¿A QUÉ OBLIGA EL PRINCIPIO DE ACCOUNTABILITY EN EL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS?

Iuliana Raluca Stroie
Investigadora del Centro de Estudios de Consumo
Universidad de Castilla-La Mancha
Iuliana.Raluca@uclm.es

Indice

I. Regulación

II. Concepto

III. Alcance

Accountability:¿una de las novedades destacables del RGDPD?

- Se mencionaba en el Documento del Grupo de Trabajo del artículo 29 (GT 29) sobre «El Futuro de la Privacidad» (WP 168) de diciembre de 2009.
- Propuesta concreta del GT 29 a través del Dictamen 3/2010, de sobre el principio de responsabilidad:
  - para la inclusión de un principio de responsabilidad que imponga a los responsables del tratamiento de datos la aplicación de medidas apropiadas y eficaces que garanticen la aplicación de los principios y obligaciones recogidos en la Directiva y, "demostrar este extremo cuando se les solicitara".

Accountability como principio (art. 5 RGPD)

Cumplir y ser capaz de demostrarlo:

- Tratar los datos de manera lícita, leal y transparente («licitud, lealtad y transparencia»);
- Recoger los datos para fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines («limitación de la finalidad»);
- Asegurar que los datos sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»);
- Asegurar que los datos sean exactos y actualizados («exactitud»);
- Mantenidos durante no más tiempo del necesario para los fines del tratamiento («limitación del plazo de conservación»);
- Tratados de manera que garantice la seguridad y protección contra tratamiento ilícito o no autorizado («integridad y confidencialidad»).

Art. 24 Responsabilidad del responsable de tratamiento de datos

- Obligación del responsable de aplicar medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con lo previsto en el Reglamento.
- Para la aplicación de dichas medidas se tendrá en cuenta:
  - la naturaleza, el ámbito, el contexto y los fines del tratamiento
  - los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas
- Para demonstrar el cumplimiento de sus obligaciones, el responsable **puede adherirse** a códigos de conducta aprobados a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42.

Además, Considerando 74 del Reglamento:

- Debe quedar establecida la responsabilidad del responsable del tratamiento por cualquier tratamiento de datos personales realizado por él mismo o por su cuenta.

- El responsable debe estar obligado a aplicar medidas oportunas y eficaces y ha de poder demostrar la conformidad de las actividades de tratamiento con lo previsto en el Reglamento, incluida la eficacia de las medidas.

- Las medidas deben tener en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como el riesgo para los derechos y libertades de las personas físicas.

¿Qué se entiende por "responsabilidad proactiva"?

- Cumplimiento de los principios del RGPD.
- Adoptar medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con lo dispuesto por el Reglamento. Por ejemplo:
  - evaluación de riesgos e impacto jurídico;
  - diseño del funcionamiento del tratamiento;
  - implementación de la seguridad;
  - llevanza de registro de actividades del tratamiento, etc.

Medidas técnicas y organizativas apropiadas:

Cfr. al Considerando 76, las medidas se han de elegir en base a la probabilidad y la gravedad del riesgo para los derechos y libertades del interesado.

La probabilidad y la gravedad del riesgo son variables, por lo que el Reglamento prevé determinadas medidas que solo deberán aplicarse cuando el tratamiento suponga un **alto riesgo** para los derechos y libertades y, en los demás casos las medidas deberán ser ajustadas en función del nivel y tipo de riesgo que el tratamiento conlleve.

Las medidas se han de adoptar antes del comienzo del tratamiento y deben ser actualizadas y revisadas durante el tratamiento.

¿Obligación de resultado?

- Deber general de cumplimiento de los principios recogidos por RGDPD.
- Obligación de adoptar las medidas técnicas y organizativas apropiadas sin especificar cuales son.
- Facultad que la norma otorga al responsable para la elección de dichas medidas, pero establece pautas.
- El RGPD determina tres niveles de obligaciones en función del grado de gravedad del riesgo, pero en todo caso, todos los responsables deben realizar una valoración de riesgo para poder determinar qué medidas deben aplicar y cómo deben hacerlo, que puede variar en función de:
  - los tipos de tratamiento;
  - la naturaleza de los datos;
  - el número de interesados afectados;
  - la cantidad y variedad de tratamientos que una misma organización lleve a cabo

Los tres niveles de obligaciones en función de la gravedad del riesgo (I)

I) Obligaciones que afectan a cualquier responsable pero con carácter general son las que deben ser adoptadas por PYMES o microempresas (art. 32):

- la seudonimización y el cifrado de datos personales;
- capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;
- capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;
- proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento;

Los tres niveles de obligaciones en función de la gravedad del riesgo (II)

2) Obligaciones que afectan a responsables que cuenten con 250 empleados o más:

- Además de las medidas anteriores deben llevar un registro de las actividades

Los tres niveles de obligaciones en función de la gravedad del riesgo (III)

3) Grandes empresas y Administraciones Públicas:

- Además de las medidas mencionadas para los dos grupos anteriores deben realizar la evaluación de impacto prevista en el art.35.

¡No se debe confundir la evaluación de impacto con la evaluación de la adecuación del nivel de seguridad del art. 32.2 que se impone a cualquier responsable!

Art. 25. Protección de datos desde el diseño y por defecto

- Obligación de utilizar la **seudonimización** como medida para aplicar de forma efectiva el principio de minimización de datos, teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas.

- Obligación del responsable de aplicar "las medidas técnicas y organizativas apropiadas" para **garantizar que, "por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento".** La obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad y garantizará en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas.

- Podrá utilizarse un **mecanismo de certificación** aprobado con arreglo al artículo 42 como elemento que acredite el cumplimiento de las obligaciones anteriores.

Art. 25. Protección de datos desde el diseño y por defecto

- ¿Podría considerarse la obligación de **garantizar que, "por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento"** una obligación de resultado?
- El ejemplo sería en este caso que un perfil de Facebook que por defecto era visible para cualquier usuario de dicha red social ahora lo será solo si el titular del mismo lo haga accesible para aquellos.
- La obligación consistiría en el diseño del programa de modo que el interesado pueda tener el control sobre su privacidad. Pero normalmente el responsable y el diseñador o un productor de un programa o una aplicación son entidades distintas con lo cuál se plantea el alcance de la obligación. (Cdo. 78 – Alentar a los productores que tengan en cuenta este derecho).
- Aunque podría considerarse una obligación de resultado, hay que tener en cuenta que con anterioridad al diseño de la aplicación el responsable debe realizar una valoración de los riesgos y documentar todos los pasos del tratamiento en los que entra el diseño de la aplicación, la implementación de las medidas de seguridad, etc. por lo que en caso de posible fallo en el resultado si aquél es capaz de demonstrar que no ha intervenido su culpa o negligencia en dicho fallo y ha adoptado las medidas de conformidad a la naturaleza, el ámbito, el contexto y los fines del tratamiento así como el riesgo para los derechos y libertades de las personas físicas sería exonerado de la responsabilidad.

¿Obligación de resultado?

- Hay que tener en cuenta que en caso de tratamientos que representan un alto riesgo, las autoridades de protección de datos pueden proporcionar directrices para la aplicación de medidas oportunas y para demostrar el cumplimiento por parte del responsable o del encargado del tratamiento, especialmente con respecto a la identificación del riesgo relacionado con el tratamiento, a su evaluación en términos de origen, naturaleza, probabilidad y gravedad y a la identificación de buenas prácticas para mitigar el riesgo (Cdo. 77).
- En caso de tratamientos que no supongan grandes riesgos se pueden indicar las medidas que se consideran suficientes en dichos casos para afrontar el riesgo en cuestión.
- Se consideran tratamientos de alto riesgo las operaciones de tratamiento a **gran escala** que persiguen tratar una **cantidad considerable de datos personales** a nivel regional, nacional o supranacional y que podrían afectar a un gran número de interesados (Cdo. 91).
- Las directrices de las autoridades de control que pueden adoptar la forma de códigos de conducta
- Conclusión: No se trata de obligaciones de resultado sino de poder probar el cumplimiento de las obligaciones. Esto es, llevar registros de todas las actividades, incluso antes del comienzo del tratamiento cuando se impone la realización de evaluaciones de riesgo e impacto jurídico.
- Se trata de deberes de diligencia en cuanto si pueden probar su falta de culpabilidad serán exonerados de responsabilidad.

Art. 32.1 Seguridad del tratamiento ¿otro supuesto de responsabilidad por el resultado?

- "Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo…".
- Se trata igualmente de un deber de diligencia;
- Se tiene que evaluar el riesgo del caso concreto y adoptar las medidas teniendo en cuenta el estado de la técnica, los costes de aplicación, etc.
- La opción de adhesión a códigos de conducta o mecanismos de certificación sirve para demonstrar el cumplimiento normativo.
- No obstante, la certificación no limitará la responsabilidad del responsable o encargado del tratamiento en cuanto al cumplimiento del presente Reglamento y se entenderá sin perjuicio de las funciones y los poderes de las autoridades de control que sean competentes en virtud del artículo 55 o 56 (art. 42).

Conclusiones responsabilidad por resultado:

- Los distintos supuestos en los que opera la responsabilidad del responsable de tratamiento se refiere a un deber general de diligencia.

- El responsable debe cumplir la normativa y poder comprobar el cumplimiento para lo que es fundamental disponer de los documentos que puedan acreditar dicho cumplimiento en todas las fases del tratamiento incluso con anterioridad al mismo.

- Conforme a las Guías sobre aplicación práctica del principio de responsabilidad activa del Supervisor Europeo de Protección de datos para instituciones o agencias de la UE: *"mantener registros de actividades y realizar evaluaciones de cumplimiento del RGDPD será suficiente para cumplir con el principio de accountability. Sólo determinados tipos de tratamiento requieren evaluación de impacto"*.

¿La opción de adhesión a códigos de conducta o mecanismos de certificación exime de responsabilidad? (Art. 24.3)

- Los códigos de conducta (art.40) son elaborados o aprobados (si son propuestos por asociaciones y otros organismos representativos de categorías de responsables o encargados del tratamiento) por las autoridades de control, con lo cual la adhesión al mismo y su cumplimiento son presunción de cumplimiento del RGDPD y exime de la obligación de probar la inocencia.

- Los mecanismos de certificación (art. 42) será expedida por los organismos de certificación (acreditados por la autoridad de control) y no limitará la responsabilidad del responsable o encargado del tratamiento en cuanto al cumplimiento del presente Reglamento (art. 42.4).

- De la mención expresa del art. 42.4 respecto a la no limitación de la responsabilidad en caso de la certificación se puede interpretar que la falta de una mención expresa similar en el supuesto de adhesión a los códigos de conducta denota un tratamiento distinto de un supuesto u otro y por consiguiente, de una limitación de la responsabilidad en este último caso.

Sujetos sometidos a la responsabilidad (I):

«responsable del tratamiento» o «responsable»: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento;

«encargado del tratamiento» o «encargado»: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento;

Sujetos sometidos a la responsabilidad (II):

- Al regular la responsabilidad, el art. 24 **se refiere solo al responsable del tratamiento** sin hacer mención al encargado.
- Cdo. 74 Debe quedar establecida **la responsabilidad del responsable** del tratamiento por cualquier tratamiento de datos personales realizado por él mismo o por su cuenta. En particular, el responsable debe estar obligado a aplicar medidas oportunas y eficaces y ha de poder demostrar la conformidad de las actividades de tratamiento con el presente Reglamento, incluida la eficacia de las medidas.
- Cdo. 79 La protección de los derechos y libertades de los interesados, así como la responsabilidad de los responsables y encargados del tratamiento, también en lo que respecta a la supervisión por parte de las autoridades de control y a las medidas adoptadas por ellas, requieren una **atribución clara de las responsabilidades** en virtud del presente Reglamento, incluidos los casos en los que un responsable determine los fines y medios del tratamiento de forma conjunta con otros responsables, o en los que el tratamiento se lleve a cabo por cuenta de un responsable.
- Cdo. 81 Para garantizar el cumplimiento de las disposiciones del presente Reglamento respecto del tratamiento que lleve a cabo el encargado por cuenta del responsable, este, al encomendar actividades de tratamiento a un encargado, **debe recurrir únicamente a encargados que ofrezcan suficientes garantías,** en particular en lo que respecta a conocimientos especializados, fiabilidad y recursos, de cara a la aplicación de medidas técnicas y organizativas que cumplan los requisitos del presente Reglamento, incluida la seguridad del tratamiento. La adhesión del **encargado** a un código de conducta aprobado o a un mecanismo de certificación aprobado puede servir de elemento para demostrar el cumplimiento de las obligaciones por parte del **responsable.**

Sujetos sometidos a la responsabilidad (III):

- La relación entre responsable y encargado:
  - debe regirse por un contrato u otro acto jurídico con arreglo al Derecho de la Unión o de los Estados miembros;
  - el contrato puede ser individual o en cláusulas contractuales tipo que adopte directamente la Comisión o que primero adopte una autoridad de control de conformidad con el mecanismo de coherencia y posteriormente la Comisión.

Responsabilidad de los encargados

- Es responsabilidad de los responsables elegir al encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiados, de manera que el tratamiento sea conforme con los requisitos del presente Reglamento y garantice la protección de los derechos del interesado – porque es el responsable quien determina los fines y los medios del tratamiento.
- El encargado necesita la autorización previa por escrito, específica o general, del responsable para recurrir a otro encargado.
- Debe seguir únicamente las instrucciones documentadas del responsable.
- No puede determinar los fines y medios del tratamiento. Si lo hace se convierte en responsable a efectos del RGDPD.
- Responde solo por sus obligaciones especificas recogidas en el art. 28.3 (asegurar que las personas a su cargo guarden la confidencialidad, ayudará al responsable a adoptar las medidas del art. 32, o le asistirá para que este pueda cumplir las solicitudes de ejercicio de los derechos de los interesados).

Los supuestos de responsabilidad del encargado (art. 28):

- Si recurre a otro encargado sin la autorización previa por escrito, específica o general, del responsable;
- Si las personas que están encargadas del tratamiento de datos (entendemos a su cargo) incumplen las obligaciones de confidencialidad;
- Si no toma las medidas que le corresponden del art. 32:
  - de seudonimización y de cifrado de datos personales;
  - no garantiza la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;
  - no procede a restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;
  - no realiza la verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

Corresponsables del tratamiento (art. 26)

- Cuando dos o más responsables **determinen conjuntamente los objetivos y los medios del tratamiento** serán considerados **corresponsables del tratamiento.** Los corresponsables determinarán de modo transparente y de mutuo acuerdo sus responsabilidades respectivas en el cumplimiento de las obligaciones impuestas por el presente Reglamento, en particular en cuanto al ejercicio de los derechos del interesado y a sus respectivas obligaciones de suministro de información a que se refieren los artículos 13 y 14, salvo, y en la medida en que, sus responsabilidades respectivas se rijan por el Derecho de la Unión o de los Estados miembros que se les aplique a ellos.

- Independientemente de los términos del acuerdo a que se refiere el apartado 1, los interesados podrán ejercer los derechos que les reconoce el presente Reglamento frente a, y en contra de, cada uno de los responsables.

¿Responsabilidad solidaria de los corresponsables?

- Cdo. 146 Si los responsables o encargados participan en el mismo tratamiento, cada responsable o encargado debe ser considerado responsable de la totalidad de los daños y perjuicios. No obstante, si se acumulan en la misma causa de conformidad con el Derecho de los Estados miembros, la indemnización puede prorratearse en función de la responsabilidad de cada responsable o encargado por los daños y perjuicios causados por el tratamiento, siempre que se garantice la indemnización total y efectiva del interesado que sufrió los daños y perjuicios. Todo responsable o encargado que haya abonado la totalidad de la indemnización puede interponer recurso posteriormente contra otros responsables o encargados que hayan participado en el mismo tratamiento.

Postura del TJUE

- STJUE 5 junio 2018, C-210/16, el administrador de una página de fans creada en Facebook es corresponsable con Facebook en el tratamiento de datos. La responsabilidad se basa en el grado de implicación de cada uno de los corresponsables y los términos contractuales entre los dos son irrelevantes.
- STJUE 10 julio 2018, C25/17, los miembros de la comunidad religiosa Testigos de Jehová que están predicando puerta a puerta son corresponsables junto a la comunidad, aunque aquellos no tengan acceso a los datos tratados o no haya directrices escritas para ellos por parte de la comunidad relativas al tratamiento de los datos.
- STJUE 29 julio 2019, C-40/17, Fashion ID es corresponsable del tratamiento junto a Facebook por tener el botón "me gusta" en su página web con lo cual participa en la recopilación y transmisión a Facebook de los datos personales de los visitadores a su página web

Art. 82 Derecho a indemnización y responsabilidad

- Toda persona que haya sufrido daños y perjuicios materiales o inmateriales como consecuencia de una infracción del presente Reglamento tendrá derecho a recibir del responsable o el encargado del tratamiento una indemnización por los daños y perjuicios sufridos.

- El derecho a la indemnización tiene que ser consecuencia del incumplimiento del Reglamento, es decir por culpa o negligencia.

- Excepción: si el responsable es una entidad pública en cuyo caso se trata de una responsabilidad objetiva.

- Para eximir la responsabilidad el responsable o encargado debe probar que no es en modo alguno responsable del hecho que haya causado los daños y perjuicios y el hecho sea consecuencia del incumplimiento del RGPD.

- El encargado únicamente responderá de los daños y perjuicios causados por el tratamiento cuando no haya cumplido con las obligaciones del presente Reglamento dirigidas específicamente a los encargados o haya actuado al margen o en contra de las instrucciones legales del responsable.

El primer caso de indemnización por daños morales por infracción del RGDPD

- La entidad de correo postal austriaca había realizado el profiling a mas de dos millones de interesados para averiguar sus orientaciones políticas sin informar sobre ello a los interesados y además, en algunos casos vendió los datos a terceras partes.
- El reclamante lo único que ha alegado a sido que se sentido molesto por haberse visto sometido a un proceso de profiling sin ser informado ni preguntado por su consentimiento.
- El Tribunal austriaco ha puesto de relieve que no cualquier mínima molestia puede justificar una reclamación por daños morales pero en este caso la molestia ha superado ese limite mínimo por lo que condena a la demandada a indemnizar al reclamante con la cantidad de 800€ sin especificar qué criterios ha utilizado para calcular ese importe.
- Ambas partes han recurrido la sentencia y además se ha comunicado que una conocida organización austriaca esta preparando una acción colectiva en representación de más de 1.600 afectados y que pretenden reclamar una cantidad de 3.000€ para cada uno.

La fuente de la información: https://digital.freshfields.com/post/102fth1/can-i-claim-damages-for-hurt-feelings-under-gdpr-an-austrian-court-says-yes .

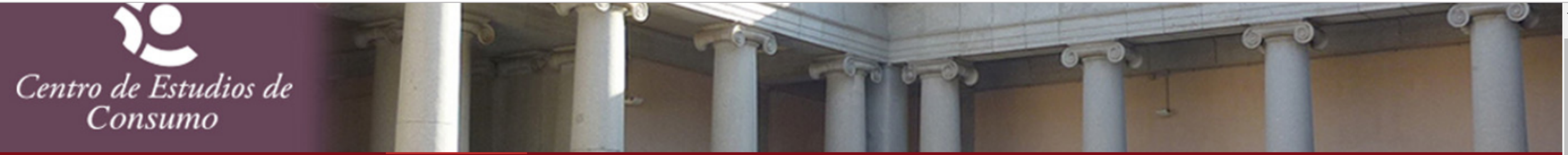
Conclusiones:

Las obligaciones del responsable no son de resultado, sino diligencia de cumplimiento normativo y también de documentar todas las actividades realizadas en el marco del tratamiento.

En el escalafón de las responsabilidades, en caso de corresponsables del tratamiento, y se tiene que realizar la ponderación de las responsabilidades teniendo en cuenta el grado de implicación en la determinación de los fines y los medios del tratamiento.

La responsabilidad prevista en el RGDPD es una responsabilidad solidaria pudiendo el interesado reclamar a cualquiera de los sujetos responsables sin perjuicio de la posibilidad que tiene aquél de repercutir contra los demás responsables.

La exención de responsabilidad solo puede operar cuando el responsable o encargado de tratamiento puedan demonstrar el cumplimiento con las disposiciones del RGDPD.



Protección de datos

Que me olviden, pero solo en Francia: más que una delimitación territorial del derecho al olvido una satisfacción parcial de éste
Iuliana Raluca Stroie
Octubre 2019

El Ayuntamiento de Parla SÍ infringió la normativa de protección de datos en la prestación de servicios de atención social
Iuliana Raluca Stroie
Septiembre 2019

El Ayuntamiento de Parla NO infringió la normativa de protección de datos en la prestación de servicios de atención social
Ángel Carrasco Perera
Septiembre 2019

Las reglas para la identificación de los interesados en las notificaciones por medio de anuncios y publicaciones de actos administrativos
Iuliana Raluca Stroie
Julio 2019

Centro de Estudios de Consumo

UCLM
UNIVERSIDAD DE CASTILLA-LA MANCHA

¡Muchas gracias por su atención!

Iuliana Raluca Stroie
Investigadora del Centro de Estudios de Consumo
Universidad de Castilla-La Mancha
Iuliana.Raluca@uclm.es