



INFORME SOBRE LA SOLICITUD DE ASESORAMIENTO FORMULADA POR LA DIRECCIÓN GENERAL DE INFRAESTRUCTURAS Y SISTEMAS DE LA CONSEJERÍA DE JUSTICIA E INTERIOR DE LA JUNTA DE ANDALUCÍA, EN RELACIÓN CON EL PROYECTO DE CONTRATACIÓN DE UN SERVICIO TELEMÁTICO DE ENVÍO DE NOTIFICACIONES JUDICIALES

I. ANTECEDENTES

Primero.- Por la Dirección General de Infraestructuras y Sistemas de la Consejería de Justicia e Interior de la Junta de Andalucía se ha remitido documentación sobre la realización de una evaluación de impacto de protección de datos sobre la posible contratación de un servicio telemático de envío de comunicaciones judiciales.

Segundo.- Según el citado documento, se han identificado riesgos asociados al posible tratamiento de datos personales, como son: la gestión deficiente de las subcontrataciones e insuficiente control sobre encargados y subcontratistas; y la carencia de medidas de seguridad o aplicación deficiente de las mismas y/o indefinición de funciones de seguridad.

Tercero.- Como consecuencia de lo anteriormente señalado, y al amparo de lo dispuesto en el artículo 36, apartados 1 y 2, del Reglamento General de Protección de Datos, por esa Dirección General se solicita asesoramiento del Consejo General del Poder Judicial, como Autoridad de Control de Protección de Datos en los tratamientos con fines jurisdiccionales.

II. CONSIDERACIONES

Primera.- El Reglamento General de Protección de Datos regula en su artículo 35 la "Evaluación de impacto relativa a la protección de datos", señalando el apartado 1 de este precepto que *"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 del 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 entrañen altos riesgos similares"*.



CONSEJO GENERAL DEL PODER JUDICIAL
Comité de Protección de Datos

Por su parte, el apartado 3 de este mismo precepto establece lo siguiente:

"La evaluación de impacto relativa a la protección de los datos a que se refiere el apartado 1 se requerirá en particular en caso de:

- a) Evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar;*
- b) Tratamiento a gran escala de las categorías de datos especiales a que se refiere el artículo 9, apartado 1, o de los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10;*
- c) Observación sistemática a gran escala de una zona de acceso público".*

Segunda.- Según el apartado 4 del artículo 35, cada autoridad de control debe establecer y publicar una lista de aquellas operaciones de tratamiento que requieran una evaluación de impacto de la protección de datos, comunicando esta lista al Comité Europeo de Protección de Datos.

También existe la posibilidad, de conformidad con el apartado 5 del artículo 35, de que la autoridad de control establezca y publique una lista referida a aquellas actividades de tratamientos que no exijan realizar una evaluación.

Para facilitar la elaboración por parte de cada autoridad de control de protección de datos de los citados listados, el Comité Europeo de Protección de Datos (CEPD) a través del documento "Directrices sobre la evaluación de impacto relativa a la protección de datos -EIPD- y para determinar si el tratamiento entraña probablemente un alto riesgo", señala, atendiendo al contenido del artículo 35.1 y 35.3, los siguientes nueve criterios que probablemente supongan un alto riesgo:

- Evaluación o puntuación, incluida la elaboración de perfiles y la predicción, especialmente de "aspectos relacionados con el rendimiento en el trabajo, la situación económica, la salud, las preferencias o intereses personales, la fiabilidad o el comportamiento, la situación o los movimientos del interesado (considerandos 71 y 91);
- Toma de decisiones automatizada con efecto jurídico significativo o similar. Por ejemplo, que el tratamiento pueda provocar la exclusión o discriminación contra las personas;



CONSEJO GENERAL DEL PODER JUDICIAL
Comité de Protección de Datos

- Observación sistemática con la finalidad de que el tratamiento permita observar, supervisar y controlar a los interesados, incluyendo los datos recogidos a través de redes o una zona de acceso público;
- Datos sensibles o muy personales, entre los que se encontrarían aquellos referidos a las categorías especiales de datos (por ejemplo, datos relativos a opiniones políticas) así como los datos de condenas e infracciones penales;
- Tratamiento de datos a gran escala, que no está definido en el RGPD que se entiende por gran escala, pero que el CEPD recomienda que se valoren estos aspectos:
 - Número de interesados afectados, bien como cifra concreta o como proporción de la población correspondiente;
 - Volumen de datos o variedad de elementos de datos distintos que se procesan;
 - Duración o permanencia de la actividad de tratamiento;
 - Alcance geográfico de la actividad de tratamiento;
- Asociación o combinación de conjuntos de datos, por ejemplo, que procedan de dos o más operaciones de tratamiento de datos realizadas para fines diferentes o por responsables distintos de una manera que exceda las expectativas razonables del interesado.
- Datos relativos a interesados vulnerables (considerando 75), cuando exista un desequilibrio de poder entre los interesados y el responsable del tratamiento, lo cual puede suponer que los interesados sean incapaces de autorizar o denegar el tratamiento de sus datos personales o ejercitar sus derechos. Entre los interesados vulnerables pueden incluirse a niños, empleados, personas con enfermedades mentales, personas mayores, solicitantes de asilo.
- Uso innovador o aplicación de nuevas sociales tecnológicas u organizativas, como podría ser combinar el uso de la huella dactilar con el reconocimiento facial para el control de acceso a unas instalaciones.
- Cuando el propio tratamiento impida a los interesados ejercer un derecho o utilizar un servicio o ejecutar un contrato.



Tercera.- En consonancia con la potestad de las autoridades de control de determinar sobre qué tratamientos se precisa realizar, con carácter previo a su puesta en funcionamiento, una evaluación de impacto de protección de datos, éstas han remitido al Comité Europeo de Protección de Datos los correspondientes listados en los que se reflejan este tipo de tratamientos, y que serían, entre otros, los siguientes:

- Monitorización de empleados (requiere siempre una evaluación de impacto al tratarse de sujetos vulnerables y un tratamiento sistemático);
- Datos biométricos (por sí sólo no representa necesariamente un alto riesgo, pero si se le une otro criterio de los descritos, entonces sí sería necesaria la evaluación de impacto);
- Datos genéticos (aplicable la misma regla que la descrita para los datos biométricos);
- Datos de localización (aplicable la misma regla que la descrita para los datos biométricos);
- Tratamiento para fines científicos o históricos sin consentimiento;
- Tratamientos que usen nuevas o innovadoras tecnologías.

La referencia del artículo 35.2.b RGPD a los tratamientos de condenas e infracciones penales a que se refiere el artículo 10 RGPD, en una interpretación sistemática con lo previsto en el artículo 2.2.d RGPD, debe entenderse respecto de aquellos tratamientos de este tipo de datos que se produzcan en contextos distintos al de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales.

En el presente caso, nos encontramos, en cambio, ante notificaciones de infracciones penales en el marco de tratamientos jurisdiccionales por lo que no resulta de aplicación lo previsto en el RGPD, de acuerdo con la delimitación de su ámbito de objetivo de aplicación efectuada por el artículo 2.2 RGPD. Coherentemente con ello, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), contiene una Disposición transitoria cuarta, denominada "Tratamientos sometidos a la Directiva (UE) 2016/680", que mantiene vigente la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y sobre todo su artículo 22, mientras no se produzca la transposición al ordenamiento jurídico español de la Directiva (UE) 2016/680: "*Los tratamientos sometidos a la Directiva*



CONSEJO GENERAL DEL PODER JUDICIAL
Comité de Protección de Datos

(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, continuarán rigiéndose por la Ley Orgánica 15/1999, de 13 de diciembre, y en particular el artículo 22, y sus disposiciones de desarrollo, en tanto no entre en vigor la norma que trasponga al Derecho español lo dispuesto en la citada directiva”.

Cuarta.- El documento remitido por la Dirección General de Infraestructuras y Sistemas de la Consejería de Justicia e Interior de la Junta de Andalucía se refiere a la realización de una evaluación de impacto de protección de datos sobre las notificaciones judiciales a través de correos de forma telemática, lo que incluiría el tratamiento de datos personales de infracciones penales. En consecuencia, no siendo de aplicación en este ámbito el RGPD, como se ha indicado anteriormente, el Consejo General del Poder Judicial no debe pronunciarse en los términos a los que se refiere el artículo 36 del mencionado RGPD.

Quinta.- El artículo 36 del RGPD recoge la posibilidad de que el responsable consulte a la autoridad de control antes de proceder al tratamiento cuando una evaluación de impacto relativa a la protección de datos muestre que el tratamiento entrañaría un alto riesgo, y que la autoridad de control se manifieste al respecto pudiendo otorgar, si así lo considera, una autorización previa para que el tratamiento de datos se ejecute. No obstante el hecho de que el CGPJ no se pronuncie en los términos previstos en el artículo 36 del RGPD, al no ser de aplicación el mismo como ya se ha manifestado, ello no es óbice para analizar la cuestiones controvertidas según lo que se desprende de la documentación aportada por esa Dirección General de Infraestructuras y Sistemas de la Consejería de Justicia e Interior de la Junta de Andalucía.

Con carácter previo, se debe precisar que, aun cuando en el apartado 2 del Informe Actividades de Tratamiento de Datos Personales, titulado “Envío de comunicaciones comerciales por correos” (entendemos que existe un error en este título, ya que no se trata de “comunicaciones comerciales”), en su punto 3 “Amenazas y riesgos”, se incluye “la existencia de datos sensibles o muy personales relacionados con la información personal de las comunicaciones objeto de tratamiento”, si bien existe esa notificación de datos relativos a condenas e infracciones, se trata de



notificaciones reguladas por las normas procesales, y que, por tanto, se realizan al amparo de la legalidad vigente.

Siguiendo con este punto, no se desprende cuál es la vulnerabilidad cuando se indica "La gestión de datos de empleados como sujetos vulnerables por existir un desequilibrio de poder entre los interesados y el responsable del tratamiento", ya que el supuesto planteado no deriva en que el responsable desee imponer a sus empleados, utilizando sus facultades de dirección, un determinado tratamiento de datos personales que menoscabe la protección de datos de los citados empleados, sin perjuicio de que, si ejecutan la labor de imprimir, ensobrar y enviar las comunicaciones a los afectados, cumplan con el deber de confidencialidad.

Sexta.- Procede analizar a continuación el apartado 2 punto 5, relativo a las "Recomendaciones y conclusiones", donde se manifiesta que "el escenario con mayor impacto sobre este tratamiento es aquel relacionado con la ausencia de acuerdos que regulen la relación con Correos como sub-encargado del tratamiento".

A tal efecto, se ha remitido el Convenio existente para la prestación de servicios postales y telegráficos entre la Junta de Andalucía y Correos, que contiene una cláusula séptima denominada "Protección de datos de Carácter Personal", con referencias a la ya derogada Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (si bien como hemos expuesto aplicable en el ámbito penal), o incluso, al Real Decreto 994/1999 (esta norma fue derogada mediante la aprobación del Real Decreto 1720/2007, de 21 de diciembre).

Pues bien, sobre el contenido que deben reflejar los contratos con encargados de tratamiento desde la aplicación del RGPD, debemos precisar lo siguiente:

En primer lugar, dicho contenido debe incluir, al menos, lo que recoge el apartado 3 del artículo 28 del RGPD, y sin perjuicio de que exista un cumplimiento material de lo contemplado.

En segundo lugar, la LOPDGDD, en su Disposición Transitoria Quinta, ha establecido un plazo para que este tipo de contratos, o en el supuesto planteado, convenios con cláusulas de encargados de tratamiento se adecúen a lo que recoge el RGPD: *"Los contratos de encargado del tratamiento suscritos con anterioridad al 25 de mayo de 2018 al amparo de lo dispuesto en el artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal mantendrán su vigencia hasta la fecha de vencimiento señalada en los mismos y en caso de haberse pactado de forma indefinida, hasta el 25 de mayo de 2022."*



Durante dichos plazos cualquiera de las partes podrá exigir a la otra la modificación del contrato a fin de que el mismo resulte conforme a lo dispuesto en el artículo 28 del Reglamento (UE) 2016/679 y en el Capítulo II del Título V de esta ley orgánica”.

Por tanto, existe una fecha límite para adecuar la citada cláusula, si bien cualquiera de las partes puede solicitar su actualización en cualquier momento.

De hecho, sería recomendable que se actualice la misma a la mayor brevedad posible para reflejar el contenido que establece el RGPD, y por tanto, adecuar dicha cláusula a la realidad normativa aplicable.

Séptima.- Por otra parte, se propone por esa Dirección General que se desarrolle un acuerdo que establezca los términos y condiciones de subcontratación del tratamiento, acuerdo que estaría firmado por un representante del responsable (órganos judiciales) y el encargado (la Dirección General de Infraestructuras y Sistemas).

Para resolver esta cuestión debemos dilucidar sobre la aplicación del RGPD en los tratamientos jurisdiccionales.

Si bien la norma europea se aplica a estos tratamientos –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 RGPD 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 RGPD 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 realidad existente.

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). 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, ello lleva implícito que por parte del encargado se designe o contrate con un subencargado que cumpla con el RGPD y la LOPDGDD, así como que puedan establecer las condiciones y requisitos de esta subcontratación, sin necesidad de que se tenga que firmar un acuerdo con un representante de los órganos judiciales, pero respetando la tutela judicial efectiva.

III. CONCLUSIONES

Primera.- Al tratarse de notificaciones que afectan a infracciones y sanciones penales no es de aplicación el Reglamento General de Protección de Datos, sino la Ley Orgánica 15/1999, de 13 de diciembre, por lo que no procede que el Consejo General del Poder Judicial valore si autoriza o no el tratamiento de datos personales en los términos descritos por el artículo 36 del RGPD.

Segunda.- La LOPDGDD ha establecido un período transitorio para adecuar los contratos con encargados de tratamientos, siendo la fecha límite el 25 de mayo del año 2022. No obstante, se recomienda que se actualice el contenido del convenio entre la Junta de Andalucía y Correos para adecuarlo a la regulación del RGPD.

Tercera.- No procede la firma de un acuerdo con un representante del ámbito judicial en el que se fije las condiciones de subcontratación, ya que la existencia de Administraciones prestacionales como encargadas de tratamiento lleva inherente que las mismas, en caso de subcontratación, puedan fijar los términos y condiciones de la subcontratación, sin afectar a la tutela judicial efectiva.