



## **NOTA LEGAL PARA APECDATA RELATIVA A LOS POSIBLES INCUMPLIMIENTOS EN MATERIA DE PROTECCIÓN DE DATOS DE LOS PLIEGOS ADMINISTRATIVOS**

### **1. Antecedentes.**

La contratación de servicios de *cloud computing* a empresas estadounidenses como, por ejemplo, Google Cloud, Microsoft Azure o Amazon Web Services, representa una problemática jurídica, dado que puede suponer la realización de transferencias internacionales de datos a terceros países que carecen de un nivel adecuado de protección en materia de protección de datos en especial, cuando dichas transferencias se realizan a Estados Unidos de América, que ofrece una protección insuficiente, tal y como fue declarada por el Tribunal de Justicia de la Unión Europea en el Asunto Schrems II<sup>1</sup>.

### **2. Cuestión planteada.**

APECDATA solicita la elaboración de la presente nota legal para conocer los requisitos en materia de protección de datos que se incluyen en los pliegos de licitación de contratación de *servicios cloud* de las Administraciones Públicas y, a su vez, la identificación los posibles incumplimientos en este ámbito a los fines de que puedan ser trasladados a los Delegados de Protección de Datos de los Ayuntamientos los aspectos de protección de datos y seguridad de la información que deben tener en cuenta para la contratación de dichos servicios.

### **3. Análisis, recomendaciones y conclusiones.**

#### **3.1. Análisis.**

Tras la revisión de los pliegos administrativos referidos a servicios de *cloud computing* publicados en la Plataforma de Contratación del Sector Público, es preciso efectuar un análisis de los mismos con el objeto de desgarnar los requisitos en materia de protección de datos y de seguridad de la información para la contratación de los servicios.

#### **3.1.1. Licitación de la Dirección General de la Entidad Valenciana de Vivienda y Suelo (EVHA). - 2022**

---

1

<https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=9853523>

En fecha 7 de octubre de 2022, se publicó la licitación para un contrato de “*Implantación de una réplica en la nube de la copia de seguridad del entorno de producción actual de la EVHA*” con plazo de ejecución de tres años y valor estimado del contrato de 29.000 euros.

En las bases de dicha licitación se detallan los requisitos técnicos a cumplir en materia de seguridad de la información por los adjudicatarios, que son los siguientes: (i) Disponer del Data Protection Credential del fabricante del equipamiento actual de repositorio de backup. Nivel partner Gold en vigor del fabricante del equipamiento actual; (ii) Certificación del Esquema Nacional de Seguridad (ENS) de nivel medio; (iii) Certificado ISO/IEC 27001 de gestión de seguridad de la información; (iv) Certificado ISO/IEC 27017 de controles de seguridad para servicios en la nube y (v) Certificado ISO/IEC 27018 de gestión de privacidad para servicios en la nube.

En relación con la protección de datos, no se realiza ninguna mención en el pliego de condiciones técnicas ni en el de cláusulas administrativas.

Por último, según el acta de adjudicación de fecha 25 de noviembre de 2022, al no haberse recibido ninguna oferta, se declara la licitación desierta.

### **3.1.2. Licitación de la Fundación Internacional y para Iberoamérica de Administración y Políticas Públicas F.S.P. - 2022**

Con fecha 7 de octubre de 2022, se publica la licitación para un contrato de “*Servicios de Cloud Computing para VPS y Aplicaciones Web*” de la propia Fundación. Se prevé una duración inicial del contrato de doce meses, aunque caben tres prórrogas, mientras que el presupuesto del contrato sin impuestos asciende a 73.140 euros.

Así mismo, existen unos requisitos obligatorios para los licitadores, de manera que no podrán concurrir a la licitación, si no disponen de los siguientes certificados referidos a la seguridad de la información: Certificación ISO 27001: Sistema de Gestión de la Seguridad de la Información (SGSI), o equivalente y Certificación en vigor durante toda la duración del contrato de Conformidad con el ENS (Esquema Nacional de Seguridad), categoría Media o Alta para los servicios gestionados ofertados.

No obstante, en cuanto a la protección de datos, no se establece ninguna exigencia aplicable a los licitadores.

Finalmente, conforme al acta de resolución de la licitación de 30 de noviembre de 2022, la misma ha quedado desierta.

### **3.1.3. Licitación de Grecnia de Personas y Ciudad, S.A Unipersonal del Ayuntamiento de San Juan de Alicante. - 2022**

Con fecha 8 de agosto de 2022, se publica el anuncio de adjudicación de un contrato de “*Sistema de almacenamiento y trabajo con archivos en la nube*”, según el cual, el adjudicatario es una PYME denominada DATAPRIUS S.L. Además, el plazo de ejecución del contrato es de cinco años, mientras que su valor estimado es de 3.168 euros, pero no se proporciona más información.

El contrato fue negociado sin publicidad y, por ello, el número de ofertas recibidas ha sido sólo uno. A este respecto, cabe señalar el artículo 118.1 de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público (LCSP), según el cual, los contratos de servicios de valor estimado inferior a 15.000 euros tienen la consideración de contratos menores con la consecuencia de no se exige la publicación de una licitación para la adjudicación de dichos contratos ni los pliegos. Además, el artículo 131.3 de la LCSP prevé la adjudicación directa del contrato sin la previa tramitación de un procedimiento de licitación.

#### **3.1.4. Licitación de Dirección de Suma Gestión Tributaria de la Diputación de Alicante. - 2022**

Con fecha 5 de agosto de 2022, se publica la licitación para un contrato de “*Suministro y servicios para la renovación del sistema de almacenamiento de datos de SUMA Gestión Tributaria de la Diputación de Alicante*” cuyo valor estimado es de 370.000 euros y la duración será de cuarenta meses.

Por otro lado, las condiciones generales de los pliegos de prescripciones técnicas establecen que “*la información a la que tenga acceso la persona adjudicataria como consecuencia del contrato tendrá un carácter confidencial*” y, además, “*no podrá transferir información alguna sobre los trabajos a terceras personas o entidades sin el consentimiento expreso y por escrito de Suma*”, de conformidad con lo previsto en el Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD), y 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 (RGPD).

Sin embargo, no se hace referencia a ninguna otra disposición en materia de protección de datos.

Igualmente, según dichas condiciones generales, se debe garantizar el cumplimiento de los principios básicos y requisitos mínimos requeridos para una protección adecuada de la información que constituyen el ENS.

Por otra parte, el día 2 de enero de 2023 se publica el anuncio de adjudicación en el que se recoge que la licitación se ha adjudicado a una PYME (LYNX VIEW S.L.), dado que ha obtenido la puntuación más alta en la valoración en su conjunto de calidad técnica.

#### **3.1.5. Licitación de la Alcaldía del Ayuntamiento de Algeciras. - 2022**

En fecha 1 de agosto de 2022, se publica un documento de pliegos referido a un contrato cuyo objeto es la creación de una “*Nube privada en el centro de proceso de datos externos del ayuntamiento de Algeciras*”. Aunque el plazo de ejecución del contrato es de un año, se admiten tres prórrogas. Y, en relación con el valor estimado del contrato, éste asciende a 432.000 euros.

En cuanto a los pliegos de condiciones técnicas, éstos establecen de forma expresa unas exigencias referidas a la protección de datos y, en concreto, al tratamiento de datos personales realizado por el adjudicatario ha de observar lo previsto en el RGPD así como la LOPDGDD. A su vez, el adjudicatario deberá contar con el certificado de cumplimiento del ENS, categoría alta y, además, mantener la confidencialidad de los datos personales mediante la adopción de medidas técnicas y organizativas. Finalmente, la ejecución del contrato por parte del adjudicatario se encuentra condicionada a que éste presente una declaración en la que señale la ubicación de sus servidores y desde dónde se prestarán los servicios, aunque, en cualquier caso, debe respetar la normativa vigente de protección de datos.

De acuerdo con el anuncio de adjudicación de fecha 10 de enero de 2023, INETUM ESPAÑA, S.A. es el adjudicatario de la licitación, debido a que la entidad había presentado la oferta más ventajosa para los intereses municipales.

### **3.1.6. Licitación de la Presidencia del Ente Público Empresarial Puertos Canarios. - 2021**

En fecha 22 de junio de 2021, la Plataforma de Contratación del Sector Público publica el pliego del contrato referido a la “*Implantación de una infraestructura de alojamiento CLOUD, para el alojamiento de los servicios y recursos del Ente Público Puertos Canarios*”. A pesar de que el contrato tendrá una duración inicial de un año, éste puede ser objeto de prórrogas sucesivas hasta un máximo de tres anualidades. Respecto al valor estimado del contrato, se indica que éste es de 102.000 euros.

Según el pliego de prescripciones técnicas, la entidad licitadora debe aportar diferentes certificados relacionados con la seguridad de la información y, en concreto, certificado del cumplimiento del Esquema Nacional de Seguridad, nivel medio, Certificación ISO/IEC 27001, Certificación del titular del Datacenter de no haber sufrido incidentes de seguridad y que los operadores de conectividad en los que se alojan los Datacenter sean miembros de los puntos neutros de intercambio de datos en España (Espanix).

En cuanto a los requisitos referidos a la protección de datos, el pliego de prescripciones técnicas obliga al adjudicatario a mantener la confidencialidad de los datos, incluidos los personales, a los que tenga acceso como consecuencia de la ejecución del contrato. Tampoco cabe la utilización de los datos para un fin distinto del previsto o la cesión de éstos. Incluso, se prevé la obligación del adjudicatario de recabar la autorización de la entidad licitadora en caso de que pretenda subcontratar el servicio.

Finalmente, de conformidad con el anuncio de adjudicación de fecha 2 de noviembre de 2021, el adjudicatario es VELORCIOS S.L., por cuanto que ha planteado la oferta económicamente más ventajosa, si bien cabe señalar que sólo se recibió una oferta en el proceso de licitación.

### **3.1.7. Licitación de la Presidencia de la Diputación Provincial de Palencia. - 2021**

Conforme al anuncio de adjudicación publicado en fecha 16 de abril de 2021, el adjudicatario del contrato referido a “*Servicio de mantenimiento de la Mediateca en la nube y del Software para la gestión integral del video-acta digital*” fue EMCO VIDEO INDUSTRIAL S.L.U. En este caso, el valor del contrato era de 24.000 euros.

Si bien no se publicaron los pliegos de la licitación, el anuncio de adjudicación recoge que los criterios de adjudicación eran exclusivamente económicos. Así mismo, con arreglo a dicho documento, la licitación fue negociada sin publicidad, de modo que sólo se recibió una oferta para la ejecución del contrato.

Consecuentemente, no se estableció ningún criterio en virtud del cual el adjudicatario debía acreditar el cumplimiento de la normativa en materia de protección de datos o, incluso, las garantías respecto a la seguridad de la información.

### **3.1.8. Licitación de la Secretaría General de la Agencia Española del Medicamento y Productos Sanitarios (AEMPS). - 2021**

Con arreglo al documento de pliegos de fecha 5 de abril de 2021, se convoca un proceso de licitación para la adjudicación de un contrato de “*Servicios de Azure en AEMPS*”, cuyo valor estimado del contrato es de 303.448,68 euros y el plazo de ejecución del mismo, de treinta y seis meses.

A su vez, en virtud de la cláusula segunda de los pliegos administrativos particulares de dicha licitación<sup>2</sup>, se pretende contratar un servicio de almacenamiento mayor en la nube utilizando el producto Microsoft Azure, para el procesamiento de datos tanto actuales como futuros. En este sentido, debe destacarse que la AEMPS utiliza dicho producto para determinados proyectos desde hace varios años.

Por otro lado, el pliego de prescripciones técnicas prevé como requisitos obligatorios para concurrir a la licitación: (i) un acuerdo de procesamiento de datos de acuerdo con la Directiva de protección de datos; (ii) cumplimiento con la normativa de seguridad en relación con los servicios prestados y, en particular, con la LOPDGDD así como el ENS; (iii) portabilidad de los datos y (iv) la prestación del servicio mediante la plataforma en la nube de Microsoft

---

<sup>2</sup> [DOC20210331131203HOJA+RESUMEN+AZURE+fda.pdf \(contrataciondelestado.es\)](#)

Azure, bajo la modalidad de Server and Cloud Enrollment (SCE), que cuenta con la certificación del ENS de Nivel Alto.

En relación con lo anterior, resulta sorprendente, o cuanto menos llamativo, que se exija el acuerdo de procesamiento de datos de acuerdo con la Directiva 95/46/CE de protección de datos, a pesar de que el artículo 94.1 del RGPD establecía la derogación de la Directiva con efecto a partir del 25 de mayo de 2018.

Por último, el anuncio de adjudicación de fecha 10 de junio de 2021 recoge que se adjudica el contrato a SEIDOR, S.A., puesto que presenta la oferta mejor valorada.

### **3.1.10. Licitación de la Presidencia Ejecutiva de la Agencia E.FE. S.A.U. -2020**

Con fecha 16 de diciembre de 2020, se publica la licitación de un contrato para un “*Servicio cloud de gestión e intercambio de ficheros*” cuyo valor estimado es de 190.125 euros. En este caso, a diferencia de los supuestos expuestos anteriormente, en los criterios de solvencia técnico-profesional se detallan unos referidos a la seguridad de la información y a la protección de datos.

En concreto, se recogen diferentes criterios, entre los que cabe señalar: ISO 270001 (Sistema de gestión de la seguridad de la información), e ISO 27018 (Sistema de gestión de privacidad en la nube y protección de los datos).

Conforme al pliego de cláusulas particulares del contrato, las partes están obligadas al cumplimiento de la LOPDGDD y RGPD. También se prevé la consideración de la entidad adjudicataria como encargada del tratamiento si el objeto del contrato conlleva el acceso a datos personales. En este sentido, se incluye un modelo de contrato de encargado del tratamiento en el pliego cuya suscripción es obligatoria para el órgano de contratación.

Por su parte, el anuncio de adjudicación de fecha 16 de marzo de 2021 establece que el adjudicatario de la licitación es SETESCA BCN S.L., dado que cumple con los requisitos técnicos exigidos y, además, ha presentado la oferta económicamente más ventajosa.

### **3.1.11. Licitación de la Fundación Estatal para la Formación en el Empleo, F.S.P. - 2019**

En fecha 3 de diciembre de 2019, se publica el documento de pliegos para la ejecución de un contrato denominado “*Servicio de Azure backup*” cuyo valor estimado asciende a 16.000 euros, mientras que la duración del mismo es de un año. Además, de conformidad con el documento de especificaciones técnicas<sup>3</sup>, el objeto del contrato era “*asegurar el correcto*

---

3

<https://contrataciondelestado.es/wps/wcm/connect/fb518080-db6b-41e2-ba76-c561a4a2f3fa/DOC20191203082628ETAzurebackup2019+DGE+pdf+firmado.pdf?MOD=AJPERES>

*funcionamiento del servicio de backup (respaldo y recuperación de información) tanto en la infraestructura local, como en Azure backup”.*

En el pliego de cláusulas administrativas particulares se prevé una cláusula sobre protección de datos, en virtud de la cual, las partes se comprometen a cumplir con la normativa vigente en materia de protección de datos y, en particular, se prohíbe: el acceso a datos personales que no estén relacionados con la prestación del servicio; y la cesión, comunicación, revelación o transferencia de los datos personales por parte del personal de la empresa adjudicataria a terceras personas. A pesar de que no se ha estipulado una cláusula sobre seguridad de la información, en la cláusula de protección de datos se recoge el deber de confidencialidad de la entidad adjudicataria.

Finalmente, el adjudicatario del contrato fue Hiberus Sistemas Informáticos, S.L., de acuerdo con el anuncio de adjudicación de 9 de enero de 2020. Respecto al número de ofertas recibidas, éstas fueron solamente dos.

### **3.1.12. Contrato de servicios en modalidad SaaS para la gestión integral de recursos humanos en el Ayuntamiento de Xàtiva - 2021**

El pliego versa sobre la necesidad de contratar servicios SaaS (*Software as a Service*), por un valor de 140.000 euros en materia de Recursos Humanos para mejorar los procesos de gestión administrativa del ayuntamiento, todo ello, en modalidad cloud, permitiendo así, que la gestión del sistema de RRHH se pueda gestionar de forma modular, abierta y flexible, además, se debe integrar en el software en la nube toda la información que gestiona el servicio con la finalidad de agilizar su trabajo diario, todo ello asegurado el cumplimiento de las obligaciones legales pertinentes.

A parte de los requisitos exigidos para los licitadores de solvencia económica y solvencia profesional, los requisitos más relevantes de proveedores de servicios de Cloud Computing que establece el Ayuntamiento, se debe acreditar por parte del licitador:

- Las características mínimas del centro de proceso de datos (CPD)
- Tier III+
- Certificado ISO 27001
- Cumplimiento con el RGPD
- Cumplimiento con el ENS (Esquema Nacional Seguridad) nivel Medio.

### **3.1.13. Contrato de suministro en régimen de alquiler de licencias, en la nube, de protección de datos (antivirus) para el Ayuntamiento de Roquetas de Mar. - julio de 2023**

El objeto del pliego consiste en la adquisición por parte del Ayuntamiento de Roquetas de Mar de de 300 licencias, en la nube, de protección de datos (antivirus), para la mejora de las medidas de seguridad, y evitar así que la información o datos personales de ciudadanos y

trabajadores del Ayuntamiento se vea expuesta debido a fallos de seguridad y por ende, que puedan ser obtenidos de manera ilícita por personas ajenas a su tratamiento.

El objetivo principal, es adquirir un software de protección que sea capaz de evitar cualquier tipo de código malicioso, ya sea que acceda mediante internet, o debido a la mala praxis del usuario.

Estas licencias, en la nube, de protección de datos corporativos basado en la monitorización de las aplicaciones en los End-Point EPP+EDR deberán incluir un sistema de gestión y auditoría de datos de información personal identificable y una plataforma de gestión de la información auditada y reportes avanzados para toda la infraestructura de red del Ayuntamiento de Roquetas de Mar.

Respecto al apartado de Protección de Datos de la licitación establece las condiciones y obligaciones relacionadas con el tratamiento de datos personales por parte del contratista en nombre y por cuenta del ayuntamiento:

- Finalidad de la cesión de datos: Los datos personales se cederán al contratista con el propósito exclusivo de permitir la prestación del servicio del antivirus en la nube.
- Obligaciones del contratista en materia de protección de datos:
  - a) El contratista sólo puede tratar los datos personales para cumplir con la prestación del servicio establecido en el contrato.
  - b) El contratista debe cumplir con la normativa nacional y de la Unión Europea en materia de protección de datos, incluyendo el Reglamento General de Protección de Datos (RGPD) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
  - c) El contratista solo puede utilizar los datos conforme a las instrucciones proporcionadas por el Ayuntamiento y no para otros fines ni comunicarlos a terceros sin consentimiento expreso por escrito del Ayuntamiento.
  - d) El contratista debe mantener en secreto la información relacionada con el contrato y el objeto del mismo.
  - e) Toda la información a la que el contratista tenga acceso debido al contrato debe ser considerada como confidencial.
  - f) Una vez finalizada la relación contractual, se destruirán los datos personales tratados al Ayuntamiento cuando éste lo solicite.



### **3.1.14. Contratación del servicio A2-PRIVCOMP: Software para la gobernanza del dato con garantías de privacidad para servicios cloud-edge - julio 2023**

El Ayuntamiento de Solana, publica un pliego donde se pretende la contratación de un proveedor de Cloud privado para la adaptación y sincronización de las actuales infraestructuras TIC instaladas, así como para la gestión y migración de los sistemas TIC Municipales que posee el ayuntamiento.

Los requisitos que el licitador debe cumplir para la adjudicación del contrato en materia de seguridad de la información es el cumplimiento del Esquema Nacional de Seguridad y el Esquema Nacional de Interoperabilidad, además, debe estar en posesión de la Certificación ISO 27001.

Además, también se exige el cumplimiento del artículo 6.2 de la Ley 11/2022 General de Telecomunicaciones, es decir, el proveedor de Cloud debe estar dado de alta debidamente en la CNMC como un operador de telecomunicaciones y poseer un título habilitante que lo faculte para la prestación de tales servicios.

Respecto al tratamiento de los datos, el pliego establece que el adjudicatario queda expresamente obligado a mantener indefinidamente, absoluta confidencialidad y reserva sobre cualquier dato que pudiera conocer con ocasión del cumplimiento del contrato, en el pliego además, se hace especial hincapié respecto a las obligaciones establecidas en el RGPD como encargado del tratamiento que tendrá que cumplir el licitador.

Por último, se establece que, al finalizar el contrato el adjudicatario procederá a la entrega de los datos a la Administración o, a indicación de esta, a su portabilidad a otra empresa, una vez entregados procederá a su destrucción o borrado seguro en las infraestructuras en que hayan sido almacenados conforme a las normas vigentes.

### **3.1.15 Contratación del alquiler de una Infraestructura como Servicio (IaaS) para el Instituto para la Diversificación y Ahorro de la Energía - junio 2023**

La Entidad Pública Empresarial El Instituto para la Diversificación y Ahorro de la Energía (IDAE) publica un pliego debido a la necesidad de adaptación de la estructura administrativa de IDAE a las nuevas exigencias de volumen y calidad impuesta por el Plan de Recuperación, Transformación y Resiliencia, como consecuencia de esta necesidad, se licitó y adjudicó el alquiler de una infraestructura como servicio (IaaS).

El contratista deberá estar en posesión de las siguientes certificaciones SAP a nivel de IaaS (Infrastructure as a Service) para poder ser admitido al procedimiento:

- SAP Certified in Hosting Services
- ISO 27001
- ITIL Foundation Certificate in IT Service Management
- VMware Certified Professional Data Center Virtualization

- PRINCE2 Foundation Certificate in Project Management

Respecto a las obligaciones en materia de protección de datos, no se menciona ninguna normativa al respecto, sin embargo, intuimos que se hace referencia al RGPD al clasificar al adjudicatario como encargado del tratamiento, y como tal, en el pliego se establecen las obligaciones de:

- 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 del responsable del tratamiento. Si el encargado del tratamiento considera que alguna de las instrucciones infringe el RGPD o cualquier otra disposición en materia de protección de datos de la Unión o de los Estados miembros, el encargado informará inmediatamente al responsable.
- c) Llevar, por escrito, un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta del responsable, que contenga:
  - El nombre y los datos de contacto del encargado/s, responsables o representantes y delegados de protección de datos
  - Las categorías de tratamientos efectuados por cuenta de cada responsable.
  - La información necesaria en caso de transferencias internacionales.
  - Una descripción general de las medidas técnicas y organizativas de seguridad a aplicar
- d) No comunicar los datos a terceras personas, salvo que cuente con la autorización expresa del responsable del tratamiento, en los supuestos legalmente admisibles.

### **3.1.16 Contratación de desarrollo del proyecto colaborativo de UNIDIGITAL: Plataforma Cloud de Interoperabilidad erasmus without papers para el espacio europeo de educación superior - marzo 2023**

El objeto de la publicación de este pliego se debe a la necesidad de desarrollar una “suite ” interoperable para las Universidades que se encuentren en el SUE (Espacio Universitario Europeo) que participen en el programa Erasmus. Para ello, se determina que se debe realizar en una plataforma Cloud, que deberá llevarse a cabo con el hiperescalador propuesto por el proveedor.

Respecto a los requisitos de la seguridad de la información se establece que el licitador debe cumplir con lo dispuesto en el Esquema Nacional de Seguridad, asimismo, el pliego también establece que el prestador del servicio deberá reportar, de manera completa y con la máxima celeridad posible, cualquier incidente de seguridad que tenga relación con el servicio prestado y colaborar activamente en el análisis, tratamiento y resolución de cualquier incidente de seguridad que pueda afectar al servicio prestado.

Respecto a la protección de los datos personales a los que se pueda tener acceso, que se estén contenidos en los Sistemas de Información de las universidades, y el pliego obliga al adjudicatario a mantener absoluta confidencialidad y reserva sobre cualquier dato que pudiera conocer en ocasión del cumplimiento del contrato, este deber se deberá mantener de forma indefinida, incluso más allá de la relación laboral o profesional con la universidad.

Adicionalmente, el pliego establece que la empresa adjudicataria deberá comprometerse por escrito al cumplimiento de las siguientes normas en lo que sean de aplicación a su prestación:

**a)** Acuerdos de confidencialidad al amparo de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

**b)** Reglamento (UE) 2016/679 de 27 de abril (RGPD).

**c)** Real Decreto 3/2010, de 8 de enero (modificada por Real Decreto 951/2015), por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

**d)** Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

### **3.1.17 Contratación de Servicios de Oracle Cloud Infrastructure para los años 2023 a 2025. - julio 2023**

El Organismo Autónomo Provincial de Gestión Tributaria de Toledo con la publicación de esta licitación pretende una transformación global de la arquitectura empresarial de tecnologías de la información de la institución toledana.

El contrato pretende la contratación de un entorno multi-cloud, de manera que se pasará de forma paulatina de una arquitectura fundamentalmente IaaS a una basada en PaaS y SaaS. Se requiere que el adjudicatario adquiera el servicio de "Oracle PaaS and IaaS Universal Credits" para que pueda desplegar los siguientes servicios:

- Oracle Database Service for Azure y sus subservicios.
- Oracle Database Backup Cloud.

Respecto a los requisitos generales en materia de seguridad de información, el pliego establece que el licitador deberá estar en condiciones de exhibir la correspondiente Certificación de Conformidad con el Esquema Nacional de Seguridad de categoría ALTA. Y en caso que el licitador actúe como proveedor de servicios pero que no sea propietario de los sistemas que prestarán los servicios, se aplica la consideración anterior a las entidades y/o sistemas finales prestatarios de los mismos.

Respecto a los requisitos en materia de protección de datos, el pliego únicamente establece que en el tratamiento que el licitador deba realizar en virtud de la prestación de sus servicios, deberá cumplirse según lo dispuesto en el Reglamento (UE) 2016/679 General de Protección de Datos (RGPD), en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) con especial incidencia a lo preceptuado en su Disposición adicional primera, y a la restante normativa que resulte de aplicación.

Por tanto, al tratarse de un proveedor de Cloud, extraemos que cobra especial relevancia las disposiciones relativas al encargado del tratamiento de los datos.

Por último, se establece que la finalidad del tratamiento de los datos personales por parte de la entidad adjudicataria será la de la prestación de los servicios comprendidos en el contrato. El uso de los datos personales para finalidades distintas a las anteriormente indicadas supondrá un incumplimiento por parte de la entidad adjudicataria, lo que podrá dar lugar a la resolución del contrato.

### **3.1.18 Contratación de servicios de instalación y mantenimiento de un cloud privado para espacios de datos, para la ETSI informáticos de la UPM - julio 2023**

La UPM, con el objetivo de impulsar la investigación, la innovación y el desarrollo de infraestructuras en la nube y de borde, así como fomentar la colaboración público-privada, se crea el proyecto “Infraestructura para la INvestigación de ESpacios de DATos distribuidos en UPM (INESData)” subvencionado por la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales (SETELECO)

Con este proyecto se pretende crear una incubadora de espacios de datos y servicios a nivel nacional que haga uso de infraestructuras federadas en la nube y de borde (cloud-edge) y que se rija por mecanismos que garanticen la soberanía de los datos.

En el presente pliego, se combina en un apartado los requisitos en materia de seguridad y de protección de los datos tratados, en cuanto a la seguridad de la información, se exige el cumplimiento del Esquema Nacional de Seguridad, dando especial relevancia al aseguramiento de el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos objeto de la contratación. En el pliego, se hace hincapié en aplicar las medidas de seguridad indicadas en el anexo II del ENS.

Respecto a la protección de los datos, el pliego establece que el licitador deberá cumplir de forma integral del RGPD, haciendo especial mención al cumplimiento del artículo 28 RGPD para lo previsto del encargado del tratamiento, del mismo modo, se exige el cumplimiento íntegro de lo dispuesto en la LOPDGDD.

### 3.1.19 Pliego para la contratación de soluciones Cloud para la continuidad automatizada en RTVE - julio 2023

El propósito del pliego es la contratación de un servicio en la nube por parte de CRTVE que suministre todos los medios materiales y humanos necesarios para la distribución de contenidos hacia operadores y plataformas de emisión y/o su difusión a través de internet, debido que RTVE no dispone del equipamiento necesario ni tampoco de medios técnicos para realizar este servicio.

El servicio que se solicita, deberá recoger y emitir contenidos vía IP, distribuirlos a través de internet a operadores de TV, y proporcionar a RTVE los datos de registro de emisión para su contabilización, donde, este servicio deberá estar operativo *“24x7 de lunes a domingo en bloques de 6 horas diarias repetidos 4 veces al día.”*

Respecto a los requisitos en materia de Seguridad de la Información, no se hace mención alguna en cuanto a normativa que deben cumplir o la posesión de ninguna ISO en materia de ciberseguridad, únicamente se hace un listado de determinadas medidas que el adjudicatario deberá cumplir:

- El acceso a la subida, descargas y/o borrado de dichos contenidos, será mediante usuario y contraseña, diferente para cada suministrador de dichos contenidos.
- Los usuarios y sus contraseñas serán almacenadas y encriptadas.
- Los usuarios en función de cada perfil tendrán acceso a diferentes carpetas contenedoras con derechos independientes de lectura, escritura y borrado de las diversas carpetas.
- Se aportará la seguridad necesaria, en cuanto a disponibilidad de los contenidos por medio de diferentes ubicaciones con contenido redundante y otros medios que pueda implementar el licitador.
- El borrado de dichos ficheros podrá realizarse de forma automática o manual.
- En caso de intento de borrado de un fichero cuya emisión esté prevista en al menos una de las cabeceras, será advertido antes de borrarse.
- En caso de estar en emisión, dicho contenido podrá ser interrumpido y/o sustituido de forma manual.

En cuanto a los requisitos respecto a los datos personales, en el pliego, se requiere que el adjudicatario se comprometa al cumplimiento de todas las obligaciones establecidas en la normativa vigente en materia de Protección de Datos personales y privacidad, tanto para los datos personales que sean facilitados como consecuencia de la participación en la licitación,

como para el tratamiento de los datos facilitados con la finalidad de la adecuada gestión de la relación contractual.

Además, en el pliego se obliga a que el adjudicatario, si la prestación del servicio se realiza a través de sus servidores, la formalización del contrato una declaración indicando la ubicación de los mismos, así como cualquier cambio de ubicación que se produzca durante la ejecución del contrato. Del mismo modo, los licitadores deberán indicar en su oferta si tienen previsto subcontratar los servidores o los servicios asociados a los mismos, relacionando nombre, perfil empresarial y solvencias de dichos subcontratistas.

### **3.1.20 Pliego para la contratación del servicio VPN Cloud siempre conectada para MUTUA MAZ M.C.S.S. N.º 11 - julio 2023**

El objeto del presente pliego persigue garantizar la continuación en la prestación de los servicios y aplicaciones, así como garantizar la continuidad de otros servicios inherentes a los centros dependientes de la Mutua MAZ, Mutua Colaboradora con la Seguridad Social N.º 11, se requiere la contratación de un servicio de VPN Cloud, en modalidad SaaS que pueda gestionar automáticamente la conexión segura a redes públicas.

Se busca que la plataforma en la nube se contrate, sea flexible y escalable para adaptarse a sus necesidades conforme estas cambien.

Los requisitos en materia de protección de datos que exige el pliego, se limita a exigir una declaración de responsabilidad por parte del licitador, sobre el conocimiento de las obligaciones establecidas en el RGPD y LOPDGDD, y por tanto, asume su cumplimiento.

Adicionalmente, se prohíbe al licitador todo uso, tratamiento, reproducción, distribución, comunicación, transformación, manipulación, cesión o transmisión de cualquier tipo de dato o información personal así como la confidencial de empresa, a la que puede indirectamente tener acceso, independientemente del soporte o medio, durante el ejercicio de la labor profesional que venga desarrollando en Mutua MAZ. Además, se establece que en caso que exista una subcontratación por parte del licitador, éstos también deberán cumplir las mismas obligaciones en materia de protección de datos, asumiendo las indemnizaciones que correspondan a la Mutua o a terceros por los daños y perjuicios causados, y que se deriven en caso de incumplimiento.

Por otro lado, respecto a las obligaciones para la Seguridad de la Información, únicamente se obliga al licitador que, en caso de detección de alguna amenaza de seguridad que pudieran afectar a los datos de la Mutua MAZ, deberá comunicarlo al correo electrónico [lopd@maz.es](mailto:lopd@maz.es)

### **3.1.21 Licitación para la contratación del suministro de licencias de una Suite ofimática basada en Cloud Computing por el Ayuntamiento de Costa del Sol. - abril 2023**

Con el objetivo de la promoción, desarrollo, y potenciación de las actividades económicas y sociales en la provincia de Málaga, la sociedad mercantil pública Turismo y Planificación Costa del Sol, S.L.U., para ello en el pliego se establece la necesidad de la contratación del suministro de licencias de una suite ofimática basada en Cloud Computing (SaaS), así como la gestión centralizada desde la nube del directorio activo de Turismo y Planificación Costa del Sol, S.L.U. cuya gestión incluye la implementación de doble factor de autenticación, gestión avanzada de grupos, gestión del directorio activo de la organización, así como la administración de los accesos por parte de los usuarios desde la propia nube, permitiendo a los empleados acceder a los recursos externos e internos a través de la misma.

Respecto a los requisitos en materia de ciberseguridad, el pliego no especifica ninguna norma o ISO que deben cumplir, sin embargo, se especifica una lista de características que se den cumplir para la prestación del servicio:

- El servicio deberá proporcionar antimalware y antispam; con cuarentena y garantizar la monitorización continua contra correo no deseado, virus y correos de suplantación de identidad.
- Se deberá garantizar el cifrado del acceso vía internet, del tránsito entre servidores y del almacenamiento de los buzones.
- Toda la información de los buzones/cuentas y la que pudieran tener asociada deberá estar ubicada íntegramente, y así deberá certificarse, dentro del territorio de la Unión Europea, incluidas la sede o sedes principales y las sedes de respaldo.

En cuanto a la protección de datos de carácter personal, el pliego menciona que el licitador deberá cumplir íntegramente lo establecido en RGPD, además, se estipula que cuando la contratación implique el acceso del contratista a datos de carácter personal, el responsable del tratamiento será Turismo y Planificación Costa del Sol, S.L.U., y el contratista, será el encargado del tratamiento.

En relación con lo expuesto en el párrafo anterior, en el pliego se establece que *“el servicio debe cumplir con la totalidad de la normativa aplicable española y europea sobre datos de carácter personal, en particular los requisitos relativos a la transferencia internacional de datos.”* Debido a que las transferencias internacionales de datos a EE.UU. no se realizan en concordancia con el RGPD, por ese mismo motivo, se requiere que el licitador esté establecido en el territorio europeo.

Por último, se requiere al licitador que, una vez extinguido el contrato, entregue a Turismo y Planificación Costa del Sol, S.L.U., cualquier dato que, como consecuencia de la prestación de servicios, ostente el contratista, asimismo, se establece la prohibición total por parte del contratista destinar los datos a otra finalidad distinta del cumplimiento del contrato.

### **3.1.22 Renovación de licencias y soporte para la solución de seguridad para el acceso a aplicaciones SAAS - julio 2023**

La Entidad Pública Empresarial Renfe, requiere la renovación de 12.500 licencias con el objetivo de establecer una capa de seguridad en el acceso a las aplicaciones SaaS en la nube, concretamente a las aplicaciones “*MVISION Cloud for Shadow IT*”, “*Office 365 Email*”, “*SharePoint and OneDrive*” y “*Teams (Germany Data Center)*”

Hasta el momento, Grupo Renfe cuenta para tal fin el Cloud Access Security Broker (CASB) de McAfee, el cual, tiene la función de llevar un control total y conocer cuáles soluciones en la nube, por ejemplo otros SaaS, tienen acceso a los datos que dispone Grupo Renfe, evitando así el acceso de no autorizado de aplicaciones a los mismos, fenómeno conocido como Shadow IT.

La contratación se realizó por un valor de 225.100€ y fue adjudicada en fecha 20 de agosto de 2023 a la empresa Telefónica Soluciones de Informática y Comunicaciones de España, S.A.

Respecto al cumplimiento normativo, en el pliego de cláusulas administrativas, se dispone de un apartado dedicado a la protección de datos de carácter personal en la prestación del servicio, el cual, aunque no se haga referencia a ninguna normativa, sí se describen las funciones que debe realizar un encargado del tratamiento en adecuación al RGPD.

Se establece que el adjudicatario, tendrá la consideración de responsable del tratamiento, y por ello, se atenderá a las siguientes obligaciones:

- Los datos se deberán tratar siguiendo las instrucciones documentadas del responsable del tratamiento.
- El encargado deberá garantizar que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad de dichos datos.
- Se deberán tomar todas las medidas de seguridad que sean necesarias para garantizar la seguridad de los datos, estas medidas deberán ser apropiadas para garantizar un nivel de seguridad adecuado al riesgo
- Asistir al responsable del tratamiento para que este pueda cumplir con con su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de acceso, rectificación, cancelación, oposición, olvido, portabilidad, limitación del tratamiento, así como el derecho a no ser objeto de una decisión individual automatizada, incluyendo la elaboración de perfiles.

Para ello, se establece que el encargado, debe comunicar al Grupo Renfe a través del correo electrónico [dpd@renfe.es](mailto:dpd@renfe.es) todas las solicitudes de derechos que reciba por parte de los interesados.

- También deberá asistir al responsable del tratamiento en las obligaciones que le corresponden respecto a:



- Implantación de las medidas de seguridad.
- Notificaciones a la AEPD de las violaciones de seguridad de los datos.
- Realización de las EIPD correspondientes, y consultar a la AEPD, cuando a raíz de una EIPD, se determine que un tratamiento de datos entraña alto riesgo.
- Realización de Registros de Actividades del Tratamiento cuando el encargado realice tratamientos de datos que puedan entrañar un riesgo para los derechos y libertades de los interesados, o se traten datos de categoría especial.

Lo más destacable que podemos extraer del pliego, es la referencia que se hace a las transferencias internacionales de datos, las cuales, en todo caso deberán ser autorizadas previamente por el responsable del tratamiento, salvo que exista alguna obligación nacional o europea que obligue a la transferencia.

Las transferencias de datos a terceros países fuera de la unión son delicadas puesto que a la luz del RGPD, muchos estados no tienen la consideración de seguros a menos que dispongan suficientes garantías, como las cláusulas contractuales tipo u otras salvaguardas jurídicas que muestran un compromiso de mantener la seguridad de los datos.

Otro punto destacable del pliego, es que Grupo Renfe, establece sanciones en caso de incumplimiento respecto las obligaciones de confidencialidad y protección de datos analizadas, donde se podrá aplicar una penalización de hasta el 20 % del importe total del contrato en función de la gravedad del incumplimiento.

### **3.1.23 Renovación y ampliación del clúster IaaS en modo nube privada de entornos de desarrollo y laboratorios para INCIBE - julio 2023**

INCIBE pretende la renovación y aplicación del clúster IaaS en modo nube privada utilizada para entornos de desarrollo y laboratorios, así como la ampliación de capacidad debido al crecimiento de INCIBE por el valor de 556.943,68 Euros.

La empresa contratista debe suministrar licencias y suscripciones de los siguientes servicios:

- Renovación del clúster IaaS en modo nube privada.
- Servicio de actualización del clúster.
- Servicio de validación del clúster
- Ampliación de las capacidades que hay actualmente.
- Formación y workshops técnicos
- Soporte técnico y mantenimiento.

Se establece en el pliego, que la ejecución del contrato tiene implícito el cumplimiento legal por parte del contratista de toda normativa española y europea en materia de protección de datos que sea de aplicación a las tareas objeto del contrato.

Se establece que a los efectos de este contrato, INCIBE tendrá la consideración de responsable del tratamiento, mientras que el adjudicatario tendrá la consideración de Encargado del Tratamiento, por tanto, todo tratamiento que realice el adjudicatario se realizará en virtud del artículo 28 del RGPD., por lo que el contratista deberá implementar mecanismos para garantizar r la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento de datos de carácter personal a los que tenga acceso para la ejecución del contrato, verificar, evaluar y valorar, de forma regular, la eficacia de las medidas técnicas y organizativas implantadas para garantizar la seguridad del tratamiento y seudonimizar los datos personales cuando corresponda.

Cuando una persona ejerza un derecho (de acceso, rectificación, supresión y oposición, limitación del tratamiento, portabilidad de datos y a no ser objeto de decisiones individualizadas automatizadas, u otros reconocidos por la normativa aplicable, ante el Encargado del Tratamiento, éste debe comunicarlo a INCIBE con la mayor prontitud.

INCIBE autoriza expresamente a que el contratista, si en la ejecución del contrato precisa recabar datos de los usuarios del servicio que sean de carácter personal según el citado Reglamento pueda tratarlos de acuerdo con lo que se determina para el encargado de tratamiento.

Por último, se establece que si el encargado del tratamiento realiza algún tratamiento de datos contrario a sus obligaciones contractuales o normativas, en dicho tratamiento, será considerado como Responsable del Tratamiento, por lo que responderá personalmente de las infracciones que haya incurrido.

En materia de seguridad de la información se exige que el proveedor de servicios que se contrate, establezca una gestión proactiva de los posibles problemas en materia de ciberseguridad que puedan surgir, en conformidad con el ENS. Asimismo INCIBE se reserva el derecho de examinar por medio de auditores, externos o propios, el nivel de cumplimiento del contratista en materia de seguridad de la información.

### **3.1.24 Servicio de migración a un modelo SAAS en Cloud para Mutua Balear - junio 2023**

La licitación emitida por la Mutua Balear, con un valor de 537.502,89€ tiene por objeto la migración de la antigua plataforma que usaba la mutua (META4) con la que se realizaban procesos asociados con la gestion y administracion de recursos humanos de la Mutua, a una solución en la nube SaaS que permita estas mismas funciones, así como una migración de datos de la antigua plataforma.

La solución en la nube deberá permitir:

- Gestionar los procesos de HR de forma integrada (RR.HH, Talento y Nómina).
- Mejorar las actuales aplicaciones a nivel operativo y funcional.

- Optimizar los procesos actuales de Administración de Personal y Nómina para una gestión más eficiente y productiva del proceso operativo.
- Evolucionar hacia áreas más estratégicas de Recursos Humanos.

La migración de plataforma, se realizará para un mínimo de 550 empleados, un máximo de 680 empleados mensuales, y se deberá disponer de un total de 10 administradores del servicio de recursos humanos.

Se solicita que la solución en la nube que se proponga, sea escalable, rápida y eficaz, que permita dotar al entorno de la flexibilidad necesaria para crecer de forma puntual, tanto en la capacidad de proceso de los servidores, así como en el caudal de las comunicaciones, y dar una respuesta adecuada frente a acontecimientos extraordinarios que desborden la operativa habitual de la misma.

Respecto a los requisitos normativos en materia de seguridad de la información que exige el pliego encontramos únicamente el cumplimiento de la ISO 27001, aunque el pliego enuncia diversos requisitos técnicos, entre ellos se requiere que el proveedor disponga de elementos de seguridad en su hosting basado en firewalls, software antivirus que se actualice frecuentemente en todos los sistemas, que se realicen escaneos internos de seguridad frecuentes con el fin de encontrar intrusiones y evaluar la seguridad y que la plataforma utilice un protocolo seguro para las comunicaciones, así como para la carga y descarga de archivos en la plataforma.

Por último, se requiere que el proveedor tenga la capacidad técnica suficiente para realizar frecuentemente copias de seguridad de los archivos en capas, conservando durante 1 día copias efectuadas cada 4 horas, por 7 días una copia diaria, por 5 semanas una copia semanal, y por 2 años una copia anual, mientras el contrato siga vigente.

En cuanto a la protección de datos, en el pliego se configura un apartado con el nombre de “Cumplimiento RGPD” donde se da a entender que se debe cumplir íntegramente el RGPD en la condición de encargado de tratamiento que tendrá el proveedor. Cabe destacar la mención que se hace en este apartado sobre el alojamiento de los datos, que se requiere que sea en el territorio de la UE, del mismo modo, también se requiere que todos los recursos físicos que se implementen por parte del proveedor, deberán estar situados en el territorio de la UE.

### **3.1.25 Suministro y mantenimiento de la plataforma de virtualización en la nube de escritorio remotos, ordenadores personales e impresoras para los Centros de Acceso Público a Internet, Ayuntamiento de San Sebastián de los Reyes - abril 2023**

El Ayuntamiento de San Sebastián de los Reyes pretende ofrecer servicios digitales a la ciudadanía y facilitar el acceso a las nuevas tecnologías e Internet, para ello, pondrá a disposición del público una serie de dispositivos con conectividad a internet en diferentes

edificios municipales. Para ello, se pretende a través del pliego, que se suministren los equipos hardware, y que los mismos dispongan del software de “*Plataforma Tecnológica en la Nube de Virtualización*” los cuales se distribuyen en los Centros de Acceso Público a Internet (CAPI)

La solución de plataforma virtualizada en la nube, debe basarse en una arquitectura de cliente ligero, con gestión centralizada del mismo en la nube, y su mantenimiento, tanto del hardware como del software corresponderá en todo caso al adjudicatario, mientras que la gestión de los usuarios y la operativa diaria se efectuará por el personal municipal, que a través de internet, se conectarán con los servicios en la nube.

Respecto a los requisitos en materia de protección de datos, el pliego establece que el adjudicatario no realiza ningún tratamiento por cuenta del Ayuntamiento, es decir, el adjudicatario no tiene autorizado el acceso a datos de carácter personal de los que el Ayuntamiento es responsable y no podrá realizar ningún tratamiento independientemente que el adjudicatario tenga la consideración de encargado del tratamiento.

El adjudicatario está obligado al cumplimiento a la normativa vigente en materia de protección de datos de carácter personal Reglamento Europeo (UE) 2016/679 de Protección de Datos Personales y Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, respecto los tratamientos de datos que haga por su cuenta y de los que sea responsable.

Entre las obligaciones del adjudicatario, se establece que este deberá guardar total confidencialidad de los datos referidos al suministro o servicio objeto del contrato. Se prohíbe la subcontratación de las prestaciones que conforman el pliego, salvo que se haya puesto en conocimiento previo del Ayuntamiento, por escrito, con una antelación mínima de 30 días. Asimismo, el adjudicatario está obligado a informar al Ayuntamiento sobre las incidencias o quiebras de seguridad que haya tenido y pudieran afectar a la prestación del contrato.

En materia de seguridad de la información, el Ayuntamiento exige el cumplimiento por parte del adjudicatario la, ISO 20000 relativa al Sistema de Gestión de Servicios de TI, la ISO 27001: Sistema de Gestión de Seguridad de la Información y la ISO 27018: Protección de la Información de Identificación Personal (PII) en Cloud. Asimismo se exige que se disponga de la certificación en el ENS nivel Alto relativo a los servicios Cloud.

### **3.2. Recomendaciones y conclusiones.**

A pesar de que no todos los pliegos analizados<sup>4</sup> incluyen requisitos o condiciones específicos relativos a la protección de datos y a la seguridad de la información, deben destacarse que algunos de ellos incluyen cláusulas relativas al cumplimiento de la normativa vigente en

---

<sup>4</sup> Han sido analizados los pliegos que se han considerado como más relevantes, sin perjuicio que existan otros pliegos que no hemos tenido en consideración para incluirlos en el presente informe.

materia de protección de datos y respecto a la seguridad de la información. Así, por ejemplo, encontramos que algunos pliegos permiten la subcontratación de otras entidades o empresas para la ejecución del contrato, mientras que otros establecen que la subcontratación podrá realizarse bajo la autorización del contratante bajo unas condiciones específicas.

**Este último aspecto es importante dado que si no se incluye un apartado referido a la subcontratación en los pliegos, se admite la posibilidad de efectuar dicha práctica sin contar con el permiso de las Administraciones Públicas** y, por tanto, se podría subcontratar la prestación de servicios de *cloud computing* a terceras empresas, ubicadas fuera de la Unión Europea y, con ello, se produciría el tratamiento de los datos personales en países que no ofrecen un nivel adecuado de protección en esta materia. Sin embargo, a medida que se analizan los pliegos en orden cronológico, encontramos la tendencia que las condiciones son más restrictivas respecto a la subcontratación de los servicios, así como se hace especial hincapié en las ubicaciones de los adjudicatarios como de los subcontratistas, tratando de evitar que se realicen transferencias internacionales a terceros estados catalogados como inseguros por la UE.

De igual forma, del análisis de los pliegos publicados recientemente, se aprecia la exigencia en algunos casos de certificados de cumplimiento tanto del ENS como de estándares internacionales referidos a la seguridad de la información como la ISO 27001.

Por último, es de especial relevancia mencionar que, en materia de protección de datos, es innegociable el cumplimiento con lo establecido en el RGPD relativo a los encargados del tratamiento, cuya función o rol debe ser desempeñada cualquier licitador que sea contratado para la prestación de cualquier servicio de Cloud Computing.

En relación con los encargados del tratamiento, es de vital importancia comprender lo delicadas que son las transferencias internacionales en territorio estadounidense debido que, por el derecho de Estados Unidos, están legitimadas las agencias gubernamentales y de inteligencia para el acceso a tales datos sin limitación alguna y sin necesidad de autorización judicial, algo totalmente contrario al RGPD, **por ello, para cualquier transferencia de datos, es requisito imprescindible, que los contratistas y/o subcontratistas estén establecidos en la Unión Europea.**

Madrid, a 11 de septiembre de 2023

Sor Arteaga  
PhD Doctora en Derecho.  
Abogada colegiada N° 105.096 del ICAM

Especialista en Telecomunicaciones y IT  
Socia de Easy Telecom Law Firm S.L.