimientos y medios utilizados para la ejecución del contrato objeto del presente pliego procedente de los titulares de derechos de propiedad industrial e intelectual sobre ellos.

Si fuera necesario, el adjudicatario estará obligado, antes de la formalización del contrato, a obtener las licencias y autorizaciones precisas que le legitimen para la ejecución del mismo.

En caso de acciones dirigidas contra la Junta de Extremadura por terceros titulares de derechos sobre los medios utilizados por el adjudicatario para la ejecución del contrato, éste responderá ante la Junta de Extremadura del resultado de dichas acciones, estando obligado, además, a prestarle su plena ayuda en el ejercicio de las acciones que competan a la Junta de Extremadura.

El adjudicatario no podrá hacer uso del nombre, marca o logotipo que le haya facilitado la Junta de Extremadura para el cumplimiento de sus obligaciones dimanantes del presente pliego, fuera de las circunstancias y para los fines expresamente pactados en éste, ni una vez terminada la vigencia del mismo.

Cuarta: Devolución de activos.

El adjudicatario se compromete a la devolución de todos los activos de que haya dispuesto para la prestación de servicios objeto del presente encargo, ya sean software, documentación corporativa, equipos y/o recursos materiales. Así mismo, si el personal del adjudicatario dispone de permisos de acceso a instalaciones o sistemas, estos deben ser devueltos o comunicados para su anulación en el momento de finalización del contrato, respondiendo de su uso una vez finalizados los servicios objeto del presente pliego.

El adjudicatario se compromete a entregar a la Junta de Extremadura toda la información y documentación resultante de los trabajos objeto del presente encargo, viniendo obligado, además, a no mantener documentación o almacenar información en locales o equipos ajenos o no autorizados por la Junta de Extremadura, durante o una vez finalizado el plazo contractual, más allá de aquella que sea necesaria para la ejecución del contrato o para el cumplimiento de los periodos de garantía y mantenimiento por parte de dicho adjudicatario. En los

casos en que esto sea necesario, deberán garantizarse niveles de seguridad acordes con la naturaleza de la información almacenada y con la Política de Seguridad de la Información de la Junta de Extremadura.

En los casos en que la Junta de Extremadura lo estime necesario podrá exigir al adjudicatario certificaciones de destrucción de documentos o eliminación de información de los equipos empleados para la realización de los servicios objeto del presente pliego, asimismo, podrá realizar revisiones de las instalaciones y procedimientos empleados por el adjudicatario.

Sin perjuicio de lo dispuesto en la legislación vigente, el incumplimiento de estos compromisos y las consecuencias derivadas de ello serán responsabilidad exclusiva del adjudicatario, que responderá frente a terceros y frente a la Administración de la Junta de Extremadura de los daños y perjuicios que pudieran generarse.

Quinta: Auditoría.

La Junta de Extremadura podrá exigir al adjudicatario cualquier evidencia de cumplimiento con la legislación aplicable, de acuerdo a lo marcado en los acuerdos firmados por ambas partes, así como con los requisitos de seguridad impuestos por parte de la Junta de Extremadura. Para ello la Junta de Extremadura se reserva el ejercicio de los siguientes derechos:

a) Revisar o auditar los mecanismos de salvaguarda de la Seguridad de la Información que tenga implementados el adjudicatario y que estén relacionados o implicados con los sistemas utilizados en la prestación del servicio contratado.

b) Revisar o auditar el cumplimiento por parte del adjudicatario con la legislación aplicable de acuerdo a lo dispuesto por los contratos firmados por ambas partes.

c) Requerir al adjudicatario los documentos derivados de los procesos de auditoría llevados a cabo por éste, así como cualquier otra evidencia sobre el cumplimiento con el marco legal aplicable y con los requisitos impuestos por el presente encargo.

d) Solicitar la implementación de cualquier mecanismo organizativo, técnico o jurídico que considere adecuado para garantizar la Seguridad de la Información.

Para facilitar el ejercicio de los anteriores derechos por parte de la Junta de Extremadura, el adjudicatario se compromete a facilitar y participar activamente en el desarrollo de las actividades anteriormente descritas.

Sexta: Cumplimiento del tercero con la política de seguridad de la información del Organismo Pagador.

El Organismo Pagador dispone de una Política de Seguridad de la Información, así como de un Marco Normativo para su desarrollo, los cuales establecen los controles de seguridad que se deben aplicar con objeto de garantizar la confidencialidad, disponibilidad, integridad, autenticidad y trazabilidad de la información. Es obligación del adjudicatario el conocimiento,

cumplimiento e implantación de aquellas medidas de seguridad establecidas en el Marco Normativo que, en base a la naturaleza de los servicios prestados, sea de aplicación. El Organismo Pagador se reserva el derecho de exigir al tercero la aplicación de las medidas de seguridad adicionales cuando los requisitos de seguridad de la información aplicables al servicio así lo requieran.

Séptima: Cumplimento por el personal del tercero de la politíca de seguridad de la información del organismo pagador.

El adjudicatario deberá concienciar y formar a su personal en materia de seguridad de la información, y en particular aquellos aspectos de la Política de Seguridad del Organismo Pagador y su Marco Normativo de desarrollo que sean de aplicación en base a la naturaleza de los servicios prestados.

Los trabajadores del adjudicatario por su parte deben tener siempre presentes durante el desempeño de sus funciones los principios de la ética, la profesionalidad, la confidencialidad y la responsabilidad.

De forma general, todo el personal del tercero que acceda a la información del Organismo Pagador deberá cumplir con las siguientes normas:

a) Acceder exclusivamente a los sistemas de información mediante el acceso y los medios autorizados.

b) Proteger la confidencialidad de la información de toda revelación no autorizada.

c) Proteger la integridad de la información del Organismo Pagador a la que tenga acceso en el ámbito de la prestación de los servicios.

d) Proteger la información y los sistemas de información de cualquier alteración no autorizada.

e) Todos los empleados del tercero deben hacerse responsables de la custodia personal de las credenciales que tienen asignadas para el acceso a los recursos de los sistemas de información del Organismo Pagador. Estas credenciales nunca pueden ser facilitadas a terceras personas, sean o no empleados del tercero, y los propietarios de las mismas deben ser únicos responsables del uso que se haga de ellas.

Además el tercero debe poner en marcha medidas de control para garantizar la supervisión de las actuaciones para sus trabajadores.

Octava: Prestación de los servicios en las instalaciones del Organismo Pagador.

El personal del adjudicatario que desempeñe sus funciones en las instalaciones del Organismo Pagador, deberá conocer y cumplir las medidas de seguridad establecidas en el "Manual de responsabilidades de Seguridad de la Información para usuarios". Es responsabilidad del adjudicatario la distribución, cuando sea necesario, de este manual entre sus trabajadores.

Novena: Transmisión de información por parte del tercero a otras entidades.

El adjudicatario no puede transmitir, enviar, compartir o poner a disposición de otras entidades información propiedad del Organismo Pagador, a no ser que de manera previa haya sido expresamente autorizado para hacerlo, independientemente del medio o formato de la información y de su contenido. En el caso de existir dicha autorización se deberá velar por el cumplimiento de las siguientes normas:

a) Deben extenderse al receptor de la información todas las obligaciones del adjudicatario en materia de Seguridad de la Información impuestas por el Organismo Pagador.

b) El adjudicatario será responsable del uso y protección de la información del Organismo Pagador que le haya sido proporcionada, así como de los perjuicios ocasionados al Organismo Pagador en los casos en los que la seguridad de la información hubiera sido comprometida.

c) Se podrá transmitir única y exclusivamente la información estrictamente necesaria para que el adjudicatario autorizado pueda llevar a cabo su cometido.

d) La información sólo podrá ser transmitida a los destinatarios autorizados, que han de estar unívocamente identificados, y por medios que garanticen la identidad del destinatario.

e) En la transmisión de la información se deben aplicar mecanismos que imposibiliten el acceso a ella por parte de otras entidades no autorizadas. Igualmente en el almacenamiento de la información en dispositivos portátiles o extraíbles se deben aplicar mecanismos que imposibiliten dichos accesos.

Décima: Protección del equipamiento informático.

En todo aquel equipamiento informático propiedad del tercero en el cual se almacene, procese o desde el que se acceda a información del Organismo Pagador, el tercero deberá aplicar las medidas de seguridad necesarias para garantizar la confidencialidad, integridad y disponibilidad de dicha información. Al menos, el tercero debe aplicar las siguientes medidas de seguridad:

a) Protección contra código malicioso: todos los equipos deben contar con programas antivirus y de protección ante software malicioso (malware) actualizados de forma automática y permanente.

b) Control de acceso: todos los equipos deben disponer de medidas que aseguren el acceso sólo por parte del personal autorizado.

c) Bloqueo de terminales: no deben dejarse los terminales desatendidos sin antes haber bloqueado la sesión de usuario con el fin de evitar accesos no autorizados. El bloqueo automático tras un periodo de inactividad también debe estar activado.

d) Actualización de sistemas: todo el equipamiento informático debe estar al día con las últimas actualizaciones y parches de seguridad disponibles.

e) Salvaguarda de la información: se han de implementar mecanismos de copia de seguridad y recuperación en aquella información del Organismo Pagador.

f) Privilegios: los usuarios no deben poder deshabilitar o desinstalar las protecciones de seguridad implantadas en los equipos.

El Organismo Pagador se reserva el derecho de exigir la implantación de las medidas de seguridad adicionales que considere oportunas en el equipamiento informático del tercero.

Décimo primera: Seguridad en las instalaciones del tercero.

En aquellas instalaciones, donde se almacene o procese información del Organismo Pagador, el adjudicatario deberá implementar medidas de seguridad física, ambiental y de control de acceso, y todo su personal deberá participar activamente en la implantación y cumplimiento de estas medidas.

Décimo segunda: Continuidad del servicio.

El adjudicatario deberá definir e implementar medidas y estrategias que garanticen la continuidad de los servicios prestados al Organismo Pagador en caso de contingencia.

Así mismo, si la naturaleza del servicio prestado lo requiere, el tercero deberá establecer planes de recuperación de los sistemas que sirvan para la prestación de los servicios al Organismo Pagador, en el caso que éstos sean comprometidos por pérdida, alteración o interrupción.

El Organismo Pagador deberá tener conocimiento de las medidas implantadas por el tercero y destinadas a garantizar la continuidad de los servicios. El Organismo Pagador se reserva el derecho de exigir al tercero medidas de continuidad adicionales cuando los requisitos de continuidad de los servicios prestados así lo requieran.