



FRANCESC GIMÉNEZ MARTÍN

El archivero/a como DPD

The archivist as DPD

Francesc Giménez Martín
francescgimenez@santcugat.cat
Ajuntament de Sant Cugat del Vallès

Citación: Giménez Martín, Francesc (2021). "El archivero/a como DPD". *Tàbula*, n. 24, pp. 21-43

Recibido: 2-3-2020. *Aceptado:* 5-10-2020
DOI: <https://doi.org/xxx>

Resumen analítico / Analytic summary

¿Es el archivero/a realmente una opción para que las organizaciones piensen en él como delegado/a de protección de datos? ¿Está el archivero/a capacitado y listo para asumir ese cargo, llegado el momento? Estas cuestiones son las que se plantearán en el presente artículo, en un intento de esclarecer dudas de terceros y de la profesión, sobre la figura del archivero/a-DPD. Se incidirá en las funciones y competencias de ambos y, por último, se aportará un ejemplo práctico de elaboración de una herramienta fundamental tanto para la gestión documental como para el RGPD: el Registro de actividades de tratamiento.

ARCHIVERO | ARCHIVERA | GESTIÓN DOCUMENTAL | DELEGADO DE PROTECCIÓN DE DATOS | DPD | RGPD

Is the archivist really an option for organizations to think of him/her as a Data Protection Officer? Is the archivist trained and ready to take on that role, when the time comes? These questions are those that will be raised in this article, in an attempt to clarify doubts, from third parties and from the profession, about the figure of the archivist-DPO. The functions and competencies of both will be emphasized and, finally, a practical example of the development of a fundamental tool for both document management and the RGPD will be provided: the Record of processing activities.

ARCHIVIST | RECORDS MANAGEMENT | DATA PROTECTION OFFICER | DPO | RGPD

¿Es el archivero/a realmente una opción para que las organizaciones piensen en él como delegado/a de protección de datos? Está el archivero/a capacitado y listo para asumir ese cargo, llegado el momento? Estas cuestiones son las que se plantean en la presente ponencia, en un intento de esclarecer dudas, de terceros y propias de la profesión, sobre la figura del archivero/a-DPD.

En esa voluntad de dar respuestas, vamos a plantear la sesión en los siguientes apartados:

- Los datos son la clave
- La figura del responsable de tratamiento
- Protección de datos desde el diseño y por defecto
- Posición del DPD en la organización
- Creación del Registro de actividades de tratamiento a partir del Cuadro de clasificación
- Conclusiones

Los datos son la clave

El Reglamento (UE) 2016/679 del Parlamento europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (de ahora en adelante, RGPD) incluye en su articulado elementos clave para entender la posición e importancia de los y las profesionales de la archivística en los fundamentos de dicha normativa.

En el RGPD los datos son la clave. De hecho, si hacemos un vaciado rápido de los términos “dato”, “documento”, “información” o “archivo” tal y como aparecen en el RGPD, obtenemos el resultado de:

- Documentación – 6 veces
- Archivo– 20 veces
- Información –169 veces
- Datos – 825 veces

Es evidente que la focalización está en los datos. Pero los datos en sí no son información, y esa es la primera premisa que la profesión tiene clara. Los datos se organizan y gestionan en un contexto organizativo y social. La asociación de datos a una persona es lo que los configura, en sí mismo, como datos personales. Estamos hablando de relaciones entre datos y atributos. Un dato sin un atributo que lo asocie a una persona, no le otorga ninguna característica personal, y queda fuera del marco de tratamiento del RGPD. El considerando 6 del RGPD indica:

«La tecnología permite que tanto las empresas privadas como las autoridades utilicen datos personales a una escala sin precedentes, cuando desarrollan sus actividades. Las personas físicas difunden un volumen cada vez mayor de información personal a escala mundial» (RGPD, considerando 6).

La difusión de datos personales confluye en un contexto social y tecnológico que propicia que dichos datos se reutilicen, se exploten, sean materia de negocio y se conviertan, por consiguiente, en valiosos activos de información. Los datos tienen su valor en su contexto atributivo, en su proposición como información de un momento, de unos sujetos, de una situación. El gran cambio con el RGPD es centrarse no en los ficheros que contienen datos, sino en los tratamientos que se hacen con los datos. Centramos la atención, así pues, en aquellos procesos administrativos que conllevan el tratamiento de datos. ¿Y qué es tratamiento? El artículo 4 del RGPD lo define como: «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» (el subrayado es propio). De este redactado hay que tener en cuenta que el concepto de tratamiento es mucho más amplio que el de “gestión”. Sólo una visualización de datos ya es tratamiento. Por ejemplo, si una persona recoge físicamente una instancia cumplimentada, ya está tratando los datos, aunque solo los traslade a un tercero que los gestione. Acceso a datos es tratamiento de datos.

Es importante, por otro lado, destacar los procesos que detecta la definición de “tratamiento”. No hace falta incidir demasiado, pero estamos hablando,

claramente, de procesos de gestión de la información. Vamos a ver el subrayado: 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. Por supuesto, como muchas ya habréis deducido, coinciden con las fases de tratamiento de la gestión de documentos. Si nos centramos en las que identifica ISO 30301 (apartado 8.2), para recurrir a un estándar internacional: captura de documentos por cada proceso de negocio, determinación del contenido, el contexto y la información del control (metadatos), establecer la forma y la estructura de la creación y captura de los documentos y la tecnología necesaria para su creación. Así mismo, elementos de control como su vinculación a la preservación del diseño, usabilidad e integridad, disposición y condiciones de administración y mantenimiento de las aplicaciones de gestión documental. Es, por consiguiente, vinculante la relación entre los procesos de gestión documental y los procesos de tratamiento que indica el RGPD. Desde la recogida (o captura) de los datos, a los que su contexto (externo e interno) nos situará dentro de un proceso específico, hasta su utilización, estructuración y conservación, los procesos de gestión documental están intrínsecamente relacionados con dichos tratamientos.

Por otro lado, aunque la atención recae en el tratamiento, los ficheros aún tienen presencia en el RGPD. Un fichero es cualquier conjunto estructurado de datos personales accesibles de acuerdo con criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica (artículo 4). Aunque ya no se habla de ficheros de datos personales, estos aún existen, entendidos como conjunto estructurado de datos personales. Observemos aquí como solo consideran fichero, en este entorno, si hay acceso. Pues hablamos de datos con atributos, datos referentes a una persona, y ya no se considera solo un archivo



Figura 1. Concepto de datos personales dentro de sistemas, en el RGPD

entendido como una propiedad de un organismo o ubicación geográfica, sino que un fichero puede descentralizarse, puede vincularse a una función transversal, pero sigue siendo contenedor de datos estructurados.

La figura del responsable de tratamiento

Otro gran concepto que hay que resaltar, para contextualizar la importancia de la figura del archivero/a como DPD, es la consideración de responsable de tratamiento. En el RGPD, artículo 4, se define dicha figura como la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento. La figura del responsable de tratamiento nos acerca a la definición de productor en el entorno de la gestión documental: persona/as o entidad/es que generan documentación por razón de su actividad. Es, a grandes rasgos, el mismo concepto que emplea el RGPD. En la gestión documental empero se centraba en el documento, en la evidencia documental de un proceso. Aquí, el centro es el propio tratamiento. Un cambio que hay que valorar en nuestro entorno: no nos centramos en el resultado, sino en lo que genera este.

Y, aparte del responsable, otra figura relacionada es la del encargado de tratamiento, entendido como la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que trata datos personales por cuenta del responsable del tratamiento. En este punto, es muy importante considerar los encargados de tratamiento como productores de información, ya que, aunque actuando en nombre del responsable, generan información por razón del tratamiento que este les ha encargado. Por lo tanto, la responsabilidad es la misma, a nivel de tratamiento, que en el caso del responsable.

Protección de datos desde el diseño y por defecto

El artículo 25 del RGPD es de especial interés para la gestión de la información y entra directamente en las consideraciones que desde la profesión siempre atendemos en materia de procesos y políticas de gestión documental. Este artículo es especialmente importante porque coloca la gestión de datos en el diseño mismo de los tratamientos y por defecto. Esto sitúa las consideraciones de los responsables de protección de datos de la organización (y, en su defecto, del delegado de protección de datos) en un entorno de definición tanto de sistemas de gestión como de proyectos. Aquí la diferencia es importante: no estamos hablando de bases de datos que se quieran contratar, sino de tratamientos de datos, es decir, de proyectos, que, en sí mismo, pueden llevar la adquisición de software, pero también el tratamiento de datos ya existentes en la organización para fines nuevos

no detectados. Estar, por ley, en estos procesos, es clave para poder actuar antes de la generación del tratamiento.

Centremos la atención en el art. 25.2: «... El responsable del tratamiento debe aplicar las medidas técnicas y organizativas adecuadas con la intención de garantizar que, por defecto, únicamente se tratan los datos personales necesarios para cada una de las finalidades específicas del tratamiento. Esta obligación se aplica a la cantidad de datos personales recogidos, al alcance del tratamiento, el plazo de conservación y la accesibilidad de los datos.»

El considerando 78 también insiste en esta cuestión, centrándose en la garantía de sistemas gestionados desde el diseño de acuerdo con el RGPD:

«La protección de los derechos y las libertades de las personas físicas en lo que respecta al tratamiento de datos personales exige que se adopten las medidas técnicas y organizativas adecuadas con el fin de garantizar que se cumplen los requisitos de este Reglamento. Para poder demostrar la conformidad con este Reglamento, el responsable del tratamiento debe adoptar políticas internas y aplicar medidas que cumplan los principios de protección de datos desde el diseño y por defecto.» (RGPD, considerando 78).

«Hay que alentar a los productores de las aplicaciones, los productos y los servicios basados en el tratamiento de datos personales para que tengan en cuenta el derecho a la protección de datos cuando los desarrollan, diseñan, seleccionan y usan.» (RGPD, considerando 78).

Como ven, estamos hablando de calidad de los datos: qué datos, qué cantidad, cómo se recogen, por qué, en qué sistemas, cuánto tiempo se conservarán y quién podrá acceder a estos datos. Esto, claramente, es gestión documental en esencia.

El repaso por el articulado es un repaso centrado en aquellos elementos que se pueden considerar intrínsecamente relacionados con las competencias y funciones de un o una profesional de la archivística o la gestión documental. No es un repaso exhaustivo ni intensivo, pero sirve para dar contexto a la importancia del conocimiento que desde los profesionales del sector podemos aportar a toda organización que tenga en consideración dicha figura como un elemento central de su estructura de gobierno de los datos personales.

Posición del DPD en la organización

Una vez hecho un repaso por la normativa, vamos a centrar la atención en la posición del DPD dentro de la organización. Es posible que muchos de los lectores no sean DPDs, pero por sus funciones, tanto en empresa privada como en entorno público, pueden solicitarlos para algunas de las funciones asociadas a la seguridad

de los datos. Asimismo, conocer las funciones y la relación con las funciones del archivero/a, puede ayudar a fortalecer este segundo frente de la organización.

La Sección 4ª del RGPD entera se dedica a la figura del DPD. En primer lugar, vamos a analizar funciones, competencias y posición orgánica. Empezamos situando la obligatoriedad de la figura. Es obligatoria cuando el tratamiento se efectúa por una autoridad o un organismo público, salvo los tribunales que actúan en el ejercicio de su función judicial. Pero también cuando las actividades principales del responsable o del encargado consisten en operaciones de tratamiento que, por razón de su naturaleza, de su alcance y/o de sus fines, requieren una observación habitual y sistemática de interesados a gran escala; o, finalmente, cuando las actividades principales del responsable o del encargado consisten en el tratamiento a gran escala de categorías especiales de datos, de conformidad con el artículo 9, o de los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10.

Posición del DPD

Cabe indicar que el delegado de protección de datos puede formar parte de la plantilla del responsable o del encargado del tratamiento o ejercer sus funciones en el marco de un contrato de servicios. Por lo tanto, puede ser personal de la empresa o contratarse externamente. En todo caso, su posición ocupa un lugar central en las decisiones estratégicas de la organización, siempre que en estas se incluya el tratamiento de datos personales.

El art. 38 determina que «el responsable y el encargado del tratamiento deben garantizar que el delegado de protección de datos participa de manera adecuada y en el momento oportuno en todas las cuestiones relativas a la protección de datos personales.»

En este artículo hay que destacar los recursos, humanos, económicos y técnicos que se incluyen como responsabilidades del responsable de tratamiento en relación con el DPD:

«Deben facilitar los recursos necesarios para cumplir estas tareas y para acceder a los datos personales y las operaciones de tratamiento, así como para mantener su conocimiento experto».

Por otro lado, hay que garantizar su independencia orgánica. No se puede entender el DPD que, en el marco de sus funciones, actúe bajo ninguna orden directa que pueda incurrir en sus tareas:

«(...) el delegado de protección de datos no reciba instrucciones sobre el ejercicio de estas tareas. El responsable o el encargado no lo puede destituir ni sancionar para ejercer sus funciones. El delegado de protección de datos debe rendir cuentas directamente al nivel jerárquico más alto del responsable o del encargado».

Esta posición lo convierte en una figura con suficiente capacidad para poder emitir informes sin estar condicionado. Asimismo, su posición hace que deba tener acceso a información que puede tener carácter de confidencial, así como recibir peticiones personales, por las que está obligado a mantener el secreto o la confidencialidad en todo lo que se refiere al cumplimiento de las sus funciones.

Por último, el DPD puede no ser un cargo de dedicación exclusiva, depende del volumen y tipología de empresa o administración pública, las tareas que desarrolla se pueden combinar con otras. Eso sí, entre ambas funciones no puede haber conflictos de intereses. ¿Y cuando hay conflicto de intereses? Cuando por su función en la empresa determinase las finalidades de los tratamientos de datos personales de una empresa. En especial, esto se refiere a los altos cargos: dirección general, de operaciones, financiero, jefe de recursos humanos o jefe del departamento TIC. En ningún lugar aparece el conflicto de intereses directo con la figura del archivero/a. Las dudas razonables están, ya que, en los tratamientos vinculados a la gestión del archivo, es el archivero/a quien decide los usos. En todo caso, la influencia a nivel estratégico es mucho menor. Solo el archivero/a que decide en el diseño puede tener conflictos, pero si este es a la vez DPD, estas decisiones se toman justamente teniendo en cuenta la protección de los datos desde el diseño y por defecto. Capacidad de decisión que va directamente ligada al código deontológico de los archiveros. Aquí hay que recordar la Declaración Universal de los Archivos (DUA), que nos compromete a trabajar para que:

- los archivos sean gestionados y preservados en las condiciones que aseguren su autenticidad, su fiabilidad, su integridad y su uso;
- los archivos sean accesibles a todos, respetando las leyes pertinentes y las relativas a los derechos de las personas, de los productores, de los propietarios y los usuarios

Es por tanto una diferencia clave respecto a otras profesiones, el acceso con el respeto a la protección de los datos está en el propio “ser” archivístico. En todo caso, como dice el GT29 (3.5), es recomendable que la propia institución determine los lugares que son incompatibles y haga una declaración conforme que su DPD no tiene ningún conflicto de intereses.

Competencias y funciones del DPD

A un DPD se le requieren competencias específicas, sobre todo conocimiento en derecho y protección de datos (art. 37.5 RGPD). Pero el GT29 aclara algún aspecto más:

- Conocimientos especializados en legislación nacional y europea en protección de datos y conocimiento del RGPD.
- Comprensión de las actividades de tratamiento.

- Comprensión de las tecnologías de la información y de la seguridad de datos.
- Conocimiento del sector empresarial y de la organización.
- Capacidad para fomentar una cultura de protección de datos dentro de la organización.

En relación con las funciones del DPD, éstas están indicadas en el art. 39 del RGPD:

- Informar y asesorar de sus obligaciones al responsable o al encargado del tratamiento y a los empleados que se ocupan del tratamiento.
- Supervisar el cumplimiento de la normativa en materia de protección de datos.
- Ofrecer el asesoramiento que se le solicite sobre la evaluación de impacto relativa a la protección de datos y supervisar su aplicación.
- Cooperar con la autoridad de control.
- Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento.

Entramos en más detalle a dos de las funciones:

- Supervisar el cumplimiento de la normativa en materia de protección de datos.

Supervisar no significa ser responsable. Como parte de la supervisión, el DPD ha de recoger información del tratamiento, analizar si se adecua a la finalidad y normativa, e informar y asesorar al respecto. El análisis de procesos es necesario para la elaboración del Cuadro de clasificación corporativo, por lo tanto, si asociamos tratamiento con proceso, podemos llegar a retroalimentar las dos funciones, archivero/a y DPD, y en realidad, reforzar la tarea del primero/a.

- Ofrecer el asesoramiento que se le solicite sobre la evaluación de impacto relativa a la protección de datos y supervisar su aplicación.

El DPD no debe hacer la evaluación de impacto, pero su asesoramiento es necesario o muy recomendable. Sobre todo, es necesario contar con el DPD para decidir si el tratamiento requiere EIPD (evaluación de impacto). También se recomienda que se le consulte la metodología y las recomendaciones para mitigar el riesgo, así como si las conclusiones y las medidas tomadas son correctas conforme el RGPD. Contar con el DPD en este momento, significa que debe formar parte de la toma de decisión de un nuevo tratamiento, situándolo en el momento en el que se puede decidir el modelo de datos necesario.

Hemos visto las funciones del DPD, claramente enfocadas a convertirse en una especie de órgano de control de la gestión interna sobre la calidad del tratamiento de datos personales. Incluyendo, por este propósito, tanto el diseño de nuevos tratamientos, por tanto, proyectos o nuevas contrataciones de sistemas de gestión, incidiendo en el modelo de datos, como en el continuo del tratamiento, las incidencias en el mismo, el acceso y la protección de los datos, hasta su valoración de tiempo de conservación.

Competencias y funciones del profesional de gestión documental y archivo

Como se ha visto, el control de la gestión de la información, angular de la gestión documental, está en todo el articulado del RGPD-LOPDGDD y normativas derivadas. Pero, y el archivero/a, ¿puede encajar con este rol? ¿O podría, al menos, ser una pieza clave del análisis de la gestión de los datos personales y los tratamientos correspondientes?

Seguro que ya sabéis la respuesta, pero vamos a verlo mejor analizando las funciones de un técnico/a de gestión documental y archivo. Nos basaremos en el análisis que la Associació d'Arxivers-Gestors de documents de Catalunya ha hecho recientemente, sobre el puesto de técnico superior archivero (<https://arxivers.com/mon-laboral/model-de-fitxa-de-lloc-de-treball/>).

En primer lugar, observaremos el objeto de puesto de trabajo:

- Garantizar la gestión eficiente y el acceso a la información corporativa de acuerdo con las competencias municipales atribuidas por la ley en materia de gestión de documentos y patrimonio cultural.
- Dirigir el sistema único de gestión de la información pública municipal que abarcará el diseño de los sistemas de producción, la captura, la tramitación, el control, la evaluación y la conservación de los datos y los documentos, y el acceso a estos.
- Asegurar que la producción documental de la corporación sea accesible, usable, íntegra, de calidad, y se garantice su confidencialidad y conservación.
- Administrar la plataforma de gestión de documentos electrónicos, elaborar planes estratégicos de preservación digital y realizar tareas de control continuas en la producción y gestión de los documentos para auditar el buen funcionamiento del sistema, además de asesorar al personal en el uso de la plataforma.
- Analizar los procesos de gestión administrativa desde la perspectiva documental para su racionalización, simplificación y mejora continua.

En segundo lugar, observaremos las funciones asociadas:

- Promoción y dirección técnica de la implantación y el mantenimiento del sistema de gestión integral de la documentación municipal.
- Formar parte integrante, con voz y voto, de todo organismo creado para la gestión de la calidad y el desempeño del ordenamiento jurídico en materia de gestión documental, protección de datos de carácter personal, acceso a los documentos, identificación electrónica del ciudadano, procesos de digitalización de procedimientos administrativos, seguridad de la información digital, transferencia masiva de datos para actualización de estándares u otra evolución tecnológica.
- Definir, implantar y mantener, con el resto de las áreas implicadas, las condiciones técnicas requeridas para cumplir las medidas mínimas para una correcta interoperabilidad.
- Dirección técnica, creación y mantenimiento del cuadro de clasificación municipal.
- Definir el listado de documentos esenciales.
- Proponer y actualizar las normas de acceso y consulta pública de la documentación.
- Definir y mantener el vocabulario de metadatos.
- Definir, supervisar y administrar el gestor documental.
- Definir, gestionar y supervisar la creación y captura de documentos.
- Supervisar el sistema de digitalización segura de la documentación.
- Controlar el buen uso de formatos de la documentación electrónica y su migración para garantizar el acceso a lo largo del tiempo y su conservación.
- Realizar las transferencias de documentación.
- Analizar los sistemas que gestionan documentación e información.
- Garantizar que se apliquen medidas de seguridad en la conservación de los documentos.
- Definir y gestionar el tratamiento archivístico integral de los documentos.
- Elaborar normas, reglamentos, protocolos.
- Participar activamente en el cumplimiento de la legislación vigente en materia de transparencia y rendimient de cuentas democrático.
- Participar activamente en el cumplimiento de la legislación vigente en materia de protección de datos y su gestión.
- Proteger la propiedad intelectual y otros derechos que afecten a la documentación gestionada.

- Participar y proponer a los organismos competentes la creación de órganos consultivos y comisiones asesoras y de trabajo en todo lo relacionado con la gestión documental y el patrimonio cultural municipales.
- Definir y gestionar los documentos que forman parte del fondo municipal y los fondos privados integrados en el Archivo.
- Elaborar las propuestas de eliminación documental.
- Disponer de unidades documentales compuestas y simples para la consulta interna y su préstamo.
- Atender las consultas externas e internas.
- Elaborar copias de planos y otros documentos.
- Informar y asesorar a los usuarios del servicio de archivo.
- Asegurar la conservación del patrimonio documental.
- Proteger la memoria corporativa, personal y colectiva.
- Difundir los fondos documentales.
- Colaborar con el servicio de informática en preparar y formular directrices encaminadas a la informatización del patrimonio documental municipal.
- Organizar, con otras concejalías, actividades de difusión del patrimonio documental del municipio.
- Asesorar y proponer la adquisición de nueva documentación.
- Asumir la búsqueda y el salvamento de documentos de archivo de instituciones o de particulares.
- Programar y presupuestar las actividades del servicio.
- Contratar, o participar en la contratación, obras, servicios o suministros necesarios según varias líneas de trabajo o requerimientos del servicio.

Vistas las funciones del DPD y de lo que podrían ser un modelo de funciones de un/a técnico/a archivero/a, vamos a resaltar aquellas funciones que justifican atenderle como un/a posible DPD o como un miembro del equipo o comisión de seguridad del organismo (Figura 2).

Como acabamos de ver, la correlación, si no exacta, sí que es coincidente, en parte o, en algunos casos, en su totalidad.

Pero si nos fijamos en las competencias, aún es más evidente (Figura 3).



Figura 2. Comparación de funciones DPD y Archivero/a



Figura 3. Comparación de competencias DPD y Archivero/a

Tres conocimientos clave comparados

Analizamos finalmente, tres conocimientos clave comparados: tecnológico, organizativo y legislativo.

- A nivel tecnológico. Un/a archivero/a requiere de un alto conocimiento tecnológico, ya que el conocimiento de los sistemas de programación y el lenguaje ayuda a la capacidad de entender los sistemas que crean datos. Un DPD, por su lado, requiere el conocimiento tecnológico necesario para comprender los datos a tratar o gestionar en los sistemas de la organización.
- A nivel organizativo. Un archivero/a requiere un conocimiento organizativo actualizado y transversal, ya que el mantenimiento de un CdC y las herramientas de gestión documental adaptadas y adecuadas a la evolución de la organización es una condición básica para un buen control y gestión de la información. Un DPD requiere el conocimiento organizativo necesario para saber qué datos personales se procesan, en qué sistemas, para qué fines y tipologías y bajo qué regulaciones o empoderamiento legal.
- A nivel legislativo. Un archivero/a requiere un conocimiento normativo tanto sobre confidencialidad, preservación, acceso a la información, transparencia, conservación documental, así como en materia de protección de datos personales, tanto en archivos históricos como administrativos. Un DPD requiere un amplio conocimiento normativo en la protección de datos, pero también de las normas sectoriales más comunes y que condicionan el posible acceso y gestión de datos. El conocimiento de la transparencia y el acceso también se convierte en clave para la gestión del RGPD.

Esta comparación deja en clara consideración la pareja relación entre archivero/a y DPD. Competencias básicas iguales, funciones y competencias asimilables.

Vamos a ver ahora, una de las herramientas básicas del RGPD y su estrecha relación con otra de las herramientas básicas de la gestión documental: el Cuadro de clasificación.

Creación del Registro de actividades de tratamiento a partir del Cuadro de clasificación

El Registro de actividades de tratamiento (RAT) es un elemento fundamental del RGPD. En él se establecen con vocación transparente, los procesos en los que hay datos personales asociados, para que un tercero, interesado o no, pueda ver todos los tratamientos de datos personales de una organización. Y no solo el listado,

sino la tipología de datos, las funciones, los accesos, la normativa que le afecta, partes interesadas, etc. Y es que, de conformidad con el artículo 30.1 del Reglamento, cada persona a cargo, y en su caso su representante, deberá llevar un registro de las actividades de tratamiento (RAT) realizadas bajo su responsabilidad.

Una de las tareas más complejas como organización, cuando se considera adaptarse al RGPD, es la realización del RAT. Detectar en qué actividades hay datos personales, y de toda la empresa o institución, puede ser un proceso que requiere meses de análisis. Si nos fijamos en los campos que debe tener el RAT, veréis lo específico y necesario que es saber, por lo tanto, cómo se procesan los datos.

¿Qué información debería tener según el art. 30 GDPR? (modelo de datos)

- El nombre y los datos de contacto de la persona a cargo
- Los fines del procesamiento
- Categorías de partes interesadas
- Categorías de datos personales
- Categorías de destinatarios a los que se han comunicado o comunicarán los datos personales
- En su caso, las transferencias de datos personales a terceros
- Si es posible, los plazos para eliminar las diferentes categorías de datos
- Si es posible, una descripción general de las medidas de seguridad técnicas y organizativas a que se refiere el artículo 32, sección 1.

Vamos a ver en detalle, alguno de los datos indicados:

- Base jurídica de los datos de tratamiento: es decir, en relación con el art. 6 del RGPD, indicar en qué os legitimáis para recoger los datos. Por qué os basáis en una ley, cuando más exacto sea, más transparente será para el usuario.
- Finalidades de tratamiento. Siempre bajo una base determinada, explícita y legítima. No se podrán tratar los datos para otros fines de los expresados, a excepción de los de archivo en interés público, de investigación científica e histórica y los fines estadísticos, como ya hemos visto.
- Categorías de interesados: es decir, de quién recogemos los datos. Hay que ser precisos y al mismo tiempo lo suficientemente generales para incluir la mayor parte de la población de quien se cojan los datos. Cuenta especialmente con los colectivos vulnerables.
- Descripción de los datos: En este punto, pueden ser más generales o concretos. En todo caso, los datos deben ser adecuados, pertinentes y limitados a lo que es necesario en relación con las finalidades para las que se tratan, así como exactos y, si es necesario, deben actualizarse. Se puede

quedar en esta generalidad, o entrar en el detalle de cada tipo de dato recogido dentro de las categorías. Es recomendable ser lo más transparente posible, pero depende del nivel de detalle al que se quiera llegar.

- Categorías de destinatarios: estamos hablando de las comunicaciones de datos, no de las transferencias internacionales. Es decir, del traspaso de datos muy vinculado a la interoperabilidad o el necesario traspaso de datos por el cumplimiento de la finalidad misma.
- Transferencias internacionales: transferencia a otros países. Si la transferencia internacional de datos a un tercer país o una organización internacional se realiza mediante garantías adecuadas, hay que hacerlo constar en este registro y aportar la documentación de estas garantías.
- Plazos previstos para suprimir los datos: este es el punto más claramente relacionado con las políticas de evaluación de la gestión documental. El vínculo con las TAAD podría ser un sistema de garantizar la supresión por razón de unos criterios técnicos y de determinación de los valores de los documentos y la información.
- Descripción de los criterios técnicos y organizativos de seguridad: siguiendo el art. 32 del RGPD, es necesario que el responsable y el encargado del tratamiento apliquen las medidas técnicas y organizativas adecuadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros: a) La pseudoanonimización y el cifrado de datos personales; b) La capacidad de garantizar la confidencialidad, la integridad, la disponibilidad y la resiliencia permanentes de los sistemas y de los servicios de tratamiento; c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de manera rápida, en caso de incidente físico o técnico; d) Un proceso para verificar, evaluar y determinar regularmente la eficacia de las medidas técnicas y organizativas establecidas para garantizar la seguridad del tratamiento.
- Procedencia de los datos: en este punto se ha de concretar las personas, instituciones u órganos que facilitarán los datos personales que se quieren recoger.
- Evaluación de impacto: Apartado para indicar si se ha hecho una evaluación de impacto de algún tratamiento, incluso, algún órgano de control proponer colgar el informe de la evaluación con relación al tratamiento.
- Encargado de tratamiento: En este punto, se incluye si hay nombrado algún encargado de tratamiento, y, en su caso, vuelve a abrirse la posibilidad de añadir el contrato, acuerdo o convenio que se firma con él.

¿Qué datos podemos aportar desde la archivística?

El vínculo evidente que hemos ido destacando a lo largo de este artículo es, sin duda, el Cuadro de clasificación funcional. El CDC, en primer lugar, funcionará si se tiene en cuenta desde su vínculo directo con el proceso administrativo. Por eso no puede funcionar con un CDC orgánico o plenamente vinculado a la estructura política.

¿Y cómo entenderemos el CDC?

La clasificación, siguiendo ISO 15489:2016, es el sistema basado en una estructura jerárquica y lógica que permite la identificación de los procesos de la organización, la identificación de la documentación generada y la agrupación física o intelectual de la información; enfocando su finalidad en el acceso y la recuperación de la información documentada generada por la organización. Las actividades de tratamiento, como actividades, no se definen en el RGPD, pero sí el tratamiento en sí, como una operación sobre datos personales. La actividad, por tanto, va ligada al tratamiento.

Así pues, ¿podemos asociar series (entendidas como procesos) como actividades de la organización? Y si las series son actividades (nos pueden venir aquí reminiscencias robergianas), ¿podríamos decir que las series con datos personales son, en sí mismas, actividades de tratamiento según el RGPD? Si os fijáis en los campos que debe tener el RAT, veréis cuán importante y necesario es conocer, por tanto, cómo se tratan los datos. Esta tarea, sin embargo, es casi comparable a la elaboración de un CDC.

La realización de un CDC parte de unas premisas básicas:

- Revisamos el contexto externo y la normativa que le afecta
- Revisamos el contexto interno (normativa)
- Revisamos la historia de la organización
- Revisamos la estructura organizativa, las funciones y la documentación
- Establecemos la jerarquía entre procesos y funciones

La elaboración del CDC, por tanto, nos aporta por cada serie: contexto legal, social, histórico y productivo, y además nos relaciona las evidencias documentales del proceso, los documentos y los datos generados. Exactamente esto es lo que necesitamos para construir un RAT. Es más, para el RAT, basta las series que tratan datos personales, pero si ya tenemos un CDC, esto ya lo podemos tener detectado; o, al menos, nos es mucho más fácil de detectar.

Por otro lado, está claro que el proceso de construcción del RAT nos aporta valor también al CDC. La obligación de vincular por cada nuevo tratamiento, una leyenda informativa y ligarla al RAT, nos envía a revisar nuestras series del CDC, transformarlas, adaptarlas o, incluso, crearlas explícitamente. Esto sólo

lo podremos ligar, pero, si lo hacemos controlando el RAT. Y es que, si controlamos el CDC, ¿por qué no podemos controlar el RAT? ¿Qué otro técnico/a del organismo conoce mejor el sistema productivo de la organización?

Si os he convencido de la importancia de vincular RAT y CDC, y que el primero refleje el segundo, así como que el segundo alimente el primero, y viceversa, el segundo paso es unificarlos. ¿Cómo?

Asociando cada actividad con el código del CDC para agilizar y racionalizar la gestión de las dos herramientas. Una gestión conjunta simplifica y da contexto a cada actividad, unifica esfuerzos y estrategias. Además, si unificamos, damos más valor al CDC, porque conseguimos controlar la entrada y la difusión de los datos siguiendo un único modelo organizativo, estable y contrastado. Por este motivo, tendremos nuevos campos a los ya vistos:

- Código de tratamiento = Código del CDC
- Nombre del tratamiento = nombre de la serie

Y si hacemos este paso, en la estructura o modelo de datos que usamos para gestionar nuestro CDC, podemos incluir también qué series tienen datos personales.

Pero podemos llegar más lejos. Recordemos que hay un dato que el RGPD nos obliga a aportar en el RAT: Plazos previstos para eliminar información. Exacto, como ya hemos dicho, aquí tenemos la puerta abierta al vínculo con las tablas de retención de las comisiones correspondientes. Un nuevo campo para nuestro modelo de datos de RAT, ya que el plazo es un campo de tiempo, necesitaremos añadir:

- Número de tabla
- Nombre de la tabla
- Política aplicada de retención

Quizá algunas ya lo piensan, y sí, estamos uniendo una nueva herramienta derivada del CDC: el calendario de conservación. De nuevo, ya teníamos el trabajo hecho (tal vez), solo basta atarlo.

¿Y aún podemos asociar más datos?

Hay que tener en cuenta que el RAT es una herramienta muy potente de información, tanto que lo acerca a las herramientas de transparencia y que las leyes como las de transparencia, no contemplaron. Curiosamente, el RGPD sí. Con todo, hay siempre partir de la información clara, sencilla y fácil para la ciudadanía. Se pueden añadir campos extras como los circuitos administrativos asociados a cada actividad, las unidades administrativas que intervienen (acceso interno), los trámites de la web por donde entra parte de la información, el vínculo entre actividades relacionadas... y podemos asociar el cuadro de acceso, si lo tenemos definido. Todo este conjunto se podrá entender si tenemos un sistema de gestión documental y gobernanza de la información establecido y estable.

Finalmente, en una organización madura desde el punto de vista de gestión informacional, se pueden informar de los documentos, tipo documental, asociados a cada actividad, dando información así de los formatos, soportes, y tramitación administrativa. Es decir, más allá de las puertas de entrada, estamos enseñando directamente la casa por dentro.

Finalmente, una vez construido el RAT-CDC hay que mantener la estructura; por este motivo, se recomienda que un equipo interdisciplinario vigile su actualización y conformidad, así como los cambios y mejoras. Este equipo debería ser el mismo que ejerce similares funciones sobre el CDC y debe incluir, por supuesto, el DPD y el archivero/a, así como equipo jurídico, organizativo y tecnológico.

Un modelo de RAT construido desde esta vertiente, es el que hemos construido en Sant Cugat del Vallès, y se puede ver en: <https://www.seu-e.cat/es/web/santcugatdelvalles/registre-de-les-activitats-de-tractament-de-dades-personals>

Conclusiones

La asunción del rol de DPD por parte del archivero/a, como resumen, queda claramente justificado. Ahora es el momento de jugar esta carta, valorar pros y contras, ver las ventajas de su posicionamiento orgánico y de la posible posición dentro del cuadro de mando donde se elaboran las políticas de datos de la organización. Es cuestión de redefinir esfuerzos, poner en balanza los recursos y los objetivos, y decidir cuál será el siguiente paso.

¿Cuáles son los elementos clave antes de aceptar el cargo? Aquí un resumen final:



Figura 4. Escalera de pasos antes de aceptar el cargo de DPD

Pactar una posición orgánica diferenciada, que no conlleve conflictos con ningún cargo. La posición del DPD no puede condicionarse a ninguna estructura organizativa intermedia. En segundo lugar, asociar a la asunción del cargo, recursos humanos y económicos, dimensionados al tamaño y características de la organización, y a las funciones de gestor documental que ya tienes asociadas y que retroalimentan, como hemos visto, el nuevo cargo. Con relación a esto, elaborar un plan de redimensionamiento de tareas y, si es el caso, una compensación horaria, ya que el volumen de trabajo asumido por la nueva posición requiere de una reconsideración del servicio o del puesto de trabajo. Este aspecto es muy importante para una auténtica fiabilidad y garantía de calidad en las competencias y funciones asumidas. Finalmente, y como garantía, es esencial pactar un tiempo de prueba, que permita evaluar la carga de trabajo y redimensionar, si es necesario, el proyecto.

En conclusión, como hemos visto a lo largo de esta exposición, el archivero/a está capacitado, tanto por funciones como por competencias, además de por sus herramientas de gestión y por su conocimiento, para ejercer el cargo de delegado/a de protección de datos. Como expertos en gestión de la información, tenemos el deber de establecer políticas para su definición, gobierno y preservación. La del DPD es una de las funciones asociadas que podemos desempeñar, una de muchas otras que pueden relacionarse con otros cargos que la gestión de datos está generando (Chief Data Officer, Data Steward, Data Governance, ...). Tenemos que saber visualizar estos nuevos puestos como oportunidades, tanto para asumirlas como para establecer alianzas, y, sobre todo, no perder la ocasión para hacer resaltar nuestras capacidades para aportar en equipos multidisciplinares. El futuro se configura en cada decisión tomada hoy. Como dice el dicho: no esperes a mañana lo que puedas hacer hoy, si no quizá ya sea tarde.

Bibliografía

- Declaración Universal de los Archivos (DUA), ICA, 10 de noviembre de 2011. <https://www.ica.org/sites/default/files/UDA_June2012_press_SP.pdf> [Consulta: 12/07/2021].
- Cataluña. Modelo de ficha de lugar de trabajo de técnico superior archivero, AAC, 2019. <<https://arxiv.com/mon-laboral/model-de-fitxa-de-lloc-de-treball/>> [Consulta: 12/07/2021].
- Unión Europea. Reglamento (UE) 2016/679 del Parlamento europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (de ahora en adelante, RGPD)
- UNE-ISO 15489-1:2016. Información y documentación. Gestión de documentos. Parte 1: Conceptos y principios. AENOR. 2016.