GRUPO DE ARCHIVOS EUROPEOS

GUÍA SOBRE PROTECCIÓN DE DATOS PARA SERVICIOS DE ARCHIVO

Directrices del Grupo de Archivos Europeos sobre la implementación de la Protección General de Datos. Regulación en el sector del archivo.

Estas directrices están pensadas para ayudar a los servicios de archivo en Europa a aplicar el RGPD. Es un trabajo en evolución, sujeto a mejoras y enriquecimiento, gracias a vuestras experiencias y comentarios. Estas directrices también pueden ser modificadas sobre la base de futura Jurisprudencia y de opiniones y directrices emitidas por el Comité Europeo de Protección de Datos.
El Grupo de Archivos Europeos agradecería con gusto sus comentarios. Los comentarios pueden ser enviados a la Dirección de correo electrónico siguiente:

SG-EAG-GUIDELINES@ec.europa.eu .

ADVERTENCIA LEGAL
Este documento no está destinado a proporcionar, y no constituye ni comprende, asesoramiento legal sobre ningún asunto en particular y se proporciona únicamente con fines de información general. No debería actuar o abstenerse de actuar sobre la base de cualquier material contenido en el mismo, sin buscar asesoramiento legal o profesional adecuado.

Título: Guidance on data protection for archive services. EAG guidelines on the implementation of the General Data Protection Regulation in the archive sector
Autor : © European Archives Group
Fecha : octubre de 2018.
Traducción de esta versión: Archivo de Castilla-La Mancha
Servicio de Protección de Datos de la Junta de Comunidades de Castilla-La Mancha

SUMARIO

18. Evaluación de impacto de la protección de datos y consulta previa (art. 35-36)

VI. Medidas de transparencia y fomento del cumplimiento.

19. Registros de actividades del tratamiento (art. 30).
20. Delegado/a de Protección de Datos (art. 37): ¿necesitan los archivos nombrar un/una DPD?

Anexos:

Glosario
Dónde buscar más orientación

ACRÓNIMOS Y ABREVIATURAS UTILIZADAS EN ESTAS DIRECTRICES

DIRECTIVA 95/46 / CE: Directiva 95/46 / CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, sobre la protección de las personas físicas en lo relativo al tratamiento de datos personales y la libre circulación de dichos datos.

APD: Autoridad de Protección de Datos

DPD: Delegado/a de Protección de Datos

GAE: Grupo de archivos europeos

CEPD: Comité Europeo de Protección de Datos

RGPD: Reglamento general de protección de datos, es decir, el *Reglamento (UE) 2016/679 de Parlamento Europeo y del Consejo, de 27 de abril de 2016, sobre la Protección de las personas físicas en el tratamiento de datos personales y sobre la libre circulación de dichos datos, y por la que se deroga la Directiva 95/46 / CE (Reglamento general de protección de datos)*

I. INTRODUCCIÓN

1. **Destinatario:**

Estas directrices están dirigidas a instituciones públicas y privadas que poseen Archivos, es decir, documentos que han sido seleccionados para su conservación permanente. No solo están dirigidas a Archivos Nacionales o a Archivos Estatales sino también a Archivos Regionales y Municipales, Museos, Bibliotecas, Fundaciones y otras entidades públicas y privadas que custodian archivos.

2. **Objetivo:**

Estas directrices tienen la intención de proporcionar información básica y orientaciones prácticas a los archiveros y archiveras en relación a los retos específicos para la aplicación del Reglamento General de Protección de Datos (RGPD) en el sector de los archivos.

3. **Alcance.**

Al igual que cualquier otra entidad pública y privada, los servicios de archivo tratan datos personales con respecto a su propio personal. Estas directrices no proporcionan orientaciones para el tratamiento de datos personales por un servicio de archivo en su función como gestor del personal. Tampoco estas directrices pretender ser una guía para el tratamiento de datos personales de los usuarios, de donantes, de contratistas, y así sucesivamente. Las Autoridades Nacionales de Protección de Datos y los gobiernos nacionales, la Comisión Europea, el Comité Europeo de Protección de Datos y otros actores ya están dando orientación sobre tales asuntos (ver el Apéndice: *¿Dónde buscar más orientación?*). Estas directrices se centran exclusivamente sobre el tratamiento de datos personales contenidos en los fondos documentales de los archivos.

4. El **RGPD: las mismas reglas en la UE (pero con excepciones para el sector de los archivos)**

Un reglamento de la UE es un acto legislativo vinculante que debe aplicarse en su totalidad en toda la Unión. La UE decidió adoptar un reglamento, en lugar de otra directiva - para reemplazar la legislación anterior de protección de datos (Directiva de la UE 95/46 / EC) para tener normas más uniformes en todos los Estados miembros. Sin embargo, el RGPD deja cierto margen para que los Estados miembros introduzcan excepciones en determinadas áreas. Una de ellas es para "fines de archivo en interés público"; otra es para la investigación histórica. Los y las archiveras tienen que ver si sus legisladores nacionales han aprovechado esta oportunidad que brinda el RGPD para regular dichas excepciones.

5. **Minimización de datos frente a preservación permanent**e.

Un principio clave de la RGPD es la minimización de datos. En realidad, no es algo nuevo: la Directiva 95/46 / CE[1] ya estaba basada sobre este principio. Los datos personales deben ser recogidos y tratados solo si es necesario hacerlo y deberían ser “mantenidos en una forma que permita la identificación de los datos de los titulares” (es decir, la persona a la que se refieren los datos) solo mientras sea necesario para lograr la finalidad para el cual se recogieron los datos personales (art. 5 (1) apartados (b) y (e)). Si no se hubieran permitido excepciones a este principio, en el futuro ya no habría archivos que contuvieran datos personales. Pero los legisladores de la UE introdujeron algunas excepciones a esta regla. Reconocieron que los archivos son necesarios para hacer cumplir los derechos fundamentales. De hecho, el RGPD afirma que “los datos personales pueden almacenarse por períodos más largos en la medida en que los datos personales se traten únicamente para fines de archivo de interés público, investigación científica o histórica. Sin embargo, esto está sujeto a condición de que se adopten las medidas apropiadas "para salvaguardar los derechos y libertades del interesado" (art. 5 (1) apartado (e)).

6. **El tratamiento de datos personales solo cuando es realmente necesario hacerlo no es nada nuevo para las personas que trabajan en los archivos**.

Una de las funciones clave de archivo es la selección de documentos para su conservación permanente. Sólo un porcentaje muy pequeño de los documentos generados o recibidos por el Estado y otras administraciones públicas, o por entidades privadas en el ejercicio de sus funciones, termina en instituciones archivísticas. Los y las profesionales seleccionan para su conservación permanente solo aquellos documentos que son necesarios para garantizar los derechos de los ciudadanos y para la investigación histórica. Las instituciones archivísticas deberían hacer públicos los criterios generales que se aplican para la selección de documentos para su conservación permanente y deberían poder explicar por qué decidieron conservar fondos de archivo específicos que contenían datos personales.

7. **Archivar datos personales no es lo mismo que facilitar su acceso**:

En todos los países miembros de la UE, la legislación nacional de cada Estado establece normas acerca del acceso a documentos custodiados en los archivos públicos. El plazo para permitir el libre acceso a los documentos que contienen datos personales, es distinto según cada país y según la naturaleza de los datos personales. En Italia, los datos personales que revelan el origen racial o étnico, las opiniones políticas y religiosas, la pertenencia a partidos y a sindicatos, no son accesibles durante 40 años, mientras que aquellos que revelan la salud y la vida sexual, el plazo es de 70 años; y los documentos que pueden revelar la identidad de una madre que quiso dar a luz de forma anónima son inaccesibles

[1] Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre 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.

durante 100 años. Los plazos de inaccesibilidad pueden ser incluso más largos; Por ejemplo, en Rumania, los registros médicos y los registros de estado civil son inaccesibles desde la fecha de su creación durante 100 años, mientras que los documentos relacionados con la vida privada de una persona son inaccesibles durante 40 años desde la fecha de su fallecimiento. Los ciudadanos pueden confiar en los servicios de Archivo: no harán accesibles sus datos personales indebidamente.

8. **El RGPD no modifica el plazo de acceso a los documentos que contienen información sobre datos personales.**

El Reglamento incluye disposiciones relativas al derecho de los ~~las personas~~ interesados a acceder a los datos que les conciernen. No incluye normas relativas al acceso a los archivos por el público en general. Los plazos de inaccesibilidad a los documentos que contengan datos personales seguirán siendo los mismos.

9. **El RGPD no modifica las leyes de libertad de información**.

La Carta de Derechos Fundamentales de la Unión Europea[2] considera tanto la protección de los datos personales y la libertad de expresión e información (que incluye la libertad de recibir y comunicar información) como derechos fundamentales. El RGPD no modifica las leyes de la libertad de información. Establece que “los datos personales en documentos en poder de una autoridad pública o de un organismo público podrían ser hechos públicos por esa autoridad u organismo público, si esta apertura estaba prevista por la legislación de la Unión o del Estado miembro del que esa autoridad pública u organismo público depende.” (Considerando 154).

10. **El RGPD no modifica las leyes de libertad de expresión.**

Los usuarios de archivos, incluyen, entre otros, periodistas, académicos y otros investigadores de todos los ámbitos sociales que, en muchos casos, publicarán sus hallazgos. El RGPD no modifica las leyes de prensa y otras normas relativas a la libertad de expresión. Dispone que: “Los Estados Miembro conciliarán por ley, el derecho a la protección de datos personales de conformidad con el presente Reglamento con el derecho a la libertad de expresión e información, incluidos los tratamientos con fines periodísticos y los fines académicos, artísticos o literarios. "(art. 85). Para este fin, los Estados miembro podrían mantener ciertas excepciones a las disposiciones de la RGPD (art. 85).

[2] 2000/C364/01

11. **Esta Guía y sus pautas no son un código de conducta**.

El RGPD fomenta “la elaboración de códigos de conducta destinados a contribuir a la correcta aplicación del Reglamento (art. 40.1). Además, dispone que “Asociaciones y otros organismos representativos de los Responsables y Encargados del tratamiento podrán elaborar códigos de conducta " (art. 40 (2)) y dictar un procedimiento específico para la aprobación de códigos de conducta por la Autoridad Nacional de Protección de Datos (si el código tuviera solo un alcance nacional) o por el Comité Europeo de Protección de Datos y por la Comisión de la UE (si el código se aplicara en diferentes Estados miembros de la UE).

Las presentes Directrices fueron redactadas por el Grupo de Archivos Europeos (EAG), un grupo de expertos de la Comisión Europea compuesto por representantes de Archivos Nacionales y de las Direcciones Generales de Archivos de los Estados miembros de la UE. Las Directrices no pasaron por el procedimiento de aprobación previsto para los códigos de conducta en el art. 40 del RGPD. Debería ser considerado un documento orientativo.

II. PRINCIPIOS GENERALES

1. PRINCIPIOS GENERALES RELACIONADOS CON EL TRATAMIENTO DE DATOS PERSONALES. (ART. 5)

Los archiveros y las archiveras deberán conocer algunos principios generales, relativos al tratamiento de los datos personales, que se hallan en el art. 5 de la RGPD, el cual establece que:

1. Los datos personales serán:

a) tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»);
b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales («limitación de la finalidad»);
c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»);
d) exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan («exactitud»);
e) conservados de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado («limitación del plazo de conservación»);
f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»).

2. El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»).

Estos principios tienen muchas consecuencias prácticas para los servicios de archivo y, por lo tanto, deberían tenerse siempre en cuenta. Las archiveras y los archiveros están familiarizados en garantizar el principio de 'confidencialidad', ya que es una práctica común en los servicios de archivo proteger la información confidencial de los accesos no autorizados. No obstante, algunas de las implicaciones de tales principios son menos obvias. Por ejemplo:

• El principio de 'transparencia' significa, entre otras cosas, que los servicios de archivo tienen que publicar información sobre su misión, clara y fácil de usar, y en particular definir por qué y cómo tratan los datos personales, y cómo los interesados pueden acceder a ellos.

• El principio de "integridad" significa, entre otras cosas, que una mala práctica archivística, que diera lugar a la pérdida de documentos que contienen datos personales, constituye no solo una violación de los principios archivísticos profesionales y de las leyes de archivos, sino también una violación del RGPD.

2. LEGALIDAD DEL PROCESO (ART. 6)

Según el RGPD, el tratamiento de datos personales es legítimo solo si al menos uno de los apartados enumerados en el art. 6 se aplica, esto es:

"la persona titular de los datos ha dado su consentimiento en el tratamiento de sus datos personales"; "el tratamiento es necesario para la ejecución de un contrato en el que la persona interesada sea parte"; el "tratamiento es necesario para el cumplimiento de una obligación legal a la cual está sujeto el Responsable", etc.

Es de interés para los archiveros y las archiveras la condición establecida en (1) punto (e)), por la que el tratamiento de datos personales es legítimo si son "necesarios para el desempeño de una tarea realizada en interés público".

El RGPD remite a la legislación de la UE o la ley nacional para determinar qué tipo de actividades son consideradas como "de interés público". La ley nacional puede incluir disposiciones que definan el tratamiento de archivos por una institución determinada, o el tratamiento de ciertos tipos de archivos para el cumplimiento de "una misión realizada en interés público".

3. EL RGPD PROTEGE ÚNICAMENTE LOS DATOS PERSONALES DE LAS PERSONAS VIVAS (PERO LA LEY NACIONAL PUEDE PROTEGER TAMBIÉN LOS DATOS DE PERSONAS FALLECIDAS)

El RGPD protege los datos personales de las personas vivas. No se aplica a los datos personales de personas fallecidas. Sin embargo, las archiveras y los archiveros deberían tener en cuenta que las leyes nacionales pueden hacerlo.
De hecho, el RGPD estipula que "los Estados miembros pueden prever normas relativas al tratamiento de datos personales de personas fallecidas". (Considerando 27).

¿Cómo pueden saber los archiveros y las archiveras si una persona titular de los datos ha fallecido? En la mayoría de los casos no pueden. Sin embargo, pueden asumir razonablemente que las personas nacidas hacen más de cien años ya no están vivos. Por ejemplo, una archivera o un archivero que estén tratando archivos personales de soldados que lucharon en la I Guerra Mundial pueden asumir que ya no están vivos y que por lo tanto el RGPD no se aplica a esos

archivos. Sin embargo, muchos otros casos no serán tan claros. Las archiveras y los archiveros deberán realizar valoraciones caso por caso de la posibilidad de que los fondos de archivos a su cargo contengan datos personales de personas vivas.

III. ¿QUÉ ES “FINES DE ARCHIVO EN INTERÉS PÚBLICO?

4. DIFERENTES REGLAS PARA DIFERENTES ARCHIVOS (“FINES DE ARCHIVO EN INTERÉS PÚBLICO” EN EL CONSIDERANDO 158)

El RGPD permite una serie de excepciones a favor de "fines de archivo en interés público". El Considerando 158 explica el significado de esta expresión.

> “Las autoridades públicas o los organismos públicos o privados que *llevan registros de interés público* deben ser servicios que están obligados, con arreglo al Derecho de la Unión o de los Estados miembros, a adquirir, mantener, evaluar, organizar, describir, comunicar, promover y difundir registros de valor perdurable para el interés público general y facilitar acceso a ellos”. (cursivas resaltadas en el documento original)

¿Qué servicios de archivo entran en esta definición? Como se puede ver, no es la naturaleza de los archivos, sino la misión de la institución que los custodia lo que determina si esta excepción se puede aplicar. Según la definición de RGPD, es seguro afirmar que, al igual que el Archivo Histórico de la Unión Europea, los Archivos Nacionales y los otros Archivos históricos dependientes del Estado o de otros organismos públicos, llevan a cabo “fines de archivo en interés público”.

De acuerdo con la legislación de los Estados miembros, otras instituciones que conservan archivos pueden incluirse en esta definición. Por ejemplo, la ley nacional podría regular qué organismos específicos tienen la misión de adquirir, conservar y poner a disposición de los investigadores los documentos personales de escritores; o se podría crear un museo sobre la Historia de la Ciencia que incluyera entre sus tareas, la adquisición y conservación de documentos personales de los científicos. La ley de un Estado miembro puede crear un instituto para la historia de un régimen autoritario del pasado, cuya misión incluya la preservación del patrimonio documental relativo a las víctimas de la represión política.

Es importante tener en cuenta que cuando el RGPD se refiere a una "ley nacional", esto no significa que sean solo leyes singulares aprobadas por los parlamentos nacionales. El considerando 41, de hecho, estipula que «cuando el presente Reglamento hace referencia a una base jurídica o una medida legislativa, esto no exige necesariamente un acto legislativo adoptado por un parlamento”. De acuerdo con los diferentes sistemas constitucionales, el instrumento legal que puede asignar a una Entidad la obligación legal de adquirir, conservar, organizar y comunicar los Archivos puede cambiar de un país a otro. Por ejemplo, podría ser una ley nacional, una ley regional, un decreto ministerial, y así sucesivamente. En cualquier caso, los archiveros y las archiveras deben tener en cuenta que un servicio de archivo u otra institución cultural que tenga la misión legal de adquirir, conservar y proporcionar acceso a los archivos para el interés público general, entraría en la definición del considerando 158.

No todas las entidades que conservan archivos tienen la obligación legal de adquirirlos y, por lo tanto, no todos ellos están comprendidos en la definición del considerando 158. Sin embargo, en muchos casos, tales entidades tienen una clara misión cultural y preservan los archivos con la finalidad de investigación histórica. El RGPD permite excepciones para el tratamiento de datos personales con fines de investigación histórica, que se disponen por todo el Reglamento y, en particular, en el artículo 89.

Finalmente, los archivistas deben ser conscientes de que las excepciones a favor de los "fines de archivo en interés público" se refiere únicamente al tratamiento de datos personales incluidos en los fondos del archivo que mantienen los servicios del archivo. Todos los demás datos personales en tratamientos llevados a cabo por los servicios del archivo están sujetos a las mismas reglas que se aplican a cualquier otra entidad pública o privada. En otras palabras, cuando los servicios de archivo tratan los datos personales de los usuarios o de los estudiantes que participan en actividades educativas, o de participantes en conferencias, etc., no gozan de ninguna excepción a las normas.

5. GARANTÍAS Y EXCEPCIONES RELATIVAS AL TRATAMIENTO CON FINES DE ARCHIVO EN INTERÉS PÚBLICO, CIENTÍFICO O FINES DE INVESTIGACIÓN HISTÓRICA O FINES ESTADÍSTICOS (ART. 89)

En todo el RGPD uno puede encontrar muchas referencias a los archivos y a la investigación histórica. Varios artículos que establecen deberes o prohibiciones para el responsable, de hecho, permiten excepciones cuando el tratamiento es necesario para fines de archivo en interés público, fines de investigación científica o histórica.

Además, el RGPD incluye un artículo específicamente dedicado al “tratamiento con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos” (art. 89). El primer párrafo de este artículo fija las reglas que son comunes tanto para el tratamiento de datos personales "con fines de archivo de interés público" como para el tratamiento con " fines de investigación científica o histórica o fines estadísticos”.

1. El tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos estará sujeto a las garantías adecuadas, con arreglo al presente Reglamento, para los derechos y las libertades de los interesados. Dichas garantías harán que se disponga de medidas técnicas y organizativas, en particular para garantizar el respeto del principio de minimización de los datos personales. Tales medidas podrán incluir la seudonimización, siempre que de esa forma puedan alcanzarse dichos fines. Siempre que esos fines pueden alcanzarse mediante un tratamiento ulterior que no permita o ya no permita la identificación de los interesados, esos fines se alcanzarán de ese modo.

El artículo 89 establece además que:

2. Cuando se traten datos personales con fines de investigación científica o histórica o estadísticos el Derecho de la Unión o de los Estados miembros podrá establecer excepciones a los derechos contemplados en los artículos 15, 16, 18 y 21…

3. Cuando se traten datos personales con fines de archivo en interés público, el Derecho de la Unión o de los Estados miembros pueden prever excepciones a los derechos contemplados en los artículos 15, 16, 18, 19, 20 y 21…

En ambos casos, las excepciones mencionadas son posibles

...bajo las condiciones y garantías contempladas en el párrafo 1 de este Artículo en la medida en que tales derechos puedan hacer imposible o perjudicar gravemente la consecución de los objetivos específicos, y tales excepciones sean necesarias para el cumplimiento de esos fines.

El principio de minimización de datos y la obligación de adoptar las garantías adecuadas con objeto de proteger los derechos de los interesados son, por lo tanto, comunes tanto al “tratamiento para fines de archivo en interés público como para el tratamiento con fines "de investigación científica o histórica o fines estadísticos”. Pero la aplicación concreta de estos principios será diferente en cada una de estas áreas.

Cuando se hace investigación médica es importante preservar la correlación de los diferentes datos médicos relativos a un determinado paciente, pero la identidad del mismo es irrelevante. En este caso, la seudonimización de los documentos sanitarios sería una medida apropiada. Sin embargo, en interés de los interesados, un servicio de archivo que custodia documentos de interés público tiene que preservar la integridad de los documentos sanitarios que hayan sido seleccionados para su conservación permanente. Por ejemplo, recientemente algunos países pudieron pagar una compensación a las personas que habían sido sometidos a la esterilización obligatoria hace décadas debido a que la integridad de los documentos sanitarios estaba garantizada. La historia europea proporciona muchos otros casos, en los que la conservación de documentos con datos personales se ha conservado integralmente y ha servido como instrumento para el restablecimiento de los derechos de los interesados.

Aplicar el derecho a la verdad y el derecho a la reparación de las víctimas por violaciones graves de los derechos humanos requieren la conservación integral de los archivos

Las víctimas de persecuciones fascistas y nazis o del uso nazi del trabajo esclavo podrían ser identificados e indemnizados gracias a que los archivos que contenían datos personales han sido conservados. Igualmente, tras la caída del comunismo, la conservación integral de los archivos ha servido como instrumento para la devolución de propiedades confiscadas. El RGPD fomenta la conservación integral de los archivos que documentan violaciones de derechos. De hecho, el considerando 158 establece:

"*Los Estados miembros también debe estar autorizados a establecer el tratamiento ulterior de datos personales con fines de archivo, por ejemplo a fin de ofrecer información específica relacionada con el comportamiento político bajo antiguos regímenes de Estados totalitarios, el genocidio, los crímenes contra la humanidad, en particular el Holocausto, o los crímenes de guerra*."

Cuando toman una decisión sobre la conservación o eliminación de registros que contienen datos personales, las archiveras y los archiveros deberían recordar que la protección de datos personales debe ser ponderada respecto al derecho a la justicia, al derecho a la verdad y al derecho a la reparación y a la restitución a las víctimas de violaciones graves de los derechos humanos.

El RGPD reconoce que el tratamiento con fines de archivo de interés público, con fines de investigación histórica o científica o con fines estadísticos requiere diferentes tipos de medidas con objeto de aplicar el principio de minimización de datos y no siempre requiere seudonimización, sólo cuando "esos fines pueden alcanzarse de ese modo".

Los archiveros y las archiveras aplican el principio de minimización de datos de forma distinta a como lo hacen el personal investigador científico y estadístico. En primer lugar, seleccionan los documentos que contienen datos personales de uso permanente, conservándolos solo cuando es realmente necesario hacerlo, de conformidad con la misión que la normativa asigna a sus servicios de Archivo. Además, aplican las normas relativas al acceso a la información contenida en los archivos, impidiendo el acceso a los documentos que contienen datos personales durante el plazo que marquen sus leyes nacionales. Las restricciones legales sobre el acceso a los archivos difieren de un país a otro y para ciertos tipos de datos personales, el período de inaccesibilidad puede llegar a ser de hasta 120 años.

Cuando los documentos que contienen datos personales se vuelven accesibles, pero hay una posibilidad que la persona titular de los datos esté todavía vivo, las archiveras y los archiveros se abstienen de cualquier tratamiento que pueda ser

perjudicial para la dignidad del interesado. Siempre deben mantener presente lo establecido en el artículo 1 de la Carta de los Derechos Fundamentales de la Unión Europea: “La dignidad humana es inviolable. Debe ser respetada y protegida”. Una promulgación concreta de este principio es el de abstenerse de publicar documentos de archivo en línea o instrumentos de descripción cuya difusión pueda perjudicar la dignidad de las personas titulares de los datos.

Los servicios de archivo también pueden hacer uso de la seudonimización, pero si se practica por los servicios de archivo debería ser completamente reversible y hacerse de una forma que no se ponga en peligro el valor probatorio de los documentos. En el caso de los datos personales conservados con fines de archivo de interés público, los servicios de archivo deberían almacenar los datos originales sin modificaciones en una instalación de almacenamiento protegida y, si tales fines pueden cumplirse de esa forma, hacer una copia seudonimizada de los datos personales para su acceso por parte de los investigadores.

¿El RGPD permite la conservación de archivos de empresas que contengan información personal?

Algunas empresas privadas conservan archivos centenarios, con datos personales entre ellos, que son tesoros de información para los historiadores. ¿Podrán los historiadores del futuro acceder a fuentes de archivo similares? En otras palabras, ¿es posible bajo el RGPD la conservación de archivos de empresas que contengan datos personales? No hay una respuesta sencilla para tal pregunta.

Los documentos creados por entidades privadas pueden ser tratados para archivo con fines de interés público como los creados por organismos públicos. Sin embargo, tal tratamiento solo se califica como con "fines de archivo en interés público" si se realiza por un organismo público o privado que tiene “la obligación legal de adquirir, conservar, valorar, organizar, describir, comunicar, promover, difundir y proporcionar acceso a documentos de valor duradero para el público en general". (Considerando 158). Lo que significa "obligación legal" difiere en el derecho civil y en el derecho común de un país a otro.

Los organismos que tienen la misión de investigación histórica, pero no tienen una obligación legal de adquirir y tratar archivos, pueden tratar archivos de empresas que contengan datos personales con fines de investigación histórica.

De hecho, tanto el principio de “limitación de la finalidad” como el de “limitación de almacenamiento” (art. 5 (1) apartados b) y e)) permiten excepciones no solo para fines de archivo en interés público, sino también con fines de investigación histórica. Tales excepciones están sujetas a la implementación de medidas apropiadas para salvaguardar los derechos y libertades del interesado. Las interpretaciones de tales disposiciones se irán aclarando a medida que las Agencias de Protección de Datos y el Consejo Europeo de Protección de Datos adopten decisiones y publiquen pautas a seguir.

IV. LOS DERECHOS DE LOS TITULARES DE DATOS

6. LA CUESTIÓN PRINCIPAL: OTORGAR A LAS PERSONAS CONTROL SOBRE SUS DATOS PERSONALES

Uno de los objetivos principales del RGPD es otorgar a las personas el control sobre sus datos personales. Por esta razón, les provee de un conjunto completo de derechos con respecto a sus datos personales (el derecho a saber qué datos se tratan y por qué, el derecho a acceder, cancelar y transferir sus datos, etc.), de los que solo se permiten excepciones limitadas. Archivar con fines de interés público es uno de los fundamentos para establecer excepciones a los derechos de las personas titulares de los datos. En dos casos, el derecho a la información (art. 14) y el "derecho al olvido" (art. 17) - el RGPD introduce directamente excepciones con fines de archivo en interés público. En los demás supuestos, se permite a los Estados miembros hacerlo. Como ya se ha dicho, el mencionado art. 89 permite a los Estados miembros establecer excepciones a los derechos establecidos en los artículos 15, 16, 18, 19, 20 y 21. Esto significa que, en cada país, respecto a algunos de los derechos de las personas titulares de los datos, las archiveras y los archiveros pueden tener que cumplir con diferentes leyes.

En todos los casos, las excepciones no son absolutas, sino que están sujetas a las garantías previstas en el art.º 89, por ejemplo, las medidas técnicas y organizativas dirigidas a aplicar el principio de minimización de datos y a la protección de los derechos y libertades del interesado. Además, los servicios de archivo deberían permitir que las personas titulares de los datos tengan el mayor control posible sobre sus datos. Este principio tiene especial relevancia cuando los servicios de archivo conservan los documentos de personas vivas, que los donaron, vendieron o depositaron en servicios de archivo; o cuando conservan las entrevistas orales recogidas durante proyectos de historia oral. Sin embargo, los servicios de archivo no pueden tener en cuenta las peticiones de los titulares de los datos personales, si eso implica tener que violar la misión legal de los servicios de archivo de preservar la integridad de los archivos y de organizarlos, describirlos y ponerlos a disposición del público.

7. LA INFORMACIÓN QUE DEBE SER PROPORCIONADA CUANDO LOS DATOS PERSONALES NO SE HAN OBTENIDO DEL TITULAR DE LOS DATOS (ART. 14).

El RGPD establece que el Responsable debe proporcionar a los titulares de los datos cierta información sobre el tratamiento que él o ella realiza. Esto es aplicable incluso si el Responsable no obtuvo los datos personales directamente del interesado, tal como se establece en el artículo 14. Esta es normalmente la situación de los servicios de archivo que tratan documentos que contienen información personal que no reunieron, pero que fue recopilada por la entidad que creó el archivo.

Sin embargo, el RGPD permite algunas excepciones, y una concierne a los archivos. De hecho, el Artículo 14 establece que, la obligación de proporcionar información a las personas titulares de los datos cuando los datos personales no se obtuvieron de ellos, no se aplica cuando resulte “imposible" o suponga un esfuerzo desproporcionado, en particular para el tratamiento con fines de archivos de interés público, fines de investigación científica o histórica o fines estadísticos. En esos casos, el Art.º14 anima explícitamente a que los Responsables pongan a disposición pública la información sobre el tratamiento.

Cuando los servicios de archivo adquieren, organizan, describen, conservan y ponen a disposición de los investigadores los fondos de archivo que contienen datos personales relativos a un número indeterminado de personas, en la medida en que informar a los interesados sobre tal tratamiento fuera “imposible o implicara un esfuerzo desproporcionado”, la mejor línea de acción parece ser hacer disponible la información sobre dicho tratamiento en el sitio web del servicio de archivo, para que el público en general pueda enterarse de la misma. En algunos casos, puede emprenderse un esfuerzo más dirigido a informar a los titulares de datos. Por ejemplo, si un servicio de archivo adquiere el archivo de una asociación, un partido político o un sindicato, que trató datos personales solo de sus asociados y asociadas, podría llegar a un acuerdo con ellos para utilizar sus canales de información (boletines, sitios web, listas de correo, etc.) para informar sobre el tratamiento que realizará el servicio de archivo.

El Art.º14 incluye una lista detallada de la información que los Responsables deberían proporcionar a las personas titulares de datos cuando los datos personales no se han obtenido de ellos. En pocas palabras, los servicios de archivo deberían explicar en términos fácilmente comprensibles para alguien que no sabe nada sobre los archivos, qué tipo de tratamiento de datos realizan y por qué, y cuál es la base legal para su tratamiento. Por otra parte, deberían informar a los y las titulares de datos cómo pueden acceder a sus datos y también explicar qué fondos de archivo son accesibles a los usuarios y a las usuarias, así como las limitaciones legales a que está sujeto el acceso a documentos que contienen información personal. Por último, si los titulares de los datos contactan con los servicios de archivos para solicitar información sobre el tipo de tratamiento que realizan, el personal de los archivos debería estar preparado para proporcionar a los titulares de los datos toda la información posible existente.

8. EL DERECHO DE ACCESO POR LOS TITULARES DE LOS DATOS (ART. 15)

Como regla general, las personas titulares de los datos tienen el derecho de obtener confirmación del Responsable si están o no están siendo tratados sus datos personales. Por otra parte, también tienen derecho a conocer los fines del tratamiento, las categorías de datos personales que se traten y cualquier otra información relativa al tratamiento de sus datos personales.

Los servicios del Archivo tratan grandes cantidades de datos personales que han sido reunidos por otras entidades. Cuando estas entidades transfieren sus documentos a un servicio de archivo, deberían también transferir los

“instrumentos de descripción” para permitir que los servicios de archivo sepan, entre otras cosas, que datos personales contienen los documentos transferidos. Sin embargo, frecuentemente sucede que los servicios de archivo reciben transferencias sin instrumentos de descripción detallados, sino solo con una hoja de remisión genérica. En consecuencia, las archiveras y los archiveros no pueden saber qué datos personales están incluidos en los documentos transferidos. Además, los servicios de archivos a menudo reciben archivos que han perdido su orden original y requieren de un cuidadoso trabajo de organización para restablecerlo.

Estas condiciones provocan dificultades objetivas para aplicar algunos de los derechos sobre los datos personales previstos en el Reglamento. El RGPD reconoce estos derechos y, como ya se ha mencionado, el artículo 89 prevé que las leyes de la Unión Europea y de los estados miembros pueden introducir excepciones a los derechos de los interesados.

Por tanto, los archiveros y las archiveras deberían verificar si la legislación nacional incluye excepciones al derecho de acceso de las personas titulares de los datos personales, de acuerdo con lo previsto en el artículo 15 del RGPD. Tales excepciones protegen a las archiveras y a los archiveros de cualquier responsabilidad si no pueden cumplir totalmente con las solicitudes de los y las titulares de datos para obtener información sobre el tratamiento de sus datos personales por un servicio de archivo. Sin embargo, estas excepciones no les eximen de hacer todo lo posible por cumplir con tales solicitudes de los interesados.

Si uno o una titular de datos personales se acerca a un servicio de archivo con el fin de acceder a sus datos personales, los archiveros y las archiveras deberían proporcionar toda la ayuda posible para explicar cómo investigar en el archivo, para indicar que fondos del archivo con la mayor probabilidad contienen información sobre sus datos personales y para asesorar cómo consultar los instrumentos de descripción y someterse a las solicitudes sobre la consulta de los expedientes. Si esas personas tienen dificultades específicas para hacer una investigación debido a su edad, el nivel de alfabetización o algún impedimento físico, los servicios de archivo les proporcionarán asistencia especial, en la medida de lo posible, teniendo en cuenta las restricciones que tengan, tales como la falta de personal.

9. EL DERECHO DE RECTIFICACIÓN (ART. 16)

El Art.16 de la RGPD estipula que los interesados tienen derecho a que sus datos personales sean rectificados si son inexactos y sean completados si están incompletos. El Responsable tiene que cumplir con las solicitudes del interesado "sin demoras indebidas".

Los servicios de archivo deben garantizar la integridad de los archivos en orden a conservar el valor probatorio de los documentos. Esto es necesario para proteger los derechos de los interesados. Por ejemplo, los archivos policiales de los típicos regímenes represivos suelen incluir información peyorativa sobre

opositores políticos. El mantenimiento de la integridad de dichos archivos es necesario para permitir que las personas titulares de los datos soliciten una indemnización por la discriminación que sufrieron a manos del régimen represivo.

El RGPD permite conciliar la responsabilidad de los servicios de archivo para mantener la integridad de los documentos y el derecho de los interesados a que sus datos personales incompletos sean completados. La rectificación se puede lograr "mediante una declaración adicional". Además, como ya se ha mencionado, el artículo 89 establece que la legislación de la Unión o de los Estados miembros puede introducir excepciones a los derechos de los interesados en los datos, de acuerdo con lo previsto en el artículo 16.

Los servicios de archivo facilitarán el ejercicio del derecho del interesado a tener sus datos actualizados, rectificados o completos mediante "una declaración adicional" y garantizar que los datos se custodien de manera que el material original permanezca separado y diferenciado de cualquier otra información complementaria.

10. EL DERECHO DE SUPRESIÓN ('DERECHO AL OLVIDO') (ART. 17)

El "derecho al olvido" dentro de la UE se estableció por primera vez en la decisión “histórica” de 2014 del Tribunal de Justicia de la Unión Europea en el caso Google-España. El Tribunal ordenó a Google-Spain eliminar de los resultados de búsqueda dos informes sobre la insolvencia de un ciudadano español, Mario Costeja González. Los informes habían sido legalmente publicados por un periódico en 1998 y continuaban apareciendo de forma destacada cuando se buscaba el nombre de Costeja. La decisión del Tribunal dejaba intactos los archivos analógicos y digitales del periódico. Solo se aplica en Google al resultado de la búsqueda por el nombre de Costeja (los informes permanecen recuperables cuando se utilizan otros términos de búsqueda). Después de la decisión del Tribunal, las personas pueden solicitar que sus datos personales (si son inadecuados, irrelevantes o ya no son pertinentes) se desvinculen (desindexar) de los motores de búsqueda para que dichos datos ya no aparezcan si una persona busca su nombre.

La decisión del Tribunal de Justicia de la UE en el caso de Google España se basó en la Directiva 95/46 / CE que no incluía explícitamente el "derecho al olvido". Por el contrario, el RGPD usa esta expresión en el título del artículo 17 “Derecho de supresión” ('derecho al olvido')".

Bajo el RGPD, el derecho al olvido no hace referencia a la desvinculación sino al borrado real de los datos personales. De hecho, el artículo 17 otorga a las personas titulares de los datos el derecho a obtener del Responsable del tratamiento que borre los datos personales que le conciernen sin dilación indebida.

Este derecho puede aplicarse cuando “los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos” o cuando “el

interesado retire el consentimiento” para seguir tratando sus datos, así como en algunas otras circunstancias. Al mismo tiempo el derecho al olvido está sujeto a diferentes restricciones, y no se aplicará si el tratamiento es necesario para fines de archivo en interés público, si el borrado fuera imposible ejecutarlo o si perjudicara gravemente el logro de los objetivos de dicho tratamiento, (art. 17 (3)).

El considerando 158 explica que las autoridades públicas y otros organismos que lleven registros de interés público son servicios que "están obligados, con arreglo al Derecho de la Unión o de los Estados miembros” a tratar archivos seleccionados para su conservación permanente. Por lo tanto, el borrado de datos personales incluidos en documentos de archivo, haría imposible que estos servicios llevaran a cabo la misión que la ley les asigna. Por lo tanto, el derecho de supresión del artículo 17 de la RGPD no se aplica a documentos seleccionados para su conservación permanente por los servicios de archivo que se encuentran bajo la definición del considerando 158.

Al mismo tiempo, los archiveros y las archiveras deberían recordar que el derecho al olvido como lo establece el Tribunal de Justicia de la UE (es decir, no el borrado, sino “la no inclusión” de los datos personales) puede ser ejecutado por los Servicios de Archivo sin menoscabo de su misión. De hecho, la desvinculación o exclusión, u otras formas de impedir la búsqueda por los motores de Internet mediante los nombres de las personas, no afecta a la integridad de los documentos, ni pone en peligro su conservación permanente. Además, los servicios de archivo pueden impedir la búsqueda de nombres de un documento en línea, mientras mantienen que sean recuperables los nombres de personas utilizando soluciones de búsqueda diferentes.

En primer lugar, los servicios de archivo deben abstenerse de publicar documentos de archivo en línea o de índices o “instrumentos de descripción” que contengan datos personales que puedan poner en peligro la dignidad de los interesados. Además, cada vez que publican documentos de archivo o instrumentos de descripción en línea que contienen datos personales, con datos de personas vivas, tienen que tener en cuenta, de acuerdo con la naturaleza de los datos personales, si sería conveniente publicarlos en un área de acceso restringido de sus sitios web que esté fuera del alcance de los motores de búsqueda. Mediante un análisis caso a caso, las archiveras y los archiveros evaluarán cómo buscar el equilibrio entre su obligación legal de "adquirir, mantener, evaluar, organizar, describir, comunicar, promover y difundir registros de valor perdurable para el interés público general y facilitar acceso a ellos" (considerando 158), y el principio de minimización de datos (art. 5), que les obliga a limitar el tratamiento de datos personales a aquello que sea necesario.

11. DERECHO A LA LIMITACIÓN DEL TRATAMIENTO (ART. 18) Y DERECHO DE OPOSICIÓN (ART. 21)

El RGPD otorga a las personas titulares de datos obtener del Responsable tanto el derecho a la limitación del tratamiento como el derecho a oponerse al tratamiento de datos personales que les conciernen. ¿Cuáles son las diferencias

entre tales derechos y cuáles son sus implicaciones prácticas relevantes para los servicios de archivo?

Tales derechos comparten el mismo objetivo final, el de otorgar a las personas el control sobre el tratamiento de sus datos personales, pero se aplican en diferentes circunstancias, y tienen diferentes consecuencias. Lo que más importa a los archiveros y a las archiveras es que, en el caso del tratamiento de datos personales para fines de archivo en interés público (art. 89 (3)), la legislación nacional puede introducir excepciones a esos derechos.

Bajo las circunstancias específicas enumeradas en el art. 18 (1), los interesados tienen derecho a solicitar la limitación del tratamiento de sus datos personales. Lo más relevante para los servicios de archivo es que la limitación de tratamiento no impide el almacenamiento de datos personales (art. 18 (2)). Por lo tanto, la conservación de los documentos de archivo no puede ser obstaculizada por esta limitación.

Además, los interesados tienen derecho a *oponerse a*l tratamiento de los datos personales, que les conciernen, incluso si el tratamiento "es necesario para el desempeño de una tarea realizada en interés público". En ese caso, "El Responsable ya no tratará los datos personales" (art. 21 (1)). Sin embargo, este puede continuar tratando datos personales, si puede demostrar y acreditar "…motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones" (art. 21 (1)). Esta disposición puede aplicarse a los tratamientos en los archivos por razones de interés público, pero las archiveras y los archiveros no deberían darlo por sentado. Es aconsejable que se mantengan informados sobre la interpretación que realicen los tribunales de justicia al respecto.

En primer lugar, los archiveros y las archiveras deberían verificar si los legisladores nacionales han hecho uso de la posibilidad de introducir excepciones a los derechos de la limitación del tratamiento (art. 18) y de oposición (art. 21) y, en este caso, si la legislación nacional indica cuáles son las salvaguardas adecuadas de los derechos y libertades de las personas titulares de datos que los servicios de archivo deberían tomar. Si la legislación nacional no sugiere las garantías apropiadas, los servicios de archivo evaluarán, caso a caso, cómo mejor aplicar los principios relacionados con el tratamiento de los datos personales enumerados en el art. 5 del Reglamento.

Por último, las archiveras y los archiveros deberían tener en cuenta que:

> De conformidad con el artículo 89, apartado 1, cuando los datos personales se tratan con fines de investigación científica o histórica o fines estadísticos, el interesado, por motivos relacionados con su situación particular, tendrá derecho a oponerse al tratamiento de datos personales que le conciernen, a menos que el tratamiento sea necesario para el cumplimiento de una misión realizada por razones de interés público. (art. 21 (6))

Esta disposición puede ser relevante para los archiveros y las archiveras que trabajan en museos u otras instituciones culturales, institutos u organizaciones que conservan archivos por razones de interés público, pero no pueden utilizarlo con "fines de archivo en interés público" de acuerdo con la definición del considerando 158.

12. OBLIGACIÓN DE NOTIFICACIÓN RELATIVA A LA RECTIFICACIÓN O SUPRESIÓN DE DATOS PERSONALES O LIMITACIÓN DE TRATAMIENTO (ART. 19)

El RGPD dispone que "el responsable del tratamiento comunicará cualquier rectificación o supresión de datos personales o limitación del tratamiento efectuada… a cada uno de los destinatarios a los que se hayan comunicado los datos personales, salvo que sea imposible o exija un esfuerzo desproporcionado" (art. 19). Como ya se ha mencionado, en caso de un tratamiento de datos personales con fines de archivo de interés público la legislación nacional puede introducir excepciones a los derechos de rectificación, cancelación o limitación del tratamiento. Por lo tanto, es poco probable que los datos personales incluidos en los fondos de archivo conservados por los servicios de archivo puedan ser objeto de rectificación o supresión o limitación de tratamiento.

Además, también la legislación nacional puede introducir una excepción a la obligación de notificación si los datos personales son tratados para fines de archivo en interés público (art. 89 (3)). Por último, las archiveras y los archiveros deberían tener en consideración que un Responsable del tratamiento datos debería cumplir con la obligación dictada por el art. 19, "salvo que sea imposible o exija un esfuerzo desproporcionado" y estos pueden ser muchos de los casos de los servicios de archivos.

13. DERECHO A LA PORTABILIDAD DE DATOS (ART. 20)

El RGPD otorga al interesado "…derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica" (art. 20 (1)). Además, "el interesado tendrá derecho a que los datos personales se transmitan directamente de responsable a responsable cuando sea técnicamente posible" (art. 20 (2)). Los servicios de archivo no reciben los datos personales custodiados en los fondos de archivo directamente de las personas titulares de los mismos, excepto en el caso de los archivos privados. La mayoría de los fondos de archivo tratados hoy por los servicios de archivo están en formato analógico, así que la transmisión a los interesados de los datos personales que se incluyen en un "formato estructurado, de uso común y lectura mecánica" no sería "técnicamente posible". Finalmente, los archivistas deberían ser conscientes de que la legislación nacional puede introducir excepciones al derecho de portabilidad de datos si los datos personales se tratan con fines de archivo en interés público (art. 89 (3)).

V. TRATAMIENTO DE CATEGORÍAS DE DATOS QUE REQUIERE SALVAGUARDIAS ESPECIALES

14. TRATAMIENTO DE CATEGORÍAS ESPECIALES DE DATOS PERSONALES.

El RGPD proporciona protección especial a ciertas categorías de datos personales, cuyo tratamiento podría crear riesgos significativos para los derechos y libertades fundamentales de los titulares de datos. Prohíbe:

> El tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física. (art. 9 (1))

Sin embargo, el RGPD permite algunas excepciones a esta disposición. La prohibición del tratamiento de dichos datos confidenciales no se aplica en los casos en que “el tratamiento sea necesario para fines de archivo en interés público" y para la investigación histórica. Tal tratamiento debe tener su base jurídica en una ley y debe ser "proporcional objetivo perseguido". Por otra parte, debe “…respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado". (art. 9 (2) punto (j)).

En su mayor parte, las disposiciones del artículo 9 no son nuevas. Ya la Directiva 95/46 / CE prohibía, con algunas excepciones, el tratamiento de categorías especiales de datos personales. El RGPD amplió las categorías de datos personales que merecen una protección especial, agregando a la lista que aparece en el art. 9 los “datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física”.

De conformidad con la legislación nacional de los Estados miembros de la UE, los documentos que contienen datos personales de categorías especiales están excluidas del acceso por períodos prolongados, que van desde unas pocas décadas a un siglo o aún más. Por lo tanto, los archivistas ya tienen una larga y exitosa experiencia en la aplicación de leyes que restringen el acceso a categorías especiales de datos personales.

15. TRATAMIENTO DE DATOS PERSONALES RELACIONADOS CON CONDENAS E INFRACCIONES PENALES (ART. 10)

El RGPD establece reglas muy estrictas con respecto al tratamiento de datos personales relacionados con condenas y delitos penales y no permite ninguna exención. El tratamiento de este tipo de datos personales “sólo podrá llevarse a cabo bajo la supervisión de las autoridades públicas o cuando lo autorice el

Derecho de la Unión o de los Estados miembros" La Ley debe establecer "las garantías adecuadas para los derechos y libertades de los interesados" (art. 10).

En los Estados miembros de la UE, las leyes nacionales regulan los plazos en los que, después de un cierto número de años - en general, 20 o 30 años – las sentencias de los tribunales, los expedientes judiciales y los registros penitenciarios seleccionados para la conservación permanente se transfieren a los Archivos Nacionales o a otros Archivos. Por lo tanto, estos servicios de archivo tratan grandes cantidades de datos relacionados con condenas penales: los seleccionan, los transfieren a sus depósitos, los organizan y los describen y los ponen a disposición de los investigadores. Este tipo de tratamiento es totalmente conforme con el RGPD, porque está regulado por ley y llevado a cabo por autoridades públicas con las garantías adecuadas para los derechos y libertades de los interesados. Por ejemplo, si la ley nacional restringe el acceso a los archivos judiciales por un número determinado de años, las archiveras y los archiveros aplican cuidadosamente tales restricciones. Si se publican en línea documentos de libre acceso relacionados con condenas penales, y existe la posibilidad de que las personas titulares de los datos estén aún con vida, los servicios de archivo pueden tomar medidas como la publicación de dichos documentos en un área de acceso restringido de sus sitios web, o la censura de nombres, de conformidad con el principio de respeto y protección de la dignidad de las personas.

Si un organismo público o privado (por ejemplo, una universidad, fundación u organización de la sociedad civil) custodia archivos jurídicos o copias de expedientes y de sentencias judiciales o por lo demás los reúne, conserva y pone a disposición de los investigadores documentos que contienen datos personales relacionados con condenas penales y delitos (por ejemplo: un centro académico especializado en el estudio del terrorismo o un centro de documentación creado por activistas antimafia), debería ponerse en contacto con su Agencia Nacional de Protección de Datos en busca de instrucciones sobre las garantías apropiadas para los derechos y libertades de los datos de los interesados.

VII. SEGURIDAD DE DATOS

16. LA PROTECCIÓN DE DATOS DESDE EL DISEÑO Y POR DEFECTO (ARTÍCULO 25): ¿QUÉ SIGNIFICADO TIENE EN LOS ARCHIVOS?

El artículo 25 establece que cuando se planifican los medios para tratar datos personales, el Responsable "aplicará medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos". Esto es a lo que el RGPD denomina "protección de datos *desde el diseño* ".

Uno de los principios fundamentales de protección de datos es la minimización de datos. De hecho, el artículo 25 requiere además que el Responsable "aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, *por defecto*, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento". (cursivas añadidas)

El artículo 25 se aplicará especialmente en el desarrollo de nuevos sistemas de información. Por ejemplo, en los Archivos, esto puede implicar:

- Creación de un repositorio digital.
- Creación de un banco de datos sobre registros de nacimientos u otros fondos que contengan información personal.
- Creación de un sistema de información para gestionar los servicios de sala de lectura.
- Creación de herramientas para el acceso en línea.

Los servicios de archivo deben de tener en cuenta el artículo 25 cuando planifican los diferentes tipos de actividades que normalmente realizan, tales como, la valoración, la organización y descripción, facilitando el acceso a los archivos y difundiéndolos.

Valoración: De acuerdo con su misión, los servicios de archivos adoptan una política de valoración que limita la conservación permanente de los documentos que contienen datos personales a lo que es realmente necesario. Ponen en práctica el artículo 25 para elaborar cuidadosamente planes de conservación que determinan qué tipo de expedientes que contienen datos personales, deben de ser seleccionados para su conservación permanente. Para los servicios de archivo, los planes de conservación son herramientas para demostrar el cumplimiento del artículo 25.

Organización y descripción: los servicios de archivo aplican el principio de minimización de los datos personales, cuando crean instrumentos de descripción. Cuando organizan y describen un fondo de archivo que incluye datos personales de personas vivas relacionados con la salud, la vida sexual, opiniones políticas y otras categorías especiales de datos, o datos relacionados con condenas penales, los servicios de archivo deben crear un instrumento de descripción que muestre nombres reales, a fin de poder responder a posibles

solicitudes de acceso de los interesados y cumplir con otros derechos de las personas titulares de los datos. Al mismo tiempo, para la investigación en línea (en caso de que su legislación nacional permita el acceso a dichos documentos), si la misión de proporcionar acceso a los archivos puede cumplirse de esta manera, los servicios de archivo pueden crear una versión del instrumento de descripción en la que los nombres reales son reemplazados por seudónimos. Un Software para la descripción de archivos que permite la creación de dos versiones diferentes de un instrumento de descripción (una con nombres reales y otra con seudónimos) es una herramienta acorde con el cumplimiento del art. 25.

Proporcionar acceso a los archivos: los servicios de archivos están obligados a asegurar que el acceso a los registros se gestiona de manera adecuada y que se implantan las garantías técnicas y organizativas correctas. Los servicios de archivo tienen un largo historial en gestionar y facilitar el acceso a los documentos, a través de controles organizativos, tales como la solicitud mediante tarjeta de investigador, verificando que los expedientes solicitados estén autorizados para ser examinados por el público y limitando el número de expedientes entregados en la sala de consulta.

En el entorno electrónico, las cuestiones de acceso se agravarán debido a la escala, variedad y complejidad de los documentos electrónicos. En muchos casos, previo a su acceso, grandes volúmenes de datos no pueden ser manualmente revisados y verificados, por lo que las salvaguardas y los controles deberán estar cada vez más automatizados.

Supervisión de actividades y colaboración con los productores de archivos. Dentro de la UE, la naturaleza de las relaciones entre las entidades que producen los archivos y los servicios de archivo, cambian de un país a otro, y según sea con el sector público y con el sector privado. En algunos casos, los Archivos Estatales tienen autoridad para supervisar, o llevar el control o asesorar, en otros no la tienen.

Para los servicios de archivo es importante el diseño de nuevos sistemas para los organismos públicos cuyos documentos pueden serles transferidos en el futuro. El reto puede ser respecto al diseño de nuevos sistemas de información que intenten cumplir con RGPD, en donde archivar por interés público no está incluido en la etapa inicial de planificación. Por lo tanto, es importante que los servicios de archivo estén involucrados en el diseño y planificación del sistema, para garantizar que, en el momento adecuado, los documentos puedan exportarse desde el sistema o ser reproducidos para su ingesta y transferencia a un servicio de archivo. En circunstancias ideales, el sistema de información debería tener en cuenta automáticamente el destino final de los documentos.

17. SEGURIDAD DE LOS DATOS PERSONALES (ARTÍCULO 32-34)

SEGURIDAD DEL TRATAMIENTO

Un principio clave del RGPD es que " el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo" (artículo 32). Este es el 'principio de seguridad'.

Cumplirlo exige que el Responsable y el Encargado ~~tengan en cuenta~~ realicen análisis de riesgos, adopten medidas técnicas y organizativas adecuadas. También tienen que tener en cuenta requisitos adicionales para la seguridad del tratamiento.

el Responsable y el Encargado pueden tener en cuenta el estado de la técnica y los costos de implementación al decidir qué medidas tomar, pero estas medidas deben ser adecuadas a las circunstancias y al riesgo que representa el tratamiento.

Las medidas deben garantizar la “confidencialidad, integridad, disponibilidad y resilencia” de los sistemas y servicios y de los datos personales que se tratan dentro de ellos. Las medidas deben también hacer posible que la persona responsable y la persona encargada restablezcan el acceso y la disponibilidad de los datos personales de manera oportuna en caso de un incidente físico o técnico.

El Responsable y el Encargado también deben asegurar que cuentan con los tratamientos adecuados para probar la efectividad de sus medidas, y acometer cualquier mejora requerida.

TÉCNICAS DE GESTIÓN DEL RIESGO

El RGPD no define las medidas de seguridad que el Responsable y el Encargado deberían contar. Este les exige tener un nivel de seguridad 'apropiado' a los riesgos que presentan sus tratamientos. Antes de decidir qué medidas son las adecuadas, necesitan realizar un análisis de riesgos de su información, mediante de una metodología formal de la gestión del riesgo.

VIOLACIONES DE SEGURIDAD DE LOS DATOS PERSONALES

El RGPD establece un sistema de notificaciones de las violaciones de seguridad en los datos personales (artículo 33). Una violación de seguridad significa que ocasiona "... la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos" (Artículo 4 (12)). Esto incluye brechas que son el resultado de causas tanto accidentales como deliberadas. También significa que una violación es algo más que solo la pérdida de datos personales.

Cuando la violación de datos personales suponga un probable riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento notificará la brecha de seguridad a la autoridad competente en materia de protección de datos tan pronto como pueda y, a ser posible, no más tarde de 72 horas.
“El encargado del tratamiento notificará sin dilación indebida al responsable del tratamiento las violaciones de la seguridad de los datos personales de las que tenga conocimiento” (artículo 33, apartado 2).

El contenido de la notificación está establecido en el artículo 33 (3) de la RGPD.

ASEGURAR EL TRATAMIENTO DE DATOS PERSONALES EN LOS ARCHIVOS Y ASEGURAR EL ACCESO NO AUTORIZADO A LOS DATOS PERSONALES CUSTODIADOS EN LOS ARCHIVOS

Los archiveros y las archiveras son responsables de la seguridad de los datos personales a su cargo y, de conformidad con las prácticas profesionales existentes, tienen que salvaguardar la integridad, autenticidad y protegerlos de accesos no autorizados, así como de su alteración, pérdida, daño o destrucción.

Los documentos deberían almacenarse de forma segura, para mantener la confidencialidad en todo momento. El acceso solo debería proporcionarse a aquellos que necesitan conocerlos y que puedan ser contemplados dentro de las leyes. La procedencia y la organización archivística no debería ser puesta en peligro mediante la separación de documentos personales y no personales.

El nivel de seguridad debería ser apropiado y proporcional a la naturaleza de los datos y al daño que podría producir una brecha de seguridad. Debe reflejar estándares profesionales y la utilización de técnicas de gestión de riesgos para evaluar la naturaleza, el nivel y el impacto de riesgos, así como las medidas adecuadas que se deben tomar para proteger los datos.

Medidas de seguridad prácticas deben tenerse en cuenta, incluyendo la instalación de dispositivos físicos de seguridad, como alarmas de intrusión, restringiendo el acceso a zonas protegidas, manteniendo un registro de entrada de visitantes y supervisando sus actividades lo máximo posible. Los datos en formato electrónico deberían estar protegidos, por ejemplo, por medios de protección de software contra virus y troyanos, y el acceso controlado por contraseña sólo para personas usuarias autorizadas. Los datos personales deberían transmitirse de forma segura, para la transmisión segura de datos personales en formato electrónico deberían utilizarse herramientas de cifrado.

Mientras los servicios de archivo existan para conservar y proporcionar acceso a los documentos, no deben divulgar documentos que contengan datos personales a menos que puedan conciliar los requerimientos de la investigación, ya sea histórica o probatoria, con los derechos y libertades fundamentales de las personas titulares de los datos.

¿QUÉ PUEDEN HACER LOS ARCHIVISTAS EN CASO DE UNA VIOLACIÓN O BRECHA DE SEGURIDAD DE LOS DATOS?

En el caso de una grave violación derivada del tratamiento, ya sea almacenamiento, acceso, comunicación ... - de los documentos, los servicios de archivo deben considerar si la violación es probable que cause un daño significativo a los intereses de las personas vivas titulares de los datos. Si es así, la notificación de la infracción debería ser contemplada según los términos del artículo 34 (3), letra c) del Reglamento, y enviarse a la autoridad de control.

El Art.34 (1) indica que "cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento la comunicará al interesado sin dilación indebida". Sin embargo, en caso de que esto suponga un «esfuerzo desproporcionado», que, por supuesto, podría ser así si se produjera una violación relativa a grandes series documentales que contienen miles de datos personales – el art. 34 (1) punto (c), ofrece la alternativa de "una comunicación pública o una medida semejante por la que se informe de manera igualmente efectiva a los interesados". Por ejemplo, podría ser un anuncio en la página web o una comunicación a través de una lista de correo.

Las quiebras de seguridad deberán ser documentadas e investigadas y se deberá formar al personal a fin de informar y reaccionar ante los incidentes producidos por las mismas.

18. EVALUACIÓN DEL IMPACTO DE LA PROTECCIÓN DE DATOS Y CONSULTA PREVIA (Artículos 35-36)

El RGPD exige a los responsables llevar a cabo una evaluación de impacto de la protección de datos (EIPD) "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" (artículo 35, apartado 1). Los EIPD son herramientas para la responsabilidad proactiva, ya que ayudan a los responsables, no solo a cumplir con los requisitos del RGPD, sino también para demostrar su conformidad con el Reglamento. [3]

¿QUÉ ES UNA EVALUACIÓN DE IMPACTO DE PROTECCIÓN DE DATOS (EIPD)?

El objetivo de una EIPD es identificar y evaluar el riesgo que podría surgir para un individuo (como ciudadano, cliente, paciente, etc.) a partir de un nuevo tipo de tratamiento. El grupo de trabajo del artículo 29, definió la EIPD como: "un proceso diseñado para describir el tratamiento, para evaluar su necesidad y proporcionalidad y para ayudar a gestionar los riesgos para los derechos y

[3] artículo 29 del Grupo de trabajo, *Directrices sobre la evaluación del impacto en la protección de datos (DPIA) y si es probable que el tratamiento resulte en un alto riesgo a los efectos del Reglamento 2016/679*, wp248 rev.01, 13 oct. 2017

libertades de las personas físicas derivados del tratamiento de datos personales, para evaluar y determinar las medidas para abordarlos." [4]

¿CUANDO SE DEBE REALIZAR (O CUÁNDO NO) LA EVALUACIÓN DE IMPACTO DE PROTECCIÓN DE DATOS?

Cuando se introducen nuevas tecnologías para el tratamiento de datos personales o un nuevo tipo de tratamiento, como primer paso se debe realizar un análisis de riesgos. Si la naturaleza de los datos o la manera de tratar los datos supone un alto riesgo para las personas titulares de los datos, se requerirá realizar una EIPD.

Una EIPD no es necesaria cuando el tratamiento *no* es probable que implique riesgos para los interesados, y cuando es similar a las actividades de tratamiento anteriores para las cuales ya se ha realizado una EIPD. De hecho, el RGPD deja claro que "una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares". (Artículo 35 (1)).

Las Autoridades de Protección de Datos publican la lista del tipo de operaciones de tratamiento que están sujetas a la obligación de realizar una evaluación de impacto de protección de datos y también las que no lo están.

¿QUÉ SIGNIFICA "ALTO RIESGO"?

El RGPD no define exactamente qué tipo de tratamiento podría conllevar un alto riesgo. Sin embargo, proporciona algunos ejemplos, incluido uno que bien puede concernir a los servicios de archivo, a saber, el tratamiento a gran escala de datos personales relacionados con delitos penales, o de datos personales sensibles (es decir, datos que revelen el origen racial o étnico, opiniones políticas, creencias religiosas o filosóficas, o afiliación sindical, datos genéticos, datos biométricos y datos sobre la salud o la vida sexual u orientación sexual de una persona) (artículo 35, apartado 3, letra b)). Además, al evaluar si el tratamiento podría resultar de alto riesgo para los derechos y libertades de los titulares de datos, los servicios de archivo deberían tener en cuenta si los datos personales se refieren a personas de colectivos vulnerables, como por ejemplo de personas con enfermedades mentales (considerando 75).

¿CUÁNDO LOS SERVICIOS DE ARCHIVO TIENEN QUE REALIZAR UNA EIPD?

Puede ser necesario una EIPD cuando los servicios de archivo deciden digitalizar material o crear instrumentos de descripción de datos personales, para su utilización "in situ" o en línea. Ciertamente, este será el caso, si se van a tratar fondos de archivo que contienen datos personales confidenciales, como los expedientes médicos, los expedientes judiciales penales o los expedientes personales de los reclusos.

[4] Ibídem

La EIPD garantizará que el servicio de archivo ha tenido en cuenta la protección de datos y los aspectos de privacidad en el proyecto o trabajo propuesto y puede demostrar a la Autoridad de Protección de Datos que tales preocupaciones fueron abordadas o analizadas desde el diseño o implementación del proyecto.

¿QUÉ HAY QUE HACER?

En el curso de la evaluación de impacto de protección de datos, la operación de planificación de tratamiento y el interés legítimo de la operación deben ser descritos de manera sistemática. En una siguiente fase, la necesidad y la proporcionalidad de la operación prevista deben ser evaluadas. Entonces, los riesgos para los derechos y libertades del interesado deben evaluarse seguidos de un plan detallado de las medidas que se adoptarán para gestionarlos. Cuando la operación del tratamiento esté en marcha debe ser monitorizada regularmente y la EIPD debe ser adaptada cuando se produzcan cambios.

Las Autoridades de Protección de Datos han publicado herramientas para ayudar a los Responsables a llevar a cabo una EIPD.

Por ejemplo, véase el software gratuito producido por la AEPD que se encuentra en:

https://www.aepd.es/es/guias-y-herramientas/herramientas/gestiona-eipd

Además, ha editado guías de ayuda en:

https://www.aepd.es/es/guias-y-herramientas/guias:

¿CUANDO LA AUTORIDAD DE CONTROL (AEPD) TIENE QUE SER INFORMADA?

La autoridad de control (es decir, la Autoridad de Protección de Datos) debe ser consultada si la evaluación de impacto de la protección de datos indica que el tratamiento "mostrara que el tratamiento entrañaría un alto riesgo si el responsable no toma medidas para para mitigarlo.” (art.36). Si la autoridad de control considera que el tratamiento planeado no se ajusta al Reglamento, o las medidas previstas no son suficientes para mitigar el riesgo, debe advertir por escrito al responsable.

VII. MEDIDAS DE TRANSPARENCIA Y FOMENTO DE SU CUMPLIMIENTO

19. REGISTROS DE ACTIVIDADES DE TRATAMIENTO (ARTÍCULO 30)

El Artículo 30 (1) establece que: “Cada responsable y, en su caso su representante, llevarán un registro de las actividades de tratamiento efectuadas bajo su responsabilidad”

El registro de actividades de tratamiento, a menudo se le cita como “registro de tratamiento (de datos)”, es un medio muy útil para servir como soporte del análisis de las implicaciones de cualquier tratamiento. Ya sea existente o planeado. El registro facilita la evaluación objetiva del riesgo de las actividades de tratamiento, realizadas por el responsable o el encargado, para los derechos de los individuos, y para la identificación e implementación de las medidas de seguridad adecuadas para la salvaguarda de los datos personales - ambos componentes son claves en el principio de responsabilidad proactiva contenidos en el RGPD.

Este registro debe constar por escrito (incluso en formato electrónico), de forma clara e inteligible. Ya que las “actividades de tratamiento”, en el contexto del RGPD se refieren a operaciones realizadas con los datos personales relacionados con una persona física identificada o identificable, solo afectan a actividades referidas a los datos personales.

La obligación de mantener un registro de las actividades de tratamiento no se aplica a las organizaciones dotadas con menos de 250 empleados, excepto si se encuentran en posición de realizar tratamientos que probablemente den lugar a un riesgo (no solo un alto riesgo) para los derechos de los interesados, o si están tratando datos personales de forma no ocasional, o si tienen tendencia a tratar categorías especiales de datos conforme al Artículo 9 (1) (es decir, datos de salud, sobre la vida sexual, los orígenes étnicos, las opiniones políticas y otros tipos de cuestiones sensibles), o datos relativos a condenas penales con arreglo al artículo 10.

Si se dan alguna de estas circunstancias, lo que de hecho sucede en la mayoría de los casos, por no decir en todos los Archivos: Una organización está obligada a mantener el registro de actividades de tratamiento.

Las organizaciones y sus representantes deben proporcionar este registro al Delegado de Protección de Datos (DPA), cuando así se les requiera.

¿QUÉ INFORMACIÓN DEBERÍA DISPONER EL REGISTRO DE ACTIVIDADES DE TRATAMIENTO?

El registro debe contener información específica sobre cada actividad de tratamiento que se lleve a cabo:

- El **nombre y datos** de **contacto** de:

    - el servicio de archivo, o su representante;
    - en su caso, otras organizaciones con las que el servicio de archivo tiene en común los fines y medios del tratamiento;
    - el Delegado de Protección de Datos (DPO), si el servicio de archivo lo ha designado;

- Los **fines** para los cuales el servicio de archivo trata información personal.

Al igual que en el pasado la 'investigación histórica' que ya ha sido reconocida como un fin, 'el archivo (finalidades) en interés público' debería ser suficiente como objetivo. No está claro si para motivar la información debe ser o no ser añadido "de interés público".

- Una descripción de los **colectivos sobre los** que el servicio de archivo trata datos. Por ejemplo: estudiantes, reclutas, acusados, pacientes…

- Una descripción de las **categorías de datos personales**: Identificando también los llamados datos “sensibles”, tales como la información sobre la salud e información judicial. Por ejemplo: actividades profesionales, transacciones financieras, información judicial sobre condenas y sentencias penales, datos a partir de los cuales pueden deducirse opiniones políticas….

- La **fecha en la que se deben eliminar los datos** (si se conoce).

Atención: Desde el punto de vista de los servicios de archivo, es de particular importancia señalar a los productores de archivos que el "período de conservación" no debe confundirse con la "eliminación" de la información, y que deben actuar de conformidad con las Leyes de Archivos y según lo estipulado en los calendarios de eliminación de documentos. Los datos archivados en interés público nunca deben ser destruidos.

- Las **categorías de destinatarios** a quienes el servicio de archivo proporciona datos personales.

Téngase en cuenta que estamos hablando de "categorías de destinatarios": es decir, por ejemplo 'universidades e instituciones de investigación', 'investigadores individuales' ...

- ¿Transfiere el servicio de archivo datos a un **país extranjero u organización internacional fuera de la UE**? Entonces debe hacerlo constar en el registro.

- La descripción general de las **medidas técnicas y organizativas** adoptadas con el fin de asegurar los datos personales que el servicio de archivo está tratando: descripción de la tecnología, las aplicaciones y el software utilizado para el tratamiento de datos, es decir,

qué tipo de ‘Protección de datos desde el diseño o por defecto' ha sido utilizado.

Las organizaciones deberían considerar este registro como una herramienta interna para ayudar a implementar el RGPD. El registro puede contener cualquier información adicional que se considere de importancia para el Delegado de Protección de Datos (DPD) en función de las actividades llevadas a cabo, por ejemplo, la indicación de la base legal del tratamiento de datos o un resumen de todas las violaciones relacionados con datos personales.

TRATAMIENTO POR SUBCONTRATISTAS

Téngase en cuenta: si un servicio de archivo autoriza a otras entidades o empresas a tratar datos personales en su lugar, debe firmarse un "encargo de tratamiento de datos" con esas organizaciones. Para la celebración del dicho encargo, el servicio de archivo garantizará que estos terceros no utilicen o traten los datos personales para sus propios fines individuales.

Solo deberían ser nombrados “encargados de tratamiento” quienes pueden garantizar plenamente que se atienen a los requisitos legales. Los Servicios de archivo que decidan externalizar las actividades de tratamiento con terceros proveedores, siguen siendo totalmente responsables de atenerse a las estipulaciones del RGPD.

ALGUNOS MODELOS DE REGISTRO DE ACTIVIDADES DE TRATAMIENTO ESTÁN DISPONIBLES EN LÍNEA, POR EJEMPLO:

El modelo ofrecido por la APD belga, que está disponible en francés y holandés:

https://www.privacycommission.be/fr/canevas-de-registre-des-activites-de-traitement

La francesa publicó dos modelos de registros, uno más complejo y otro más simple:

https://www.cnil.fr/fr/rgpd-et-tpepme-un-nouveau-modele-de-registre-plus-simple-et-plus-didactique

El Supervisor Europeo de Protección de Datos (es decir, la autoridad independiente de Protección de Datos de la UE) publicó una "Plantilla-modelo de registro"

https://edps.europa.eu/data-protection/our-work/publications/other-documents/register-template-0_en

Los estados miembros pueden crear una aplicación del registro de actividades de tratamiento, cuyo uso es obligatorio para los servicios públicos. Bélgica es un buen ejemplo.

20. EL DELEGADO DE PROTECCIÓN DE DATOS (ARTÍCULO 37): ¿NECESITAN LOS ARCHIVOS NOMBRAR UNO O UNA?

El Delegado de Protección de Datos (DPD) asesora al responsable o al encargado en todos los asuntos relativos a la protección de datos personales. Sus principales tareas son:

- Informar y asesorar al responsable y a los empleados que entre sus obligaciones se encuentra la de realizar tratamientos bajo el RGPD y las normas nacionales de protección de datos.
- Hacer el seguimiento del cumplimiento de la RGPD.
- Proporcionar asesoramiento en relación a la evaluación del impacto de la protección de datos (EIPD)
- Cooperar con la autoridad de control (AEPD);

El RGPD introdujo la obligación de designar un DPD por parte de las autoridades públicas y para Entidades privadas que lleven a cabo determinados tipos de actividades de tratamiento. Todas las autoridades públicas deben tener un DPD, pero esto no significa que cada servicio de archivo en el sector público necesite nombrar una. En muchos casos, su institución matriz puede designar a una DPD cuyas responsabilidades se extienden al servicio de archivo. Por ejemplo, un municipio podría tener una DPD responsable de hacer el seguimiento del cumplimiento del RGPD y asesorar a todas las oficinas del municipio, incluido el Archivo Municipal.

Las entidades del sector privado deben nombrar una DPD si:

- Su actividad principal requiere hacer un seguimiento regular y sistemático a gran escala de personas titulares de datos.
- Su actividad principal consiste en el tratamiento de datos personales que revelen el origen racial o étnico, opiniones políticas, creencias religiosas o filosóficas, o pertenecer a un sindicato, y el tratamiento de datos genéticos, datos biométricos con el propósito de identificar de manera única a una persona física, datos concernientes salud o datos relacionados con la vida sexual u orientación sexual de una persona física, o datos personales relacionados con condenas y delitos penales.

Es muy improbable que fundaciones, museos, bibliotecas, asociaciones culturales y otros organismos del sector privado que custodian archivos lleven a cabo un “seguimiento regular y sistemático de datos a gran escala”. Por el contrario, es muy posible que su actividad principal consista en el tratamiento de datos personales sensibles.

De hecho, existen fundaciones, archivos comunitarios y otros organismos del sector privado especializados en el tratamiento de los archivos producidos por ONGs y por organizaciones de derechos humanos que, en el curso de sus actividades, pueden incluir, por ejemplo, datos personales que revelan el origen racial o étnico de las personas víctimas de actos de intolerancia. Como ya se

mencionó, hay centros académicos especializados en el estudio del terrorismo o archivos de centros de documentación creados por activistas contra la mafia que tratan datos personales relacionados con condenas y delitos penales. Puede haber centros de documentación que custodian archivos producidos por organizaciones feministas que asisten a mujeres víctimas de violencia de género y que incluyen todo tipo de datos personales altamente sensibles.

En todos estos casos, los organismos privados que tratan archivos deben designar una DPD. " El delegado de protección de datos podrá formar parte de la plantilla del responsable o del encargado del tratamiento o desempeñar sus funciones en el marco de un contrato de servicios" (Artículo 37.6). Una empresa pequeña puede compartir un DPD con otras entidades similares. Es muy recomendable para organismos pequeños que traten archivos para "fines de archivo en interés público" o para fines de investigación, compartir el mismo DPD con otros organismos similares para que este pueda adquirir conocimientos especializados en el tratamiento que llevan a cabo de este tipo concreto de datos personales.

ANEXOS

GLOSARIO

Archivo: El RGPD no define el término "archivo". A lo largo de este documento, “archivo” se utiliza para referirse al conjunto de documentos creados y recibidos por una persona, familia u organización, pública o privada, en la gestión de sus competencias, y seleccionados para su conservación permanente. En algunas lenguas europeas, el mismo término el mismo término se usa para referirse tanto a los documentos administrativos, como a los documentos seleccionados para la preservación permanente. En este texto, el término archivo se utiliza solo para referirse a los documentos seleccionados para la conservación permanente.

Autoridad de Control: El art. 51 de la RGPD estipula que cada Estado miembro deberá contar con una o más autoridades públicas independientes, que serán responsables del seguimiento de la aplicación del Reglamento. Tales autoridades tienen nombres diferentes en los diferentes países (por ejemplo, en Finlandia “Office of the Data Protection Ombudsman ", en Francia" Commission Nationale de l'Informatique et des Libertés ", en Irlanda “Data Protection Commissioner”, en Italia “Garante per la protezione dei dati personali"), y se conocen comúnmente como" Autoridades de Protección de Datos "(APD).

Autoridad de Protección de Datos (APD): ver Autoridad de Control

Categorías especiales de datos personales: Datos personales que revelan el origen racial o étnico, opiniones políticas, creencias religiosas o filosóficas, o afiliación sindical, datos en relación con la salud o los datos relativos a la vida u orientación sexual de una persona física; datos genéticos y datos biométricos que se tratan para identificar de manera única a un individuo (RGPD, art. 9). Tales tipos de datos a menudo se denominan "datos personales sensibles".

Comité Europeo de Protección de Datos (CEPD): El RGPD reemplazó el grupo de trabajo del Artículo 29 por el CEPD. A diferencia de su predecesor, el CEPD tiene el estatus de un organismo de la UE con personalidad jurídica y cuenta con una Secretaría independiente. Tiene amplios poderes para decidir sobre disputas entre las autoridades nacionales de supervisión y asesorar y orientar en conceptos clave del RGPD. Se compone por responsables de las autoridades de control de cada Estado miembro (DPA) y del Supervisor Europeo de Protección de Datos. La Comisión tiene derecho a participar en sus reuniones.

Datos personales: " toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona (RGPD, art. 4)

Los y las archiveras deberían tener en cuenta que el RGPD protege solo los datos personales de personas vivas, sin embargo, la legislación nacional también puede prever la protección de los datos de personas fallecidas.

Encargado:

Grupo de trabajo del artículo 29: Grupo de trabajo creado de conformidad con el art. 29 Directiva 95/46 de la UE. El grupo de trabajo estuvo compuesto por personas representantes de las Autoridades de Protección de Datos en los Estados miembros, la Supervisora de Protección de Datos de la Comisión Europea y una persona representante de la Comisión de la UE. El grupo de trabajo dejó de existir el 25 de mayo de 2018 cuando fue reemplazado por el Consejo Europeo de Protección de Datos (CEPD).

Delegado de Protección de Datos:

Delegado de Protección de Datos (DPO): El DPO asiste al Responsable o al ~~la persona~~ encargado en todas las cuestiones relativas a la protección de datos personales. El RGPD introdujo la obligación de designar un DPO para las autoridades públicas y para las entidades privadas que llevan a cabo cierto tipo de actividades de tratamiento.

Encargado del tratamiento: “la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento;” (RGPD, art. 4).

Responsable: “la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determina los fines y medios del tratamiento” (RGPD, art. 4).

Interesado: Persona titular de los datos, cuyos datos personales son tratados.

Supervisor Europeo de Protección de Datos (SEPD): el SEPD es un organismo independiente de la UE responsable de hacer el seguimiento de la aplicación de las normas de protección de datos dentro de las Instituciones de Europa y para investigar las quejas.

Tratamiento: “cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción;”. (RGPD, art. 4).

De acuerdo con el RGPD, las archiveras y los archiveros deberían tener en cuenta que las actividades tales como la selección de documentos que contengan datos personales para su conservación permanente, transfiriéndolos al archivo de una institución, organizarlos, describirlos y ponerlos a disposición de los usuarios, todas ellas se consideran "tratamiento de datos personales".

Violación de la seguridad de los datos personales: “toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos;” (RGPD, art. 4).
Esta definición es de suma importancia para los archiveros y las archiveras. Implica que, si los datos personales han sido seleccionados para su conservación permanente y pasan a ser custodiados en el archivo de una Institución, el personal de los archivos debe proteger su integridad. De hecho, entre los principios relacionados con el tratamiento de datos personales, el Reglamento incluye, “la integridad y la confidencialidad” (art. 5). La pérdida accidental o la alteración de tales registros violaría no solo la ética archivística sino también el cumplimiento del RGPD. Lo mismo ocurre si el personal de los archivos permite la revelación o acceso no autorizado a datos personales.

Seudonimización: “el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable; ". (RGPD, art. 4).
Es importante tener en cuenta que el RGPD sugiere la posibilidad de seudonimizar los datos personales conservados para fines de archivo en interés público o para fines de investigación histórica y no menciona la "anonimización". A diferencia de la anonimización, la seudonimización preserva la correlación de diferentes datos relacionados con una persona, así como la relación entre diferentes registros de datos. Los datos personales seudonimizados permite mantener la naturaleza de datos personales, y por lo tanto cumplir con las disposiciones del Reglamento.

DONDE BUSCAR MÁS ORIENTACIONES

- La Comisión Europea tiene una sección en su sitio web “Data protection. Rules for the protection of personal data inside and outside the EU” https://ec.europa.eu/info/law/law-topic/data-protection_en, en donde ha publicado algunas preguntas frecuentes sobre RGPD, por ejemplo, ¿Qué son los datos personales? ¿qué constituye el tratamiento? ¿Qué son las Autoridades de Protección de Datos (APD) ?, etc. La información está destinada a lectores que no tienen conocimientos previos sobre el RGPD. Actualmente, está solo disponible en ingles

- *Manual sobre la ley europea de protección de datos*, edición 2018 - https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_es.pdf El manual ha sido preparado por la Agencia de los Derechos fundamentales de la UE (ADF), con el Consejo de

Europa (junto con la Secretaría del Tribunal Europeo de Derechos Humanos) y el Supervisor Europeo de Protección de Datos. Resume tanto las normas de protección de datos de la Unión Europea (UE) y del Consejo de Europa (CoE) e incluye la jurisprudencia seleccionada del Tribunal Europeo de Derechos Humanos (TEDH) y la del Tribunal de Justicia de la Unión Europea (TJUE).

- El Comité Europeo de Protección de Datos (CEPD) va a publicar las directrices, recomendaciones y mejores prácticas. Por lo tanto, será útil echar un vistazo a su web https://edpb.europa.eu/edpb_en que está disponible en todas las lenguas de la UE (aunque, por el momento, la mayoría de los documentos están disponibles solo en inglés). En sus primeros días de existencia, el CEPD aprobó las pautas producidas por su antecesor, el Grupo de Trabajo del artículo 29.

- El Grupo de Trabajo del Artículo 29 (que dejó de existir el 25 de mayo de 2018) publicó nueve directrices y otros documentos sobre la implementación del RGPD, con el objetivo de contribuir a su interpretación y a su implementación uniforme por parte de las diferentes APD y por los gobiernos de toda la UE. El Comité Europeo de Protección de Datos (CEPD) aprobó todos estos documentos y los puso disponibles en su sitio web https://edpb.europa.eu/edpb_en

    - *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679* (wp251rev.01), 13-02-2018

    - *Guidelines on Consent under Regulation 2016/679* (wp259), 24-01-2018, [[Adaptado, pero aún por finalizar]

    - *Guidelines on Data Protection Impact Assessment (DPIA) on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679* (wp248rev.01) 13-10-2017

    - *Guidelines on Data Protection Officers ('DPOs')* (wp243rev.01), 30-10-2017

    - *Guidelines on Personal data breach notification under Regulation 2016/679* (wp250rev.01), 13-02-2018

    - *Guidelines on the application and setting of administrative fines* (wp253). Now including available language versions, 13-02-2018

    - *Guidelines on the Lead Supervisory Authority* (wp244rev.01), 31-10-2017

    - *Guidelines on the right to "data portability"* (wp242rev.01), 27-10-2017

    - *Guidelines on Transparency under Regulation 2016/679* (wp260), 24-01-2018 [Adaptado, pero aún por finalizar]

- *Position paper on the derogations from the obligation to maintain records of processing activities pursuant to Article 30(5) GDPR*, 19–04-2018.

- Las autoridades de protección de datos de los Estados miembros de la UE publican material informativo, como folletos, hojas informativas, infografías, traducciones del Grupo de Trabajo del Artículo 29, directrices, para explicar sus nuevos derechos a los ciudadanos, y para ayudar a las administraciones públicas y a las pequeñas y medianas empresas a cumplir con el RGPD.

  https://ec.europa.eu/justice/article-29/structure/data-protection-authorities/index_en.htm.

  https://www.aepd.es/es

- El Supervisor Europeo de Protección de Datos (SEPD) tiene un *Glosario* (en inglés, francés y alemán) con más de 70 entradas en su sitio web:

  https://edps.europa.eu/data-protection/data-protection/glossary_en .

  Además, ha publicado un acceso gratuito a la Biblioteca de referencia https://edps.europa.eu/data-protection/data-protection/reference-library_en y otros materiales informativos, principalmente destinados a guiar a las instituciones de la UE en la implementación del RGPD, pero que puede ser útil para el público nacional y también para las entidades privadas.

- El Archivo Nacional del Reino Unido, junto con los líderes de la política gubernamental de los archivos y la Asociación de Archivos y Registros, ha preparado una *Guía para el archivo de datos personales*, y está disponible gratuitamente en su página web. También puede ser útil su lectura para las archiveras y los archiveros de otros estados miembros con la condición de que tengan en cuenta que esta *guía* es específica para el sistema legal británico.

  http://www.nationalarchives.gov.uk/information-management/legislation/data-protection/

  https://www.nationalarchives.gov.uk/documents/information-management/guide-to-archiving-personal-data.pdf