



## CONSEJO GENERAL DEL PODER JUDICIAL

En relación al escrito remitido por la Dirección General de Relaciones con la Justicia de la Consejería de Administraciones Públicas, Justicia y Seguridad del Gobierno de Canaria a este Comité de Protección de Datos del Consejo General del Poder Judicial (CGPJ) se procede a informar lo siguiente:

### **ANTECEDENTES**

**PRIMERO.-** Según el escrito presentado por esa Dirección General, mediante resolución de 31 de diciembre de 2018, se ha procedido a adjudicar a la entidad mercantil Accenture S.L, el contrato para la integración del servicio de "textualización" de las grabaciones de juicios en el módulo del puesto de trabajo del juez de las aplicaciones de gestión procesal con presencia en la Comunidad Autónoma de Canarias.

**SEGUNDO.-** Este servicio, desarrollado mediante un motor basado en inteligencia artificial, permitirá realizar la identificación de entidades clave a partir de las transcripciones de los vídeos. Concretamente, nombre y apellidos, direcciones, plazos, fechas, cantidades y referencias jurídicas, lo que supone un tratamiento de datos personales.

**TERCERO.-** Para el desarrollo de este servicio, la empresa adjudicataria Accenture S.L, ha suscrito un acuerdo con la empresa Veritone, para que realice la "textualización" de los datos contenidos en los vídeos, estableciéndose en las cláusulas de privacidad de datos y seguridad de la información, firmadas en el citado acuerdo, que las partes reconocen y acuerdan que el proveedor utiliza una infraestructura en la nube facilitada por Amazon Web Services (AWS) para proporcionar sus servicios y software.

**CUARTA.-** Los servidores de AWS se encuentran localizados dentro de la Unión Europea, por lo que se garantiza que no exista una transferencia internacional de datos.

También se indica que esta plataforma ostenta un certificado de conformidad con el Esquema Nacional de Seguridad y que cumple con el Reglamento General de Protección de Datos, y que por su parte, Accenture S.L no dispondrá de ninguna cuenta de usuario ni de token para acceder al contenido de los archivos multimedia en formato mp3 alojados en la nube ni tampoco al resultado del proceso de transcripción de texto (archivo en formato JSON).



## **CONSEJO GENERAL DEL PODER JUDICIAL**

Respecto a la empresa encargada de prestar este servicio (Veritone), cumplirá con el Reglamento General de Protección de Datos y cifrará toda la información que se transmita, con doble nivel de autenticación.

**QUINTO.-** Puesto que como se ha mencionado anteriormente, este servicio de "textualización" realizará un tratamiento de datos personales, según este escrito, se aconseja solicitar al órgano competente, el Consejo General del Poder Judicial como titular de los datos, la autorización para su tratamiento.

### **CONSIDERACIONES JURÍDICAS**

**PRIMERA.-** El artículo 4 del Reglamento General de Protección de datos define en su apartado 7) al responsable del tratamiento o responsable, como *"la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros"*.

Según el artículo 236 ter de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, los tribunales y juzgados pueden tratar datos personales con fines jurisdiccionales o no jurisdiccionales, de manera que en el primer caso, el tratamiento se limita a los datos en tanto se incorporen a los procesos que se conozcan y su finalidad se relacione directamente con el ejercicio de la potestad jurisdiccional.

En este sentido, la mencionada Ley Orgánica 6/1985, de 1 de julio, en su artículo 236 sexies, determina respecto a los tratamientos con fines jurisdiccionales que el responsable del tratamiento es el órgano jurisdiccional u oficina judicial, y que en el caso de los no jurisdiccionales, esta responsabilidad recae en la oficina judicial correspondiente al órgano judicial con el que se relacionen los datos que a los mismos se incorporen.

En consecuencia, dicha Ley Orgánica establece de forma clara quién es el responsable de los tratamientos en el ámbito de la Administración de Justicia, dependiendo si la finalidad es jurisdiccional o no.



## **CONSEJO GENERAL DEL PODER JUDICIAL**

**SEGUNDA.-** Por lo que se refiere a la posición que ostenta el Consejo General del Poder Judicial, ya que en el escrito de la consulta se cita a este Consejo como “titular de los datos”, respecto a los tratamientos de datos personales que tienen lugar en los órganos jurisdiccionales, la Ley Orgánica 6/1985, de 1 julio, preceptúa en el artículo 236 nonies que las competencias atribuidas a la Agencia Española de Protección de Datos respecto a los tratamientos con fines jurisdiccionales, le corresponden a este Consejo.

Es decir, el Consejo General del Poder Judicial, no es el “titular de los datos” como se afirma en el escrito de consulta, sino que actúa como autoridad de control de protección de datos en relación con los tratamientos de datos con fines jurisdiccionales.

En cambio, cuando el tratamiento de los datos personales no se realice para fines jurisdiccionales, la competencia como autoridad de control corresponde a la Agencia Española de Protección de Datos.

Indicar también que ambas instituciones firmaron el 6 de julio de 2017 un Convenio de Colaboración con el objeto de articular su relación en el ejercicio de la función inspectora en materia de protección de datos sobre los órganos jurisdiccionales.

**TERCERA.-** Una vez expuesto quién actúa como responsable de tratamiento de datos personales en el ámbito de la Administración de Justicia, conforme a los argumentos jurídicos referidos en los apartados anteriores de este informe, procede analizar la relación entre responsable y encargado de tratamiento, ya que del texto de la consulta realizada se desprende la existencia de varios encargados de tratamiento (o sub-encargados).

Para ello, debemos partir del hecho de que en el ámbito de la Administración de Justicia, tanto las Comunidades Autónomas a las que se les ha transferido competencia en esta materia, como el Ministerio de Justicia en aquellas Comunidades que no han recibido esa transferencia, debido a que el ordenamiento jurídico los configura como entes prestacionales ya que deben proveer los medios materiales y personales, a efectos de lo regulado por la normativa de protección de datos, actúan como encargados de tratamiento de datos personales de los órganos jurisdiccionales. Y éstos, cómo anteriormente hemos expuesto, ostentan la condición de responsables de tratamiento.



## CONSEJO GENERAL DEL PODER JUDICIAL

A mayor abundamiento, recordar que la Ley Orgánica 6/1985, de 1 de julio, establece en su artículo 37.1 el siguiente mandato:

*"Corresponde al Ministerio de Justicia o al órgano competente de la comunidad autónoma con competencias en materia de justicia proveer a los juzgados y tribunales de los medios precisos para el desarrollo de su función con independencia y eficacia".*

En este sentido, y siguiendo con el contenido de la consulta planteada por la Dirección General de Relaciones con la Justicia de la Consejería de Administraciones Públicas, Justicia y Seguridad del Gobierno de Canaria, la contratación del servicio de "textualización" se ha adjudicado a la empresa Accenture S.L.

Es decir, esa Dirección General, como encargada de tratamiento, habría acudido a su vez, para prestar este servicio de "textualización", a una empresa (Accenture S.L), que actuaría como encargada (subencargada).

A su vez, la citada empresa (Accenture S.L) recurre a la subcontratación de otras dos entidades empresariales: Amazon Web Services (AWS) y Veritone.

**CUARTA.-** En conexión con lo expuesto en el apartado anterior, el artículo 28 del Reglamento General de Protección de Datos regula la figura del encargado del tratamiento, así como las obligaciones que debe asumir el encargado en relación con el tratamiento de datos personales que vaya a realizar por cuenta del responsable.

Así, y conforme a lo dispuesto en el apartado 3 del artículo 28, deberá existir un contrato u otro acto jurídico que vincule al encargado respecto al responsable, que establezca el objeto, duración, naturaleza y finalidad del tratamiento, tipo de datos personales y categorías de interesados, obligaciones y derechos del responsables, así como otra serie de cuestiones que refleja la norma comunitaria, entre las que podemos destacar, que tratará los datos siguiendo las instrucciones del responsable, la adopción de las medidas necesarias conforme al artículo 32 del RGPD, o que a elección del responsable, una vez finalizada la prestación de



## **CONSEJO GENERAL DEL PODER JUDICIAL**

tratamiento de datos, suprimirá o devolverá los datos, y suprimirá las copias existentes a menos que se requiera la conservación.

Esta regulación de la relación entre el responsable y encargado se completa con lo dispuesto en el artículo 33 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y Garantía de Derechos Digitales.

También procede mencionar el apartado 2 de la Disposición adicional primera de la citada Ley Orgánica 3/2018, de 5 de diciembre, en virtud del cual, *"en los casos en los que un tercero preste un servicio en régimen de concesión, encomienda de gestión o contrato, las medidas de seguridad se corresponderán con las de la Administración pública de origen y se ajustarán al Esquema Nacional de Seguridad"*.

Asimismo, el artículo 122.2 de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014, establece que *"Sin perjuicio de lo establecido en el artículo 28.2 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 la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, en aquellos contratos cuya ejecución requiera el tratamiento por el contratista de datos personales por cuenta del responsable del tratamiento, adicionalmente en el pliego se hará constar:*

- a) *La finalidad para la cual se cederán dichos datos.*
- b) *La obligación del futuro contratista de someterse en todo caso a la normativa nacional de la Unión Europea en materia de protección de datos, sin perjuicio de lo establecido en el último párrafo del apartado 1 del artículo 202.*
- c) *La obligación de la empresa adjudicataria de presentar antes de la formalización del contrato una declaración en la que se ponga de manifiesto dónde van a estar ubicados los servidores y desde dónde se van a prestar los servicios asociados a los mismos.*
- d) *La obligación de comunicar cualquier cambio que se produzca, a lo largo de la vida del contrato, de la información facilitada en la declaración a la que se refiere la letra c) anterior.*
- e) *La obligación de los licitadores de indicar en su oferta, si tienen previsto subcontratar los servidores o los servicios asociados a los mismos, el nombre o el perfil empresarial, definido por referencia a*



## CONSEJO GENERAL DEL PODER JUDICIAL

*las condiciones de solvencia profesional o técnica, de los subcontratistas a los que se vaya encomendar su realización.*

**QUINTA.-** A este respecto, y teniendo en cuenta que como bien se indica en el mencionado escrito de consulta, al implementar este servicio se va a realizar un tratamiento de datos personales, el apartado 2 del artículo 28 del RGPD dispone que *"El encargado del tratamiento no recurrirá a otro encargado sin la autorización previa por escrito, específica o general, del responsable. En este último caso, el encargado informará al responsable de cualquier cambio previsto en la incorporación o sustitución de otros encargados, dando así al responsable la oportunidad de oponerse a dichos cambios"*.

Es decir, para que se pueda realizar la subcontratación del servicio, o en otras palabras, el encargado del tratamiento (o primer subencargado, Accenture S.L), pueda recurrir a otro encargado (concretamente, a otras dos empresas), es necesaria la autorización previa del responsable del tratamiento.

Por tanto, y si se aplicase literalmente el artículo 28.2 del RGPD, cada uno de los juzgados o tribunales que fuese a utilizar este servicio, como responsables del tratamientos de datos con fines jurisdiccionales, tendría que autorizar la subcontratación de dicho servicio.

**SEXTA.-** No obstante lo anterior, si bien la norma europea se aplica a estos tratamientos jurisdiccionales –así se desprende del Considerando 20 cuando se dice que *"Aunque el presente Reglamento se aplica, entre otras, a las actividades de los tribunales y otras autoridades judiciales..."*– debe realizarse una interpretación del contenido del Reglamento General de Protección de Datos que se adecue a la realidad existente en el ámbito de la Administración de Justicia, en el que como indica la Ley Orgánica del Poder Judicial en su artículo 236 sexies, el órgano jurisdiccional actúa como responsable del tratamiento, y por otra parte, existen en virtud de mandato legal, una serie de Administraciones prestacionales que actúan como encargadas de tratamiento, al tener la obligación de facilitar los medios personales y materiales en el ámbito de la Administración de Justicia.

Debido a esta situación, la aplicación del Reglamento al ámbito judicial debe realizarse de forma que mejor respete la participación de cada uno de los agentes involucrados, y por tanto, se ajuste a la actuación efectiva de cada uno de ellos.



## CONSEJO GENERAL DEL PODER JUDICIAL

Así, y a modo de ejemplo, teniendo en cuenta que son las Administraciones prestacionales las encargadas de facilitar los sistemas de gestión procesal, les correspondería a éstas la realización del análisis de riesgos (artículo 24 y 32 del RGPD) o de las evaluaciones de impacto de la protección de datos (artículo 35 RGPD). En este sentido, ya se manifestó este Consejo General del Poder Judicial con ocasión del informe evacuado ante la petición de la Dirección General de Infraestructuras y Sistemas de la Consejería de Justicia e Interior de la Junta de Andalucía en relación la realización de una evaluación de impacto de protección de datos sobre la posible contratación de un servicio telemático de envío de comunicaciones judiciales.

Además, el hecho de que el propio ordenamiento jurídico haya impuesto a las Administraciones prestacionales la obligación de facilitar los medios personales y materiales supone que, a efectos de la contratación de un sub-encargado, lleva implícito que por parte del encargado se designe o contrate con un sub-encargado que cumpla con el RGPD y la LOPDGDD, así como que puedan establecer las condiciones y requisitos de esta sub-contratación, sin necesidad de que se tenga que firmar un acuerdo con un representante de los órganos judiciales, pero respetando la tutela judicial efectiva.

Por lo tanto, si bien no se estima necesaria esa autorización, al menos, y a efectos de la aplicación del principio de transparencia, sí debe comunicarse la citada subcontratación a la Sala de Gobierno del Tribunal Superior de Justicia.

**SÉPTIMA.-** Por otra parte, y una vez analizada la necesidad o no de autorización, procede valorar el mismo a los efectos de lo regulado en el Reglamento General de Protección de Datos.

Según el escrito de la consulta, este nuevo servicio es “capaz de realizar la transcripción de las intervenciones ocurridas durante la grabación de un juicio que esté integrado con el sistema de gestión procesal”. También se indica que “se ha desarrollado un motor basado en inteligencia artificial, que permitirá realizar la identificación de las entidades clave a partir de las transcripciones de los vídeos. En concreto: nombre y apellidos, direcciones, plazos, fechas, cantidades y referencias jurídicas”.



## **CONSEJO GENERAL DEL PODER JUDICIAL**

Procede traer a colación, sin perjuicio del resto de obligaciones que impone el Reglamento General de Protección de Datos a responsables y encargados (obviamente, también a aquellos que actúen como sub-encargados), la posibilidad de que, previamente a que se ponga en marcha un tratamiento de datos de carácter personal, se realice una evaluación de impacto de la protección de datos, puesto que según el artículo 35.1 del Reglamento, *"Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación de impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que no entrañen altos riesgos similares"*.

Asimismo, y respecto al ámbito penal, aunque la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo, no ha sido transpuesta todavía a nuestro ordenamiento jurídico, siendo de aplicación a este ámbito jurisdiccional la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y sobre todo su artículo 22, según lo contemplado por la Disposición transitoria cuarta de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y Garantía de Derechos Digitales, la citada Directiva recoge al respecto:

- 1. Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, suponga un alto riesgo para los derechos y libertades de las personas físicas, los Estados miembros dispondrán que el responsable del tratamiento lleve a cabo, con carácter previo, una evaluación del impacto de las operaciones de tratamiento previstas en la protección de datos personales.*
- 2. La evaluación mencionada en el apartado 1 incluirá, como mínimo, una descripción general de las operaciones de tratamiento previstas, una evaluación de los riesgos para los derechos y libertades de los interesados, las medidas contempladas para hacer frente a estos riesgos, y las garantías, medidas de seguridad y mecanismos destinados a garantizar la protección de los datos personales y a demostrar la conformidad con la*



## **CONSEJO GENERAL DEL PODER JUDICIAL**

*presente Directiva, teniendo en cuenta los derechos e intereses legítimos de los interesados y las demás personas afectadas.*

Si realizamos una comparativa entre lo recogido en el Reglamento General de Protección de Datos y la Directiva 2016/680, que hemos transcrito anteriormente, observamos que ambas normas se alinean en el mismo sentido al contemplar la realización de una evaluación de impacto de la protección de datos en aquellos supuestos en que se vayan a utilizar nuevas tecnologías que supongan un riesgo para los derechos y libertades. En consecuencia, sería conveniente que antes de ponerse en marcha este nuevo servicio se realizase una evaluación de impacto de la protección de datos.

**OCTAVA.-** Por otra parte, en la consulta también se hace referencia a que este servicio se adecua al Reglamento General de Protección de Datos y al Esquema Nacional de Seguridad, si bien, no se presenta documentación al respecto que pueda acreditarlo.

En todo caso, debemos recordar que según el apartado 4 del artículo 28 establece que *"Cuando un encargado del tratamiento recurra a otro encargado para llevar a cabo determinadas actividades de tratamiento por cuenta del responsable, se impondrán a este otro encargado, mediante contrato u otro acto jurídico establecido con arreglo al Derecho de la Unión o de los Estados miembros, las mismas obligaciones de protección de datos que las estipuladas en el contrato u otro acto jurídico entre el responsable y el encargado a que se refiere el apartado 3, en particular la prestación de garantías suficientes de aplicación de medidas técnicas y organizativas apropiadas de manera que el tratamiento sea conforme con las disposiciones del presente Reglamento. Si ese otro encargado incumple sus obligaciones de protección de datos, el encargado inicial seguirá siendo plenamente responsable ante el responsable del tratamiento por lo que respecta al cumplimiento de las obligaciones del otro encargado"*.

Para ello, si por parte de esa Comunidad Autónoma lo considera puede utilizar el modelo que se aporta junto con este informe en el Anexo I, a los efectos de cumplir con lo anteriormente transcrito.

En consecuencia, y a la vista de la argumentación jurídica esgrimida procede adoptar las siguientes CONCLUSIONES:

**PRIMERA.-** No corresponde a este Consejo General del Poder Judicial autorizar la subcontratación del servicio de "textualización", a los efectos de



## **CONSEJO GENERAL DEL PODER JUDICIAL**

un encargado de tratamiento recurriendo a otro encargado, ya que el Consejo no actúa como responsable de tratamientos en el ámbito jurisdiccional, sino como autoridad de control, no siéndole aplicable, por tanto, lo dispuesto en el artículo 28.2 del RGPD.

**SEGUNDA.-** No es necesaria la autorización de cada uno de los órganos jurisdiccionales que actúan como responsables de tratamiento para realizar la subcontratación del mencionado servicio, si bien deberá comunicarse por esa Dirección General a la Sala de Gobierno del Tribunal Superior de Justicia a los efectos de que tengan conocimiento de la puesta en marcha de este nuevo servicio, así como de las contrataciones realizadas para su ejecución.

**TERCERA.-** Las empresas subcontratas para la prestación del servicio de transcripción (“textualización”) al realizar un tratamiento de datos personales deberán cumplir lo regulado tanto en el Reglamento General de Protección de Datos como en la Ley Orgánica 3/2018, de 5 de diciembre, pudiendo utilizarse para este fin, las cláusulas que se incorporan a este informe como Anexo.

**CUARTA.-** Por último, y antes de que se ponga en funcionamiento este nuevo servicio, por esa Dirección General podría realizarse, con la finalidad de garantizar la seguridad y evitar que el tratamiento de datos personales de este nuevo servicio vulnere la normativa vigente, una evaluación de impacto de la protección de datos.

### **MODELO DE CLÁUSULAS PARA CONTRATOS DE ENCARGADOS DE TRATAMIENTO REALIZADO POR LAS ADMINISTRACIONES PRESTACIONALES EN EL ÁMBITO DE LA ADMINISTRACIÓN DE JUSTICIA**

#### ***Introducción***

La Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial (LOPJ) configura como responsable de los tratamientos de carácter jurisdiccional, a los Juzgados u Oficina Judicial “ante el que se tramiten los procesos cuyos datos se incorporen al fichero” y a la Oficina Judicial correspondiente del órgano judicial como responsable de los que no ostentan tal carácter (artículo 236 sexies apartado 1 de la LOPJ).

En el ámbito de la Administración de Justicia, destaca la existencia de encargados de tratamiento en virtud del traspaso de competencias



## **CONSEJO GENERAL DEL PODER JUDICIAL**

efectuado a las Comunidades Autónomas, además del Ministerio de Justicia respecto a aquellas Comunidades a las que no se ha realizado dicho traspaso.

Así, puesto que tanto las Comunidades Autónomas con competencias transferidas como el Ministerio de Justicia en las que no se ha realizado el mencionado traspaso, deben proveer de los medios personales y materiales en este ámbito, a efectos de la protección de datos personales, actúan respecto a los juzgados y tribunales como encargados de tratamiento.

Se trata, por tanto, de la existencia de encargados de tratamiento que vienen clasificados como tales por el ordenamiento jurídico en función de esa provisión anteriormente referida.

Si bien no existe un contrato de encargado de tratamiento, con el contenido del artículo 28.3 del Reglamento General de Protección de Datos (RGPD), entre los responsables (Juzgados y Tribunales) y las Comunidades Autónomas y Ministerio, puesto que no es necesario al tratarse de un encargado de tratamiento que viene impuesto por el ordenamiento jurídico (competencias asumidas por los Estatutos de Autonomía y Reales Decretos de transferencia), al amparo de lo dispuesto en el artículo 28.4 del RGPD, sí debe existir el mismo cuando las Comunidades Autónomas y Ministerio contraten con un tercero servicios que afecten a la Administración de Justicia y que supongan un tratamiento de datos personales, pudiendo utilizar para ello las siguientes cláusulas.

## **CONFIDENCIALIDAD Y PROTECCIÓN DE DATOS**

### **1.- Confidencialidad.**

El adjudicatario (sub-encargado) se comprometerá a mantener en secreto todos los datos e informaciones facilitados y que sean concernientes a la prestación del Servicio aquí regulado. En particular, será considerado como Información Confidencial todo el know how o saber hacer resultante de la ejecución de los servicios contratados (los Servicios), debiendo el adjudicatario mantener dicha información en reserva y secreto y no revelarla de ninguna forma, en todo o en parte, a ninguna persona física o jurídica que no sea parte del contrato.

### **2 Protección de datos.**

#### **2.1. Normativa.**



## **CONSEJO GENERAL DEL PODER JUDICIAL**

De conformidad con la Disposición adicional 25ª de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014, los contratos que impliquen el tratamiento de datos de carácter personal deberán respetar en su integridad 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 (RGPD), y la normativa complementaria.

Para el caso de que la contratación implique el acceso del contratista a datos de carácter personal, de cuyo tratamiento la entidad contratante ostenta la consideración de encargado de tratamiento, aquél tendrá también la citada consideración (sub-encargado). En este supuesto, el acceso a esos datos no se considerará comunicación de datos, cuando se cumpla lo previsto en el artículo 28 del RGPD. En todo caso, las previsiones de este deberán de constar por escrito.

### **2.2. Tratamiento de Datos Personales.**

Para el cumplimiento del objeto de este pliego, el adjudicatario (sub-encargado) deberá tratar los datos personales de los cuales (Comunidad Autónoma/Ministerio) es encargado del tratamiento de la manera que se especifica en el Anexo a este pliego, denominado "Tratamiento de Datos Personales". Ello conlleva que el adjudicatario (sub-encargado) actúe también en calidad de Encargado del Tratamiento (de forma más precisa, como Sub-Encargado del Tratamiento) y, por tanto, tiene el deber de cumplir con la normativa vigente en cada momento, tratando y protegiendo debidamente los Datos Personales.

Por tanto, si bien la (Comunidad Autónoma/Ministerio) actúan como encargado de tratamiento asumiendo sus respectivas responsabilidades, también existen las mismas en relación con el adjudicatario (sub-encargado).

En este sentido, si el adjudicatario (sub-encargado) destinase los datos a otra finalidad, los comunicara o los utilizara incumpliendo las estipulaciones del contrato y/o la normativa vigente, será considerado como Responsable del Tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.



Por otra parte, el Anexo "Tratamiento de Datos Personales" describe en detalle los Datos Personales a proteger, así como el tratamiento a realizar y las medidas a implementar por el adjudicatario (sub-encargado). En caso de que como consecuencia de la ejecución del contrato resultara necesario en algún momento la modificación de lo estipulado en el Anexo XXX "Tratamiento de Datos Personales", el adjudicatario (sub-encargado) lo requerirá razonadamente y señalará los cambios que solicita.

En caso de que la (Comunidad Autónoma/Ministerio) estuviese de acuerdo con lo solicitado emitiría un Anexo "Tratamiento de Datos Personales" actualizado, de modo que el mismo siempre recoja fielmente el detalle del tratamiento.

### **2.3 Estipulaciones como Encargado de Tratamiento.**

De conformidad con lo previsto en el artículo 28 apartado 2 en relación con lo dispuesto en apartado 4, ambos del RGPD, el adjudicatario (sub-encargado) se obliga a y garantiza el cumplimiento de las siguientes obligaciones, complementadas con lo detallado en el Anexo "Tratamiento de Datos Personales":

- a) Tratar los Datos Personales conforme a las instrucciones documentadas o demás documentos contractuales aplicables a la ejecución del contrato y aquellas que, en su caso, reciba de la (Comunidad Autónoma/Ministerio) por escrito en cada momento. El adjudicatario (sub-encargado) informará inmediatamente a la (Comunidad Autónoma/Ministerio) cuando, en su opinión, una instrucción sea contraria a la normativa de protección de Datos Personales aplicable en cada momento.
- b) No utilizar ni aplicar los Datos Personales con una finalidad distinta a la ejecución del objeto del Contrato.
- c) Tratar los Datos Personales de conformidad con los criterios de seguridad y el contenido previsto en el artículo 32 del RGPD, así como observar y adoptar las medidas técnicas y organizativas de seguridad necesarias o convenientes para asegurar la confidencialidad, secreto e integridad de los Datos Personales a los que tenga acceso, y adoptar lo previsto en el Esquema Nacional de Seguridad.

En particular, y sin carácter limitativo, se obliga a aplicar las medidas de protección del nivel de riesgo y seguridad que correspondan.



## **CONSEJO GENERAL DEL PODER JUDICIAL**

d) Mantener la más absoluta confidencialidad sobre los Datos Personales a los que tenga acceso para la ejecución del contrato así como sobre los que resulten de su tratamiento, cualquiera que sea el soporte en el que se hubieren obtenido. Esta obligación se extiende a toda persona que pudiera intervenir en cualquier fase del tratamiento por cuenta del adjudicatario (sub-encargado), siendo deber del adjudicatario (sub-encargado) instruir a las personas que de él dependan, de este deber de secreto, y del mantenimiento de dicho deber aún después de la terminación de la prestación del Servicio o de su desvinculación.

e) Llevar un listado de personas autorizadas para tratar los Datos Personales objeto de este pliego y garantizar que las mismas se comprometen, de forma expresa y por escrito, a respetar la confidencialidad, y a cumplir con las medidas de seguridad correspondientes, de las que les debe informar convenientemente. Y mantener a disposición de la (Comunidad Autónoma/Ministerio) dicha documentación acreditativa.

f) Garantizar la formación necesaria en materia de protección de Datos Personales de las personas autorizadas a su tratamiento.

g) No comunicar (ceder) ni difundir los Datos Personales a terceros, ni siquiera para su conservación.

h) Nombrar Delegado de Protección de Datos, en caso de que sea necesario según el RGPD y la LOPDGDD, y comunicarlo a la Agencia Española de Protección de Datos. También realizará esta acción cuando haya sido designado de forma voluntaria.

i) Una vez finalizada la prestación contractual objeto del presente Pliego, se compromete, según corresponda y se instruya en el Anexo "Tratamiento de Datos Personales", a devolver o destruir (i) los Datos Personales a los que haya tenido acceso; (ii) los Datos Personales generados por el adjudicatario (sub-encargado) por causa del tratamiento; y (iii) los soportes y documentos en que cualquiera de estos datos consten, sin conservar copia alguna; salvo que se permita o requiera por ley o por norma de derecho comunitario su conservación, en cuyo caso no procederá la destrucción.

El adjudicatario (sub-encargado) podrá, no obstante, conservar los datos durante el tiempo que puedan derivarse responsabilidades de su relación con el Encargado del Tratamiento. En este último caso, los Datos



## **CONSEJO GENERAL DEL PODER JUDICIAL**

Personales se conservarán bloqueados y por el tiempo mínimo, destruyéndose de forma segura y definitiva al final de dicho plazo.

j) Según corresponda y se indique en el Anexo "Tratamiento de Datos Personales, a llevar a cabo el tratamiento de los Datos Personales en los sistemas/dispositivos de tratamiento, manuales y automatizados, y en las ubicaciones que en el citado Anexo se especifican, equipamiento que podrá estar bajo el control de la (Comunidad Autónoma/Ministerio) bajo el control directo o indirecto del adjudicatario (sub-encargado), u otros que hayan sido expresamente autorizados por escrito por la (Comunidad Autónoma/Ministerio), según se establezca en dicho Anexo en su caso, y únicamente por los usuarios o perfiles de usuarios asignados a la ejecución del objeto de este Pliego.

k) Salvo que se indique otra cosa en el Anexo "Tratamiento de Datos Personales" o se instruya así expresamente por la (Comunidad Autónoma/Ministerio), a tratar los Datos Personales dentro del Espacio Económico Europeo u otro espacio considerado por la normativa aplicable como de seguridad equivalente, no tratándolos fuera de este espacio ni directamente ni a través de cualesquiera subcontratistas autorizados conforme a lo establecido en este Pliego o demás documentos contractuales salvo que esté obligado a ello en virtud del Derecho de la Unión o del Estado miembro que le resulte de aplicación.

En el caso de que por causa de Derecho nacional o de la Unión Europea el adjudicatario (sub-encargado) se vea obligado a llevar a cabo alguna transferencia internacional de datos, el adjudicatario (sub-encargado) informará por escrito a la (Comunidad Autónoma/Ministerio) de esa exigencia legal, con antelación suficiente a efectuar el tratamiento, y garantizará el cumplimiento de cualesquiera requisitos legales que sean aplicables a la (Comunidad Autónoma/Ministerio), salvo que el Derecho aplicable lo prohíba por razones importantes de interés público.

l) De conformidad con el artículo 33 RGPD, comunicar a la (Comunidad Autónoma/Ministerio), de forma inmediata y a más tardar en el plazo de 72 horas, cualquier violación de la seguridad de los datos personales a su cargo de la que tenga conocimiento, juntamente con toda la información relevante para la documentación y comunicación de la incidencia o cualquier fallo en su sistema de tratamiento y gestión de la información que haya tenido o pueda tener que ponga en peligro la seguridad de los Datos Personales, su integridad o su disponibilidad, así como cualquier posible vulneración de la



## **CONSEJO GENERAL DEL PODER JUDICIAL**

confidencialidad como consecuencia de la puesta en conocimiento de terceros de los datos e informaciones obtenidos durante la ejecución del contrato. Comunicará con diligencia información detallada al respecto, incluso concretando qué interesados sufrieron una pérdida de confidencialidad.

m) En los casos en que la normativa así lo exija (ver art. 30.5 RGPD), llevar, por escrito, incluso en formato electrónico, y de conformidad con lo previsto en el artículo 30.2 del RGPD un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de la (Comunidad Autónoma/Ministerio) que contenga, al menos, las circunstancias a que se refiere dicho artículo.

n) Disponer de evidencias que demuestren su cumplimiento de la normativa de protección de Datos Personales y del deber de responsabilidad activa, como, a título de ejemplo, certificados previos sobre el grado de cumplimiento o resultados de auditorías, que habrá de poner a disposición de la (Comunidad Autónoma/Ministerio) a requerimiento de esta.

o) Las obligaciones y prestaciones que aquí se contienen no son retribuíbles de forma distinta de lo previsto en el presente pliego y demás documentos contractuales y tendrán la misma duración que la prestación de Servicio objeto de este pliego y su contrato, prorrogándose en su caso por períodos iguales a éste.

No obstante, a la finalización del contrato, el deber de secreto continuará vigente, sin límite de tiempo, para todas las personas involucradas en la ejecución del contrato. Para el cumplimiento del objeto de este pliego no se requiere que el adjudicatario (sub-encargado) acceda a ningún otro Dato Personal, y por tanto no está autorizado en caso alguno al acceso o tratamiento de otro dato, que no sean los especificados en el Anexo "Tratamiento de Datos Personales.

Si se produjera una incidencia durante la ejecución del contrato que conllevara un acceso accidental o incidental a Datos Personales no contemplados en el Anexo "Tratamiento de Datos Personales el adjudicatario (sub-encargado) deberá ponerlo en conocimiento de la (Comunidad Autónoma/Ministerio de Justicia), en concreto a su Delegado de Protección de Datos, con la mayor diligencia y a más tardar en el plazo de 72 horas.



## **CONSEJO GENERAL DEL PODER JUDICIAL**

p) Cuando el pliego permita la subcontratación de actividades objeto del pliego, y en caso de que el adjudicatario (sub-encargado) pretenda subcontratar con terceros la ejecución del contrato y el subcontratista, si fuera contratado, deba acceder a Datos Personales, el adjudicatario (sub-encargado) lo pondrá en conocimiento previo de la (Comunidad Autónoma/Ministerio), identificando qué tratamiento de datos personales conlleva, para que se decida, en su caso, si otorgar o no su autorización a dicha subcontratación.

En todo caso, para autorizar la contratación, es requisito imprescindible que se cumplan las siguientes condiciones (si bien, aun cumpliéndose las mismas, corresponde a la (Comunidad Autónoma/Ministerio) la decisión de si otorgar, o no, dicha autorización):

- Que el tratamiento de datos personales por parte del subcontratista se ajuste a la legalidad vigente, lo contemplado en este pliego y a las instrucciones de la (Comunidad Autónoma/Ministerio).
- Que el adjudicatario (sub-encargado) y la empresa subcontratista formalicen un contrato de encargo de tratamiento de datos en términos no menos restrictivos a los previstos en el presente pliego, el cual será puesto a disposición de la (Comunidad Autónoma/Ministerio) a su mera solicitud para verificar su existencia y contenido. El adjudicatario (sub-encargado) informará a la (Comunidad Autónoma/Ministerio) de cualquier cambio previsto en la incorporación o sustitución de otros subcontratistas, dando así a la (Comunidad Autónoma/Ministerio) la oportunidad de otorgar el consentimiento previsto en esta cláusula. La no respuesta de la (Comunidad Autónoma/Ministerio) a dicha solicitud por el contratista equivale a oponerse a dichos cambios.

### **ANEXO "TRATAMIENTO DE DATOS PERSONALES"**

Descripción general del tratamiento de Datos Personales a efectuar:

El tratamiento consistirá en: (descripción detallada del servicio y del tratamiento). Especificar de acuerdo con el artículo 28.3 RGPD naturaleza, finalidad, objeto del tratamiento:

El personal adscrito por la organización adjudicataria, para proporcionar los Servicios establecidos en el Pliego puede tratar Datos Personales. Los Datos Personales se tratarán únicamente por el personal adscrito y al único fin de efectuar el alcance contratado. En caso de que



**CONSEJO GENERAL DEL PODER JUDICIAL**

como consecuencia de la ejecución del contrato resultara necesario en algún momento la modificación de lo estipulado en este Anexo, el adjudicatario (sub-encargado) lo requerirá razonadamente y señalará los cambios que solicita. En caso de que la (Comunidad Autónoma/Ministerio) estuviese de acuerdo con lo solicitado, emitirían un Anexo actualizado, de modo que el mismo siempre recoja fielmente el detalle del tratamiento.

Colectivos y Datos Tratados

Los colectivos de interesados y Datos Personales tratados a las que puede tener acceso el adjudicatario (sub-encargado) son:

Colectivos de interesados afectados por el tratamiento de datos	(Determinar colectivos)
Tratamiento de datos	(Determinar el tipo de datos a tratar) -Pj DNI/NIF; nombre y apellidos; dirección; firma; datos de empleo; datos económico, financieros y seguros-

Elementos del tratamiento

El tratamiento de los Datos Personales comprenderá: (marca lo que proceda):

<input type="checkbox"/> Recogida (captura de datos)	<input type="checkbox"/> Registro (grabación)	<input type="checkbox"/> Estructuración	<input type="checkbox"/> Modificación
<input type="checkbox"/> Conservación (almacenamiento)	<input type="checkbox"/> Extracción (retrieval)	<input type="checkbox"/> Consulta	<input type="checkbox"/> Cesión
<input type="checkbox"/> Difusión	<input type="checkbox"/> Interconexión (cruce)	<input type="checkbox"/> Cotejo	<input type="checkbox"/> Limitación
<input type="checkbox"/> Supresión	<input type="checkbox"/> Destrucción (de copias temporales)	<input type="checkbox"/> Conservación (en sus sistemas de información)	<input type="checkbox"/> Otros:

Disposición de los datos al terminar el Servicio

Una vez finalice el encargo, el adjudicatario (sub-encargado) debe:



## **CONSEJO GENERAL DEL PODER JUDICIAL**

- a) Devolver a la (Comunidad Autónoma/Ministerio) los datos de carácter personal y, si procede, los soportes donde consten, una vez cumplida la prestación. La devolución debe comportar el borrado total de los datos existentes en los equipos informáticos utilizados por el encargado. No obstante, el encargado (sub-encargado) puede conservar una copia, con los datos debidamente bloqueados, mientras puedan derivarse responsabilidades de la ejecución de la prestación. Por otra parte, la (Comunidad Autónoma/Ministerio) podrá requerir al encargado (sub-encargado) para que en vez de la opción a), cumpla con la b) o con la c) siguientes:
- b) Devolver al encargado que designe por escrito la (Comunidad Autónoma/Ministerio), los datos de carácter personal y, si procede, los soportes donde consten, una vez cumplida prestación. La devolución debe comportar el borrado total de los datos existentes en los equipos informáticos utilizados por el encargado (sub-encargado). No obstante, el encargado (sub-encargado) puede conservar una copia, con los datos debidamente bloqueados, mientras puedan derivarse responsabilidades de la ejecución de la prestación.
- c) Destruir los datos, una vez cumplida la prestación. Una vez destruidos, el encargado (sub-encargado) debe certificar su destrucción por escrito y debe entregar el certificado a la (Comunidad Autónoma/Ministerio). No obstante, el encargado (sub-encargado) puede conservar una copia, con los datos debidamente boqueados, mientras puedan derivarse responsabilidades de la ejecución de la prestación.

### Medidas de seguridad

El adjudicatario (sub-encargado) deberá adoptar las medidas necesarias para garantizar la seguridad del tratamiento de los datos personales adaptándose al Esquema Nacional de Seguridad.