

Comentarios de Belén Durán Cardo sobre las *Guidelines 07/2020 on the concepts of controller and processor in the GDPR, version 1.0, adopted on 02 September 2020, del European Data Protection Board*

A continuación se indican los comentarios sobre las *Guidelines 07/2020 on the concepts of controller and processor in the GDPR, version 1.0, adopted on 02 September 2020, del European Data Protection Board* (en adelante “Guía”) por temática¹:

1. Respecto al elemento subjetivo de los conceptos de responsable y encargado

Parágrafos 17 y 18.

- En la Guía se indica que puede ser responsable del tratamiento una organización, un individuo o un grupo de individuos. Por tanto, parece que al nombrar un grupo de individuos se admitiría que pudieran ser responsables las entidades sin personalidad jurídica. Esto debería dejarse claro, ya que están surgiendo divergencias en los Estados miembros porque se está interpretando el concepto siguiendo una tendencia continuista respecto a sus anteriores leyes e interpretaciones². Si lo que se pretende es tener una interpretación homogénea del concepto en toda la UE, que esté en línea con el carácter de concepto autónomo, es relevante que se deje claro en la Guía.
- Habría que diferenciar entre lo que sería la asignación del rol de responsable del tratamiento a efectos de asignar responsabilidades derivadas del cumplimiento del RGPD y lo que sería una asignación a nivel interno de responsabilidades, con el fin de poder cumplir de manera efectiva la normativa de protección de datos. Es decir, independientemente de que en el ámbito interno de la organización se puedan establecer responsabilidades para quienes decidan internamente sobre los fines y medios de los tratamientos, el rol de responsable del tratamiento a efectos externos y de cumplimiento de la normativa debería de asignarse por regla general a la organización que tenga personalidad jurídica³.

¹ Los comentarios representan las opiniones personales de su autora y derivan principalmente de sus investigaciones sobre los conceptos de responsable y encargado realizadas principalmente durante la elaboración de su tesis doctoral y posteriores publicaciones.

² Por ejemplo, el ICO no admite que pueda ser responsable una entidad sin personalidad jurídica, pese a que permite que pueda identificarse como tal ante los interesados. *Guide to the General Data Protection Regulation (GDPR). Controllers and processors*, ICO, 24.4.2019-1.0.3, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/controllers-and-processors/> (Consulta: 8.2.2020). En algunas de las leyes nacionales previas al RGPD, adoptadas por los Estados miembros, se admitía expresamente que pudieran ser responsables del tratamiento entidades sin personalidad jurídica. Estas leyes eran la española, la chipriota, húngara y polaca. Además, otras leyes que no hacían referencia expresa a esta posibilidad también indicaban en sus definiciones de responsable a entidades como departamentos o unidades (ley italiana), oficinas de órganos (ley austríaca) o asociaciones de hecho (ley belga), referencias que iban en esta línea de admitir claramente esta posibilidad. En España se admitía que pudieran ser responsables del tratamiento las sociedades civiles, las comunidades de propietarios, las sucursales o las uniones temporales de empresas. DURÁN CARDO, B., *La figura del responsable en el derecho a la protección de datos*, La Ley, Wolters Kluwer, Las Rozas (Madrid), 2016, pp. 181, 207.

³ El hecho de que en organizaciones grandes o complejas sea lógico que las decisiones se adopten por algunas unidades y que otras sean las que ejecutan las mismas, queda patente en las *Directrices para determinar la autoridad de control principal de un responsable o encargado del tratamiento*, adoptadas el 13.12.2016, revisadas el 5.4.2017, 16/ES WP 244 rev.01, Grupo de Trabajo sobre Protección de Datos del Artículo 29. No obstante, es necesario tener criterios claros en este sentido, puesto que esta realidad podría llevar a considerar a las unidades organizativas que adoptan decisiones como responsables del

- En línea con esta aclaración también debería indicarse de forma específica si puede asignarse el rol de responsable del tratamiento a un órgano administrativo, sin personalidad jurídica propia⁴. En este sentido, añaden confusión los términos utilizados en la versión española del RGPD. En la versión inglesa este bloque se refiere a “natural or legal person, public authority, agency or other body” y en la versión española a “la persona física o jurídica, autoridad pública, servicio u otro organismo”. La palabra “servicio”, traducción de “agency” parece, de entrada, más proclive a permitir esta asignación del rol a un órgano administrativo, mientras que en la versión en inglés es el término “body” el que parece permitir esta asignación.

La sentencia del TJUE (Sala Tercera) de 9 de julio de 2020 considera que debe calificarse como responsable del tratamiento la Comisión de Peticiones del Parlamento del *Land* de Hesse porque la incluiría en el término de “autoridad pública” del 4.7 RGPD⁵. Esta Comisión de Peticiones aparentemente no goza de personalidad jurídica independiente y es un órgano del Parlamento del *Land*. Por tanto, en línea con esta interpretación del TJUE debería admitirse que órganos sin personalidad jurídica también pudieran considerarse responsables del tratamiento⁶.

Habría que indicar en la Guía las consecuencias de esta interpretación y los criterios para que las Administraciones puedan determinar qué órganos pueden considerarse responsables del tratamiento. Dependiendo de cómo se haga esta interpretación esto puede incrementar enormemente la complejidad del cumplimiento de la normativa en el seno de una Administración Pública.

Por otro lado, como el objetivo que está detrás de esta asignación del rol al órgano administrativo suele ser la transparencia, se podría optar por asignar el rol a la Administración Pública, con personalidad jurídica o que tenga claramente una autonomía funcional, pero incorporar en la información a los interesados qué órgano administrativo concreto es el que está realizando el tratamiento o decidiendo sobre el mismo. En todo caso,

tratamiento a efectos del RGPD. Para evitar que esta postura implique grandes divergencias entre los enfoques de las organizaciones (una empresa que considere que todos sus departamentos son responsables del tratamiento frente a otra que considere que la empresa es responsable) deberían darse criterios para guiar a todas las organizaciones en esta tarea tan esencial de determinación del rol.

⁴ La ley irlandesa de protección de datos, que, en la línea de la regulación anterior al RGPD, mantiene la posibilidad de que se designe como responsable del tratamiento a un funcionario de la administración pública, sin perjuicio de que la posible sanción luego se imponga a la administración que designe a este funcionario. *Data Protection Act 2018*, <http://www.irishstatutebook.ie/eli/2018/act/7/enacted/en/html> (Consulta: 8.2.2020).

⁵ Sentencia del TJUE de 9 de julio de 2020 *VQ c. Land Hessen*, C-272/19, ECLI:EU:C:2020:535.

⁶ Así lo entiende también el Supervisor Europeo de Protección de Datos, que, en su Guía sobre los conceptos de responsable y encargado del tratamiento, indica que las definiciones de responsable del tratamiento del Reglamento (UE) 2016/679 y el Reglamento (UE) 2018/1725 son esencialmente funcionales, de manera que la entidad que decide el “qué” y el “cómo” del tratamiento será responsable, independientemente de su estatus organizativo. No obstante, en la definición del art. 3.8 del Reglamento (UE) 2018/1725 se deja claro que puede considerarse responsable del tratamiento “la institución o el organismo o la dirección general u otra entidad organizativa de la Unión que, por sí sola o conjuntamente con otros, determine los fines y medios del tratamiento de datos personales”. Como especifica el Supervisor, esta definición se adapta a las características de las instituciones europeas en las que las direcciones generales son divisiones organizativas comunes. La gran envergadura y autonomía de estas entidades justifica que puedan asumir el rol de responsables. EUROPEAN DATA PROTECTION SUPERVISOR, *Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725*, 7.11.2019, p. 7.

es importante que quede clara la postura del EDPB para que todos los Estados miembros apliquen la misma interpretación.

- Otra cuestión que sería necesario dejar clara es si deben considerarse responsables del tratamiento aquellas unidades o personas que, dentro de una organización ostentan un rol por el que deben actuar con independencia o por el que tienen un margen de actuación limitado por la legislación. Ejemplo de ello pueden ser los delegados de personal o comités de empresa, los delegados de prevención de riesgos laborales o comités de prevención de riesgos laborales, los comités de igualdad, los concejales de los ayuntamientos, los socios o asociados de sociedades o asociaciones. Otro ejemplo sería el propio Delegado de Protección de Datos. Debería hacerse referencia en la Guía a esta problemática y valorar qué papel ostentarían. Para ello, también sería necesario analizar si se les podría encajar en el papel de “personas autorizadas” o de “encargados del tratamiento” (por ejemplo cuando el Delegado de Protección de Datos lo ejerce una empresa contratada por el responsable del tratamiento).

Esto enlazaría con otra cuestión relativa a si hay que optar por un sistema completo de asignación de roles o no. Es decir, todos los sujetos que realicen un tratamiento, según se define en el RGPD ¿deberían tener un rol asignado de acuerdo con el propio RGPD, ya sea responsable del tratamiento, encargado o persona autorizada?

Parágrafo 75

- Uno de los requisitos para ser encargado del tratamiento es que estemos ante una entidad diferenciada del responsable del tratamiento. No obstante, en la Guía se indica: “On the other hand, a department within a company cannot generally be a processor to another department within the same entity”. El término “generally” implica que excepcionalmente sí podría entenderse que un departamento de una empresa pudiera considerarse encargado del tratamiento de otro departamento de la misma empresa. De hecho, esto enlazaría de nuevo con la necesidad de dejar claro si, al igual que con el concepto del responsable del tratamiento (esta parte es exactamente igual en ambos conceptos), se debe entender que pueden ser encargados del tratamiento entidades que no tienen personalidad jurídica y, en el ámbito de la Administración Pública, si pueden ser órganos administrativos respecto a otros órganos administrativos de la misma Administración⁷.

Si se admite esta posibilidad, entonces debería decirse claramente y no limitar el ejemplo a departamentos de una empresa, si no dejar claro que también puede suceder respecto a órganos de una Administración Pública. No obstante, de nuevo hay que valorar la complejidad que se añadiría al cumplimiento. Como parece sugerir el *European Data Protection Supervisor* lo mejor sería mantener este requisito y no admitir que se considere encargado del tratamiento a un órgano administrativo ni a un departamento de una empresa, pero incentivar que, en aras de cumplir con la responsabilidad proactiva resultaría

⁷ La Ley española vigente (Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales), respecto al encargado del tratamiento, especifica, en su artículo 33.5, que, en el ámbito del sector público se pueden atribuir las competencias de un encargado del tratamiento a un determinado órgano mediante la adopción de una norma reguladora de dichas competencias, que deberá incorporar el contenido establecido por el artículo 28 RGPD. Por tanto, se admite que el encargado pueda ser un órgano.

recomendable que, en estos casos, se suscribieran acuerdos internos equiparables a los de encargado del tratamiento⁸.

En definitiva, está claro que, en estructuras complejas o grandes, a nivel interno existirán unidades, departamentos, áreas u órganos que serán los que, en realidad determinarán los fines y medios de los tratamientos que realicen o que pueden actuar dando soporte a otros, pero no debería implicar que se les asigne el rol de responsable o encargado.

2. El control deriva de una competencia legal explícita

Parágrafo 21 y Anexo I

- Es importante que quede claro que lo que debe primar para determinar si estamos ante un responsable del tratamiento es si determina los fines y los medios esenciales. De esta forma podría darse el caso de que en una ley se designe a un sujeto como responsable y que no fuera este el que realmente tiene esta capacidad de control sobre el tratamiento. Por lo tanto, debería primar la realidad ante la posibilidad de que la designación que realice el legislador sea incorrecta.

Por eso también es importante que esto se refleje en el gráfico que está en el Anexo I.

3. Proveedores que no deben acceder a datos personales

Parágrafo 81. Example: IT-consultant fixing a software bug

- Respecto a este ejemplo entiendo que lo que se quiere reflejar es un caso en el que no debería haber tratamiento de datos personales, igual que sucede con un servicio de limpieza de oficinas, por ejemplo. De este modo, lo que debería adoptarse son medidas de seguridad para evitar que estos servicios que se presupone que no deben tratar datos personales, no accedan a ellos. Tal como se indica en un ejemplo que se menciona posteriormente (a continuación del Parágrafo 87), relativo precisamente a un servicio de limpieza, también en este supuesto se calificaría al proveedor como un tercero (third party).

4. Concepto de destinatario

- Respecto a este concepto debería aclararse la lógica de su incorporación en el RGPD, que entiendo no es otra que la de establecer el alcance de la información que debe proporcionarse al interesado⁹.

Este concepto, tal como se señala en la Guía, se mantiene prácticamente inalterable respecto al que incorporaba la Directiva 95/46/CE¹⁰. Hay que decir que este concepto se incluyó en la versión final de la Directiva 95/46/CE directamente, a iniciativa de la delegación francesa y de la Comisión, que propusieron separar esta noción de la de tercero¹¹. La

⁸ EUROPEAN DATA PROTECTION SUPERVISOR, *Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725*, 7.11.2019, pp. 15-16.

⁹ Ver DURÁN CARDO, B., *La figura del responsable en el derecho a la protección de datos*, op. cit., pp. 369-371 y DURÁN CARDO, B., *El Delegado de Protección de Datos en el RGPD y la nueva LOPDGDD*, La Ley, Wolters Kluwer, Las Rozas (Madrid), 2019, pp. 211-215.

¹⁰ Así, el destinatario se define en la Directiva 95/46/CE como «la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que reciba comunicación de datos, se trate o no de un tercero. No obstante, las autoridades que puedan recibir una comunicación de datos en el marco de una investigación específica no serán considerados destinatarios» (art. 2.g) Directiva 95/46/CE).

¹¹ HEREDERO HIGUERAS, M., *La Directiva comunitaria de protección de los datos de carácter personal (Comentario a la Directiva del Parlamento Europeo y del Consejo 95/46/CE, relativa a la protección de las*

explicación para hacerlo fue «que es útil para garantizar la transparencia de los tratamientos con respecto a las personas afectadas»¹². Por tanto, la única finalidad por la que se introdujo este concepto de destinatario en la Directiva 95/46/CE fue para proporcionar información sobre el tratamiento de datos al interesado¹³.

De la misma forma, el destinatario aparece principalmente en los preceptos que el RGPD dedica a establecer obligaciones informativas. Así, tanto en la información que el responsable debe facilitar cuando obtenga los datos del interesado como cuando los obtenga de otra fuente, figura la relativa a los destinatarios (art. 13.1.e y 14.1.e RGPD). En el caso de recogida indirecta de datos se añade la necesidad de informar de la intención de “transferir datos personales a un destinatario en un tercer país” (art. 14.1.f RGPD).

El responsable debe informar también de los destinatarios, incluso los que estén en terceros países en caso de que el interesado ejerza su derecho de acceso (art. 15.1.c RGPD). Asimismo, aparece el término destinatario en la obligación de notificación que tiene el responsable a aquellos sujetos a los que hubiera comunicado datos personales, en caso de que los afectados hubieran ejercido los derechos de rectificación, supresión o limitación del tratamiento (art. 19 RGPD). También el responsable debe incluir en el registro de las actividades de tratamiento las categorías de destinatarios a quienes se comuniquen los datos (art. 30.1.d RGPD).

Hay que añadir que la definición establece que las autoridades no deben considerarse destinatarios, lo que implicará, por lo tanto, que no deberá informarse a los afectados sobre estas comunicaciones de datos.

En conclusión, hay que entender que el concepto de destinatario tiene una finalidad eminentemente informativa.

- En la Guía debería aclararse si, como se indicaba en las Directrices sobre transparencia, adoptadas por el Grupo del Artículo 29, el concepto de destinatario se refiere a quien se comuniquen los datos, sea un tercero o no, lo que incluiría a otros responsables del tratamiento, corresponsables o encargados del tratamiento¹⁴. Por tanto, no incluiría a “las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable o del encargado”, ya que deberá entenderse que respecto a estas personas no se produce una comunicación de datos.

5. Subcontratación

- Debería dejarse claro el alcance de la regulación de las subcontrataciones por los encargados del tratamiento ¿Esta regulación se refiere a todas las contrataciones de servicios que

personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, Aranzadi, Cizur Menor (Navarra), 1997, p. 82.

¹² Posición común (CE) n.º 1/95 adoptada por el Consejo el 20.2.1995 con vistas a la adopción de la Directiva 95/.../CE del Parlamento Europeo y del Consejo, de..., relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, DO C 93 de 13.4.1995, apdo. 2.i.

¹³ DURÁN CARDO, B., *La figura del responsable en el derecho a la protección de datos*, op. cit., pág. 369 y DURÁN CARDO, B., *El Delegado de Protección de Datos en el RGPD y la nueva LOPDGDD*, La Ley, Wolters Kluwer, Las Rozas (Madrid), 2019, pp. 183-186..

¹⁴ Directrices sobre transparencia en virtud del Reglamento (UE) 2016/679, 17/ES WP 260 rev.01, adoptadas el 29.11.2017, revisadas por última vez y adoptadas el 11.4.2018, Grupo de Trabajo Artículo 29 sobre la Protección de Datos, p. 18.

puedan hacer los encargados del tratamiento que tengan acceso a los datos personales, aunque se trate de servicios que no sean los contratados por el responsable? Por ejemplo, si un responsable del tratamiento A contrata los servicios de asesoramiento empresarial (contable, laboral) a un asesor X y este subcontrata parte de estos servicios a otro asesor Y, por lo que el asesor Y debe tratar los datos personales del responsable del tratamiento (de sus empleados, clientes, etc.). El asesor X se considerará encargado del tratamiento y el asesor Y también. Si el asesor X contrata los servicios informáticos para realizar sus actividades a una empresa B, ¿debe considerarse a esta empresa B encargado del tratamiento del responsable del tratamiento A porque tendrá un acceso a los datos personales de este responsable (de sus empleados, clientes, etc.) o como se trata de un servicio informático, que se consideraría un medio no esencial sobre el que podría decidir el encargado del tratamiento, debería considerarse que la empresa B es encargado del tratamiento del asesor X? ¿O, por el contrario, se debe interpretar que la decisión sobre contratar a la empresa B es un medio esencial, ya que significa dar acceso a esta empresa a los datos personales del responsable?

6. Alcance de la corresponsabilidad

Parágrafo 164

- Hay que tener en cuenta que lo que hace el TJUE es acotar el elemento objetivo al que se refiere el concepto de responsable. Es decir, la corresponsabilidad se limita a aquellas operaciones de tratamiento sobre las que ambos corresponsables decidan sobre fines y medios esenciales. En consecuencia, el acuerdo de corresponsabilidad debería centrarse en establecer las responsabilidades de cada parte respecto a estas operaciones de tratamiento. Esto implicará que los corresponsables podrán, a su vez, ser responsables de otras operaciones anteriores o posteriores a las que sean objeto de este régimen de corresponsabilidad.

Así, por ejemplo, en el asunto Fashion ID la corresponsabilidad se refiere a la recogida de datos y comunicación de estos a Facebook. Pero las operaciones de tratamiento que realiza Facebook después no serían objeto de la corresponsabilidad y se menciona, por ejemplo, la conservación de los datos. No obstante, que la conservación de los datos la realice Facebook sí tiene efectos en la corresponsabilidad, ya que Fashion ID no podrá atender las solicitudes de ejercicio de derechos de los interesados. Por otro lado, como Fashion ID es el que instala el plug in en su página web, será el que pueda proporcionar la información necesaria para cumplir con el artículo 13 RGPD. Pero ¿debería Fashion ID informar sobre esta recogida y la transmisión a Facebook exclusivamente o también deberá informar sobre el tratamiento posterior que Facebook realizará? La Guía debería abordar las problemáticas derivadas de limitar la corresponsabilidad a unas operaciones de tratamiento que pueden estar englobadas en otros tratamientos de los corresponsables.

Cuando la corresponsabilidad sea el fruto de una decisión conjunta de varios agentes que se ponen de acuerdo “conscientemente” en realizar un tratamiento sobre el que decidirán fines y medios esenciales será más fácil que si estamos ante corresponsabilidades en las que convergen decisiones de un modo no tan consciente pero de forma que el tratamiento no pueda realizarse sin la actuación indisociablemente unida de las partes.