LA AUTOEVALUACIÓN EN MATERIA DE PROTECCIÓN DE DATOS: UN EJERCICIO DE RESPONSABILIDAD PROACTIVA DE LAS ENTIDADES LOCALES

Lluís Sanz Marco
Delegado de Protección de Datos
Ayuntamiento de Barcelona

Ana Marzo
Abogada Equipo Marzo

M. Ascensión Moro Cordero
Responsable del Departamento de Gobierno Abierto
Delegada de Protección de Datos
Ayuntamiento de Sant Feliu de Llobregat

"Principio: los datos, tan abiertos como sea posible, tan cerrados como sea necesario". Directiva (UE) 2019/1024 del Parlamento Europeo y del Consejo de 20 de junio de 2019 relativa a los datos abiertos y la reutilización de la información del sector público

RESUMEN: Los nuevos modelos de relación de la ciudadanía con las Administraciones públicas exigen, como presupuesto previo, dar cumplimiento a un marco regulatorio complejo y profuso, garantizando la seguridad jurídica y mejorando la eficiencia administrativa.
En este punto, el liderazgo de las Administraciones públicas en cuanto a la cultura de respeto a los derechos y libertades de las personas físicas en relación con el tratamiento de datos personales, es clave para garantizar a la ciudadanía un "ecosistema de confianza" en un escenario de permanente transformación digital, disrupción y generación de nuevos riesgos.
Por ello, es prioritario que, en particular, las entidades locales dispongan de herramientas fácilmente utilizables y accesibles, que garanticen adecuadamente los derechos de protección de datos de las personas interesadas en su relación con las Administraciones públicas.

PALABRAS CLAVE: autoevaluación, protección de datos, privacidad, *accountability*, confianza, transformación digital, integridad, Buen Gobierno, Buena Administración, *compliance.*

ABSTRACT: The new models of relationship between citizens and public administrations require, as a prior budget, compliance with a complex and profuse regulatory framework, guaranteeing legal certainty and improving administrative efficiency.
On this point, the leadership of public administrations in terms of the culture of respect for the rights and freedoms of natural persons in relation to the processing of personal data, is key to guaranteeing citizens an "ecosystem of trust" in a scenario of permanent digital transformation, disruption and generation of new risks.
For this reason, it is a priority that, in particular, local entities have easily usable and accessible tools that adequately guarantee the data protection rights of the persons interested in their relationship with public administrations.

KEYWORDS: self-assessment, data protection, privacy, accountability, trust, digital transformation, integrity, Good Governance, Good Administration, compliance

DE DATOS. III. LA NECESIDAD DE UNA POLÍTICA INTEGRAL DE PROTECCIÓN DE DATOS EN LAS ENTIDADES LOCALES. IV. UNA HERRAMIENTA PARA FACILITAR LA EVALUACIÓN Y EL AUTODIAGNÓSTICO. V. CONCLUSIONES. VI. BIBLIOGRAFÍA

I. INTRODUCCIÓN

Es evidente que nos encontramos transitando hacia un nuevo orden social, económico y político en el que las tecnologías disruptivas, en especial la Inteligencia Artificial (IA), suponen un desafío enorme en múltiples dimensiones. En este camino, las Administraciones públicas llevan ya bastante tiempo inmersas en un proceso de cambio profundo y estructural hacia una administración inteligente, sostenible, abierta, inclusiva y social, que sea capaz de abordar desafíos en materia de emergencia climática, transformación digital, sostenibilidad, resiliencia, lucha contra desigualdades de todo tipo, en definitiva, la consecución de los objetivos de desarrollo sostenible que nos marca la Agenda 2030 a nivel global y otras agendas a nivel europeo, estatal, autonómico e, incluso, local.

Parte de este cambio se debe, entre otros muchos factores, al enorme impacto que supone la revolución digital y la nueva economía de los datos que, en los últimos años, ha crecido exponencialmente llegando a cifras realmente estratosféricas: si en 2018 el volumen de datos producidos anualmente se calculó en 33 zettabytes, para 2025 se estima que sean 175 zettabytes (siendo un zettabyte el equivalente a mil trillones de bytes).

Este intercambio masivo de datos provoca, a su vez, un aumento también exponencial de los tratamientos que se pueden desarrollar con estos datos, lo que genera al mismo tiempo un mayor interés entre las empresas, centros de investigación y Administraciones públicas para utilizar estos datos con distintas finalidades. Y es en este escenario de transformación integral y holística donde aterriza 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 (RGPD), en plena efervescencia de los nuevos retos que para la protección de datos plantea la rápida evolución tecnológica y la globalización (Considerando 6 RGPD). Este desafío, junto al que supone el volumen cada vez mayor de información personal que difunden las personas físicas a escala mundial,

hace necesario regular de forma homogénea la garantía de este derecho fundamental a la protección de datos.

Junto a este Reglamento, el marco normativo español en materia de protección de datos se complementa con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD). Un binomio normativo (JIMÉNEZ ASENSIO, 2019) que viene a cambiar radicalmente la forma y la cultura de la gestión de los datos personales, pasando de un modelo reactivo, en el que se determinaban las medidas aplicables en función del tipo de datos objeto del tratamiento, **a un modelo proactivo y centrado en la gestión de riesgos,** es decir, en establecer medidas técnicas y organizativas en función de los riesgos detectados mediante la realización del análisis previo, lo que se entiende como **privacidad por defecto y desde el diseño.** El objetivo es disponer de instrumentos que nos permitan garantizar la protección de datos y los derechos y libertades de la ciudadanía en un mundo cada vez más digitalizado y sometido a una aceleración constante, sobre todo en lo referente a los procesos tecnológicos.

Esta orientación preventiva precisamente trata de anticiparse a la irrupción vertiginosa de la tecnología que implica un uso masivo y exponencial de datos, con el objetivo de preservar la privacidad y los derechos y libertades fundamentales de la ciudadanía. Al final, de lo que se trata, es de que las personas físicas tengan control de sus propios datos personales (Considerando 7 RGPD), que puedan conocer y decidir de forma continua sobre el acceso y uso de sus datos y, para ello, es necesario reforzar su seguridad jurídica y práctica con el objetivo de generar la confianza necesaria para permitir el desarrollo integral de la economía digital en todo el mercado interior.

Casi a punto de cumplirse cinco años desde la plena aplicabilidad del RGPD, parece necesario que, en particular, las entidades locales dispongan de instrumentos para poder evaluar el grado de cumplimiento de esta normativa como garantía máxima de protección de datos, derechos y libertades de una ciudadanía cada vez más concienciada y empoderada que reclama confianza en el uso de sus datos por parte de las instituciones públicas.

II. EL REGISTRO DE ACTIVIDADES DE TRATAMIENTO: UN INSTRUMENTO ESENCIAL PARA GARANTIZAR EL DERECHO A LA PROTECCIÓN DE DATOS

Con la vigente normativa de protección de datos personales no se requiere ninguna actividad de notificación o inscripción de ficheros a la Agencia Española de Protección de Datos (AEPD) o autoridad autonómica competente, pero en cambio, se obliga a las organizaciones a implementar el llamado Registro de Actividades de Tratamiento (RAT). El cambio conceptual es muy relevante, ya que pasamos del concepto "fichero" (¿qué datos tratamos?) al concepto "tratamiento" (¿cómo y para qué tratamos los datos?). La diferencia fundamental (SANZ MARCO, 2018) radica en que "el primero se basa en la naturaleza de los datos tratados, mientras que el segundo se apoya en dos conceptos: los procesos que intervienen en el tratamiento de los datos y el nivel de riesgo específico inherente a los mismos, donde hay que considerar no sólo la naturaleza de los datos, sino también la tecnología empleada en el tratamiento, el alcance del mismo y cobertura normativa".

De hecho, estas definiciones vienen recogidas en el artículo 4 del RGPD:

> *«Fichero»: todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica.*
>
> *«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.*

Para facilitar este tránsito de conceptos, la AEPD propone dos vías para generar el primer registro de actividades de tratamiento:

- Partir de los ficheros que ya estuvieran inscritos en las autoridades de control y realizar un ejercicio de identificación de los tratamientos que identifiquen finalidades diferentes.

- Considerar las diferentes operaciones básicas de tratamiento concretas a una finalidad básica común de todas ellas.

Por lo tanto, los responsables y encargados de tratamientos de las Administraciones públicas deberán crear y mantener este Registro de Actividades de Tratamiento por escrito, incluso en formato electrónico, que deberá estar a disposición de la Autoridad de Control. El contenido y funciones del Registro de Actividades de Tratamiento está regulado en el artículo 30 del RGPD:

> *"1. Cada responsable y, en su caso, su representante llevarán un registro de las actividades de tratamiento efectuadas bajo su responsabilidad. Dicho registro deberá contener toda la información indicada a continuación:*
> *a) el nombre y los datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable, y del delegado de protección de datos;*
> *b) los fines del tratamiento;*
> *c) una descripción de las categorías de interesados y de las categorías de datos personales;*
> *d) las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales;*
> *e) en su caso, las transferencias de datos personales a un tercer país o una organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49, apartado 1, párrafo segundo, la documentación de garantías adecuadas;*
> *f) cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos; g) cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 32, apartado 1.*
>
> *2. Cada encargado y, en su caso, el representante del encargado, llevará un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de un responsable que contenga:*
> *a) el nombre y los datos de contacto del encargado o encargados y de cada responsable por cuenta del cual actúe el encargado, y, en su caso, del representante del responsable o del encargado, y del delegado de protección de datos;*

b) las categorías de tratamientos efectuados por cuenta de cada responsable;
c) en su caso, las transferencias de datos personales a un tercer país u organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49, apartado 1, párrafo segundo, la documentación de garantías adecuadas;
d) cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 30, apartado 1."

Es importante señalar que no disponer de dicho registro supone una infracción grave tal y como se indica en el artículo 73 n) de la LOPDGDD y que, además, el RAT deberá hacerse público en virtud del artículo 31 de la citada Ley Orgánica que, a su vez, mediante Disposición final undécima modificó la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información y buen gobierno, añadiendo un nuevo artículo 6 bis para recoger esta obligación.

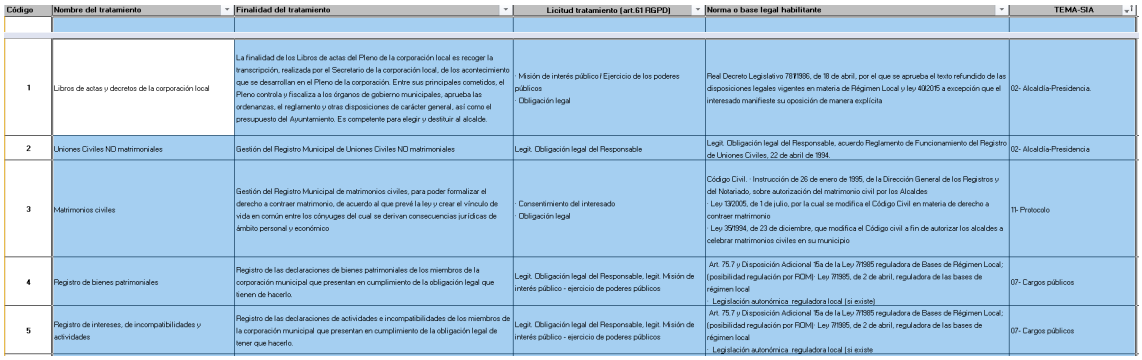
Se trata pues de un instrumento fundamental para garantizar el principio de responsabilidad proactiva y "accountability" que propugna este nuevo paradigma de gestión de los datos personales y, por lo tanto, se debe prever también su mantenimiento y actualización permanente. Para ello se requiere:

- Realizar autoevaluaciones periódicas en el marco de la organización de la seguridad y la privacidad de cada institución

- Formación y seguimiento con los ámbitos responsables directos de los diferentes tratamientos

- Incorporar en los procedimientos de contratación, convenios, etc. formularios en relación con el tratamiento de datos personales para que, en su caso, se pueda identificar la necesidad de incorporar nuevos tratamientos en el RAT, modificar los existentes o, incluso, la necesidad de realizar una evaluación de impacto.

Para facilitar la tarea de elaboración del RAT, el grupo de trabajo de la comisión de *"Sociedad de la Información, Innovación Tecnológica y Agenda Digital"* de la Federación Española de Municipios y Provincias (FEMP), integrado por Ayuntamientos y Diputaciones provinciales, ha elaborado una propuesta de RAT tipo con aquellos tratamientos que cualquier entidad local, sea cual sea su tamaño, debería contemplar en su inventario con la información mínima a la que obliga la normativa vigente. Esta propuesta de RAT básico (que se publicitará desde la FEMP) se articula en torno a 60 tratamientos en los que ya aparecen predeterminados los campos siguientes: nombre del tratamiento, finalidad, licitud, norma o base legal habilitante, correspondencia con la temática del Sistema de Información Administrativa (SIA).



Código	Nombre del tratamiento	Finalidad del tratamiento	Licitud tratamiento (art.6 RGPD)	Norma o base legal habilitante	TEMA-SIA
1	Libros de actas y decretos de la corporación local	La finalidad de los Libros de actas del Pleno de la corporación local es recoger la transcripción, realizada por el Secretario de la corporación local, de los acontecimiento que se desarrollan en el Pleno de la corporación. Entre sus principales cometidos, el Pleno controla y fiscaliza a los órganos de gobierno municipales, aprueba las ordenanzas, el reglamento y otras disposiciones de carácter general, así como el presupuesto del Ayuntamiento. Es competente para elegir y destituir al alcalde.	· Misión de interés público / Ejercicio de los poderes públicos · Obligación legal	Real Decreto Legislativo 781/1986, de 18 de abril, por el que se aprueba el texto refundido de las disposiciones legales vigentes en materia de Régimen Local y ley 40/2015 a excepción que el interesado manifieste su oposición de manera explícita	02- Alcaldía-Presidencia
2	Uniones Civiles NO matrimoniales	Gestión del Registro Municipal de Uniones Civiles NO matrimoniales	Legit. Obligación legal del Responsable	Legit. Obligación legal del Responsable, acuerdo Reglamento de Funcionamiento del Registro de Uniones Civiles, 22 de abril de 1994.	02- Alcaldía-Presidencia
3	Matrimonios civiles	Gestión del Registro Municipal de matrimonios civiles, para poder formalizar el derecho a contraer matrimonio, de acuerdo al que prevé la ley y crear el vínculo de vida en común entre los cónyuges del cual se derivan consecuencias jurídicas de ámbito personal y económico	· Consentimiento del interesado · Obligación legal	Código Civil. · Instrucción de 26 de enero de 1995, de la Dirección General de los Registros y del Notariado, sobre autorización del matrimonio civil por los Alcaldes · Ley 13/2005, de 1 de julio, por la cual se modifica el Código Civil en materia de derecho a contraer matrimonio · Ley 35/1994, de 23 de diciembre, que modifica el Código civil a fin de autorizar los alcaldes a celebrar matrimonios civiles en su municipio	11- Protocolo
4	Registro de bienes patrimoniales	Registro de las declaraciones de bienes patrimoniales de los miembros de la corporación municipal que presentan en cumplimiento de la obligación legal que tienen de hacerlo.	Legit. Obligación legal del Responsable, legit. Misión de interés público - ejercicio de poderes públicos	Art. 75.7 y Disposición Adicional 15a de la Ley 7/1985 reguladora de Bases de Régimen Local; (posibilidad regulación por RDM) · Ley 7/1985, de 2 de abril, reguladora de las bases de régimen local · Legislación autonómica reguladora local (si existe)	07- Cargos públicos
5	Registro de intereses, de incompatibilidades y actividades	Registro de las declaraciones de actividades e incompatibilidades de los miembros de la corporación municipal que presentan en cumplimiento de la obligación legal de tener que hacerlo.	Legit. Obligación legal del Responsable, legit. Misión de interés público - ejercicio de poderes públicos	Art. 75.7 y Disposición Adicional 15a de la Ley 7/1985 reguladora de Bases de Régimen Local; (posibilidad regulación por RDM) · Ley 7/1985, de 2 de abril, reguladora de las bases de régimen local · Legislación autonómica reguladora local (si existe	07- Cargos públicos

Figura 1: extracto de la imagen del RAT básico propuesto por la FEMP

Más adelante la idea es también relacionar este registro con las medidas de seguridad vinculadas a los riesgos tecnológicos, para poder disponer de cuadros de seguimiento del cumplimiento del RGPD que nos permitan anticiparnos a posibles situaciones de riesgo y, por tanto, alinear así el RGPD con las medidas establecidas en el Esquema Nacional de Seguridad (ENS).

III. LA NECESIDAD DE UNA POLÍTICA INTEGRAL DE PROTECCIÓN DE DATOS EN LAS ENTIDADES LOCALES

El RGPD en su artículo 24 establece como una obligación de responsabilidad proactiva del responsable del tratamiento, la necesidad de establecer las oportunas políticas de protección de datos, a fin de garantizar y poder demostrar que el tratamiento es conforme con el citado reglamento.

En la misma línea, el artículo 28 de la LOPDGDD, indica que, los responsables y encargados, teniendo en cuenta los elementos enumerados en los artículos 24 y 25 del RGPD, determinarán las medidas técnicas y organizativas apropiadas que deben aplicar a fin de garantizar y acreditar que el tratamiento es conforme con el citado reglamento, con la citada Ley orgánica, sus normas de desarrollo y la legislación sectorial aplicable.

De hecho, una de las funciones de los delegados y delegadas de protección de datos es precisamente, ex artículo 39.b) del RGPD, la de supervisar el cumplimiento de lo dispuesto en el RGPD, otras disposiciones de protección de datos de la UE o de los Estados miembros y de las políticas de protección de datos del responsable y del encargado del tratamiento.

El establecimiento de políticas como forma o medio de cumplimiento de la normativa de protección de datos tiene como finalidad dirigir y controlar la actividad de una organización siendo además estas políticas, un elemento clave del nuevo modelo de cumplimiento de la normativa sobre la base de la *gestión de riesgos* para los derechos y libertades de las personas físicas que anteriormente hemos mencionado.

En este escenario y sin perjuicio de las funciones propias del delegado o delegada de protección de datos, corresponde al órgano de gobierno de cada entidad local aprobar y establecer la llamada "política de protección de datos" del organismo como garantía de cumplimiento de la normativa de protección de datos y como medida de prevención para impedir tratamientos que vulneren los derechos y libertades fundamentales de las personas físicas en relación con el tratamiento de sus datos personales.

La aprobación de esta política de protección de datos constituye una facultad indelegable del órgano de gobierno de las entidades locales. En este sentido además, la diligencia debida en el cumplimiento de la normativa de protección de datos depende en gran medida del inequívoco compromiso y apoyo del órgano de gobierno de cada entidad local puesto que, el comportamiento y la implicación de dicho órgano, es clave para trasladar una cultura de cumplimiento al resto de la entidad.

Por el contrario, la ambigüedad o la indiferencia ante su aprobación puede llevar al personal de la entidad a entender que el incumplimiento de la normativa es un riesgo que la corporación puede asumir frente a las dificultades organizativas o técnicas en relación con la implantación de medidas para el cumplimiento de la normativa. Ello, porque debemos admitir que dar cumplimiento a la normativa de protección de datos supone llevar a cabo cambios organizativos, cambios técnicos en los sistemas e inversión en recursos.

En definitiva, si los principales responsables de la corporación no muestran su capacidad de liderazgo en la exigencia del cumplimiento de la normativa, difícilmente podrá admitirse que exista una verdadera cultura de respeto a los derechos y libertades de las personas físicas en relación con el tratamiento de datos personales por parte del resto del personal de la corporación.

Así, con la aprobación de una política de protección de datos **la corporación debe asumir un compromiso institucional y público de cumplir la normativa de protección de datos** reclamando a todo su personal el respeto de las medidas de protección de datos establecidas en el desarrollo de sus funciones y competencias.

En cuanto al contenido de la política de protección de datos, lo habitual será que ésta enuncie las obligaciones y los principios generales de protección de datos que debe cumplir la institución en congruencia con lo establecido en la normativa aplicable, siendo dichos principios y obligaciones posteriormente desarrollados por normas, instrucciones y procedimientos internos en la entidad local al amparo y en el marco de la política de protección de datos de la entidad.

En todo caso, veamos a continuación a grandes rasgos cuáles deberían ser estas obligaciones y principios a enunciar en la política de protección de datos de cada entidad local.

- La política de protección de datos debe hacer explícita la obligación de la entidad local de elaborar y publicar un registro de actividades de tratamiento así como de mantenerlo debidamente actualizado.

- Asimismo, la política de protección de datos debe identificar los datos de contacto del delegado o delegada de protección de datos y poner de manifiesto que su nombramiento ha sido comunicado a la autoridad de control correspondiente, donde igualmente estará publicada la dirección electrónica de contacto. En la política se hará evidente que dicho delegado o delegada cuenta con el respaldo de la corporación en el desempeño de las funciones que le atribuye el RGPD, en la disponibilidad de los recursos necesarios para el desempeño de dichas funciones y en el acceso a los datos personales y a las operaciones de tratamiento de la entidad.

- La política de protección de datos exigirá el cumplimiento del principio de transparencia y licitud del tratamiento de los datos personales de forma que cualquier actividad de tratamiento de datos personales llevada a cabo por la entidad local sea informada a las personas afectadas a través de la publicación de los correspondientes registros de actividad de tratamiento así como mediante la inserción de los avisos y textos legales en los documentos de recogida de datos, quedando prohibida cualquier recogida de datos y tratamiento posterior sin dar cumplimiento al citado principio y sin la existencia de una base jurídica lícita.

- Además, la política de protección de datos exigirá que el procedimiento de contratación de la entidad local esté adaptado a la normativa de protección de datos de manera que, aquellas licitaciones y contrataciones realizadas por la entidad (cualquiera que sea la cuantía) que requieran del tratamiento de datos personales, contengan las previsiones y medidas de protección establecidas en el RGPD para la contratación de terceros prestadores de servicios que tienen acceso y tratan datos personales por cuenta de la entidad local, teniendo en cuenta además, las limitaciones previstas en la normativa vigente para la contratación de contratistas ubicados en terceros países fuera del Espacio Económico Europeo.

- La política de protección de datos exigirá el compromiso del personal de la corporación con la seguridad y la confidencialidad de los datos personales de las personas afectadas por los tratamientos de datos personales así como la notificación inmediata de cualquier brecha de seguridad que pueda acontecer en relación con los citados datos.

- **Un elemento fundamental de la Política es el compromiso de la corporación con la atención y gestión de las solicitudes de ejercicio de derechos de las personas afectadas**, para lo cual se exigirá en la Política que la entidad local disponga de un procedimiento electrónico de tramitación de los derechos de protección de datos de las personas físicas, a través del cual éstas pueden solicitar el acceso, la rectificación, la supresión, la oposición, la limitación del tratamiento y la portabilidad de sus datos personales así como no ser sometida a una decisión basada exclusivamente en el tratamiento automatizado de sus datos personales y cuando proceda, retirar el consentimiento prestado a un tratamiento. El procedimiento además debe garantizar la atención por parte de la entidad local del ejercicio de los derechos en el debido plazo y forma.

- La Política mostrará el compromiso de la corporación de cooperar con las autoridades de control competentes en materia de protección de datos para proteger los derechos y las libertades de las personas interesadas en relación con el tratamiento de sus datos personales, atendiendo los requerimientos y solicitudes de información que dichas autoridades notifiquen a la entidad local y adoptando las medidas que, en su caso, las autoridades de control soliciten de la institución para garantizar o reponer en sus derechos y proteger los datos personales de las personas afectadas.

- La política de protección de datos pondrá de manifiesto el hecho de que la entidad local dispone de normas para la conservación y supresión de los datos contenidos en los tratamientos de datos personales bajo su responsabilidad teniendo en cuenta asimismo, cuando corresponda, el marco de la gestión de archivos y documentos a que está obligada la entidad, en virtud de las normas reguladoras del patrimonio histórico y sistema de archivos.

- La política de protección de datos incluirá un compromiso explícito de la corporación de llevar a cabo controles internos y auditorías periódicas emitiendo los correspondientes informes de control en los que se reflejan las irregularidades detectadas y el plan de acción para la mejora y corrección del cumplimiento, los cuales deberán ser entregados al órgano de gobierno de la entidad local.

- La política de protección de datos mostrará el firme compromiso de la entidad local de llevar a cabo actividades de concienciación en materia de protección de datos y garantizando además que todo el personal a su cargo pueda recibir la formación necesaria en esta materia.

- Y finalmente, a través de la política de protección de datos, la corporación asumirá su responsabilidad en cuanto al cumplimiento del RGPD y la LOPDGDD, así como de lo dispuesto en la propia política, adoptando medidas de responsabilidad proactiva para demostrar dicho cumplimiento, en particular, a través de medidas técnicas y organizativas adecuadas, incluidas otras políticas internas y procedimientos que desarrollen los distintos principios y obligaciones de protección de datos enunciados en la política de protección de datos de la entidad local.

Esta política, deberá ser publicada por la entidad local, de forma que, tanto la ciudadanía como el propio personal de la institución, tengan acceso y disponibilidad sobre la misma, constituyendo además dicha publicación, un acto de compromiso y transparencia de la corporación.

Expuesto todo lo anterior, no se entendería la política de protección de datos de la entidad local sin la coexistencia de ésta con un sistema de gestión y gobernanza de la protección de los datos personales diseñado especialmente para dar cumplimiento a la citada política y resto de normativa de protección de datos personales.

IV. UNA HERRAMIENTA PARA FACILITAR LA EVALUACIÓN Y EL AUTODIAGNÓSTICO

El ciclo de madurez en protección de datos personales en las Administraciones públicas se puede definir en cuatro etapas:

1) Transparencia en la gestión de los tratamientos de datos personales.

2) Garantía de los derechos de la ciudadanía en la materia.

3) Modelo de gobernanza para el desempeño de las obligaciones relativas a los responsables y encargados de tratamiento y su relación con el/la delegado/a de protección de datos.

4) **Gestión proactiva del cumplimiento normativo** en los tratamiento de datos, responsabilidad de la corporación.

Cada una de las etapas especificadas deberá acompañarse de las actividades de formación y difusión interna necesarias para garantizar su correcto despliegue en la corporación.

El entorno de las entidades locales es, sin duda el más heterogéneo dentro de las Administraciones públicas españolas, dado que reúne a más de 8.000 municipios que van desde las grandes capitales españolas hasta los municipios más pequeños de menos de 100 habitantes.

A fecha de 1 de enero de 2023, sólo 417 municipios superaban los 20.000 habitantes. En el resto de municipios de población inferior a los 20.000 habitantes es donde las Diputaciones provinciales y los Cabildos insulares, cumplen una labor de asistencia clave en muchos temas y, entre ellos, en la gestión de las obligaciones de la normativa en materia de protección de datos personales.

En este sentido, resultará de especial interés la compartición de experiencias entre Ayuntamientos de tipo medio por encima de los 20.000 habitantes y las entidades locales provinciales en su labor de asistencia a los municipios más pequeños.

Como ya hemos mencionado antes, el artículo 24.1 del RGPD especifica que "*el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el RGPD".*

También el art 28.1 de la LOPDGDD dentro de las obligaciones del responsable y del encargado del tratamiento especifica que éstos *"determinarán las medidas técnicas y organizativas apropiadas que deben aplicar a fin de garantizar y acreditar que el tratamiento es conforme con el RGPD, la LOPDGDD, sus normas de desarrollo y la legislación sectorial aplicable".*

Para conseguir lo regulado en dichos artículos la mayoría de los autores coinciden en la **necesidad de adoptar un programa de cumplimiento como base de un sistema de gestión de la protección de datos (SGPD)**.

Esto es especialmente recomendable en las Administraciones públicas, dada la obligación de éstas de nombrar delegado o delegada de protección de datos (DPD) y que según marca el artículo 39 del RGPD, la supervisión del cumplimiento en materia de protección de datos es una de las funciones encomendadas al DPD.

En el mercado existen grandes soluciones para la gestión de la protección de datos, pero habitualmente, dirigidas a grandes corporaciones, empresas multinacionales con variados sistemas normativos o con modelos de legitimación basados en el interés legítimo y/o consentimiento, que obligan a una gestión compleja de este último. Por otra parte, no siempre los costes de las herramientas o los servicios de terceros serían viables para el rango de ayuntamientos y corporaciones locales de tipo medio.

En este sentido, el ya citado Grupo de trabajo en protección de datos de la comisión de *"Sociedad de la Información, Innovación Tecnológica y Agenda Digital"* de la FEMP, además de elaborar un RAT tipo básico, se fijó el objetivo de elaborar un modelo que permitiera a los ayuntamientos de tamaño medio, superiores a los 20.000 habitantes, así como a las Diputaciones provinciales y Cabildos insulares, coordinadoras de esta gestión en los municipios menores de 20.000 habitantes, realizar una autoevaluación del nivel de cumplimiento en las nuevas normativas de protección de datos, adaptando las actuales herramientas publicadas por las Autoridades de Control españolas para los tratamientos habituales en estas entidades locales.

El modelo implementado no pretende sustituir un SGPD sino garantizar la disponibilidad de una herramienta de fácil adaptación y sin costes específicos, que permita cubrir de forma sencilla las principales obligaciones reflejadas en el ciclo de madurez ya comentado.

Además, con ello se da cumplimiento a las obligaciones de control y auditoría las cuales la AEPD ya ha manifestado que son necesarias cuando las medidas de cumplimiento adoptadas sufren cualquier cambio.

En este sentido, la FEMP ofrece una herramienta, de forma libre que ha sido desarrollada en Microsoft Excel asistida por macros en visual basic que permite las siguientes funcionalidades básicas:

a) Integración del registro básico de actividades de tratamiento para un ayuntamiento de tipo medio, permitiendo su mantenimiento y su correspondiente exportación en los formatos más habituales (pdf, ficheros ofimáticos), para su posterior publicación en la sede electrónica de la corporación o en la página web estipulada para ello.

b) Disponibilidad de un cuestionario para la verificación de cumplimiento normativo con los siguientes bloques:

- Disponibilidad de los datos necesarios para el cumplimiento del artículo 30 y la publicación del RAT.
- Cumplimiento de los principios regulados por la normativa en materia de protección de datos.
- Garantía de los derechos de la ciudadanía.
- Garantía de cumplimiento de las obligaciones del responsable del tratamiento.

- Evaluación de los criterios básicos de la seguridad de los datos.

c) Para cada uno de los controles relativos a los cinco bloques anteriores, la herramienta integra un sistema de evaluación de riesgos iniciales basada en las guías: *"Gestión del riesgo y evaluación de impacto en tratamientos de datos personales"* de la AEPD y la "*Guía pràctica sobre l'avaluació d'impacte relativa a la protecció de dades"* de la APDCAT.

d) Dispone de la posibilidad de revisión de los riesgos iniciales por parte del personal especializado, así como la conexión a un sistema de medidas mitigadoras de cada nivel de riesgo.

e) A efectos de *accountability*, incluye un pequeño gestor documental, que permite relacionar documentos demostrativos o evidencias de cumplimiento y relacionarlos con el control de cumplimiento al que aplican.

No se pretende entregar un modelo cerrado, sino que se trata de un modelo abierto que pueda incentivar su adaptación a modelos específicos y crear un espíritu de comunidad entre estos ayuntamientos con problemáticas similares.

Cada una de las preguntas del cuestionario tiene la correspondiente ayuda que puede ser modificada para los propósitos específicos de cada corporación. Estos textos de ayuda no es obligatorio seguirlos en su totalidad, sino que representan un apoyo a la persona usuaria para decidir el sentido de las respuestas. Algunas ayudas pueden estar en blanco porque no se consideran necesarias por la evidencia de la pregunta ya auto explicativa. También incluye un manual técnico y de usuario de la misma.

Desde el punto de vista técnico, ha sido desarrollada en Microsoft Office 2010 y revisada para su compatibilidad con Microsoft Office 365.

Permite un uso básico sin más requerimientos que un nivel correcto de Microsoft Excel, pero para las personas usuarias avanzadas en programación permite la parametrización de múltiples factores como la modificación de los controles, sus interdependencias funcionales o la modificación de sus riesgos asociados.

Es importante tener en cuenta que todas las celdas son modificables y el acceso a la codificación Visual Basic de las macros también, lo que supone por un lado que las personas usuarias lo puedan re-parametrizar y adaptarlo en gran medida a las necesidades de cada instalación sin necesidad de añadir ninguna programación o macro. Sin embargo, también hay que ser consciente de que muchas celdas pueden ser erróneamente modificadas si no se conoce exactamente la disposición y funciones que tengan asignadas, sus fórmulas asociadas y la diferenciación entre aquellas de "valor libre" (sin repercusión en el funcionamiento del libro) frente a las estructurales.

Las funcionalidades específicas de la herramienta se engloban en un menú flotante, a fin de independizarlas de los menús habituales de Microsoft Excel.

El primer objetivo, la generación del RAT, se realiza desde la opción correspondiente del menú tal y como se aprecia en la siguiente figura.

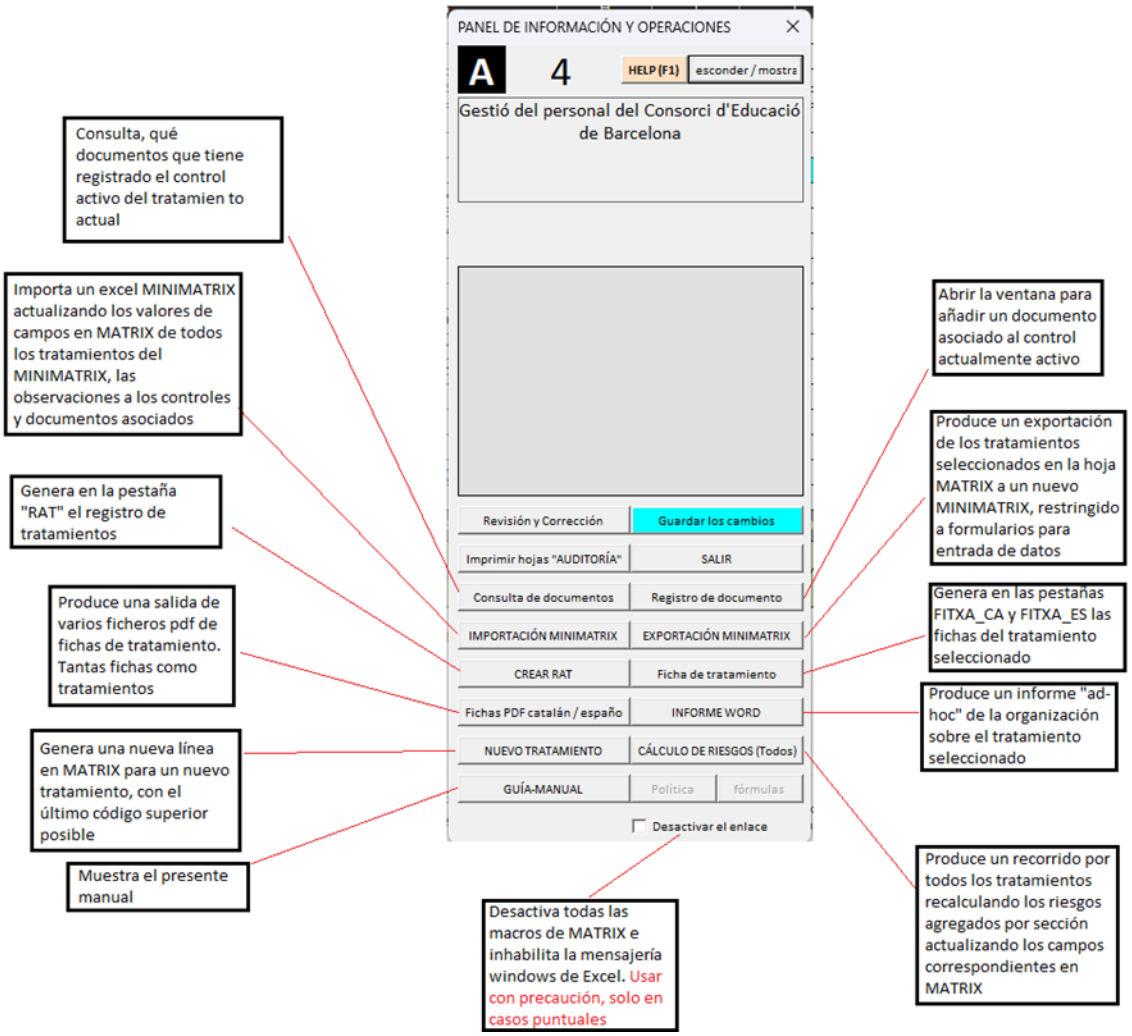


Figura 2: Funciones del menú flotante - generación RAT

La herramienta permite una visión integrada de todos los tratamientos y la generación del correspondiente RAT, así como una visión de los riesgos inherentes a cada tratamiento concreto, pudiendo generar un informe a modo de ficha de riesgos de cumplimiento para cualquier tratamiento.

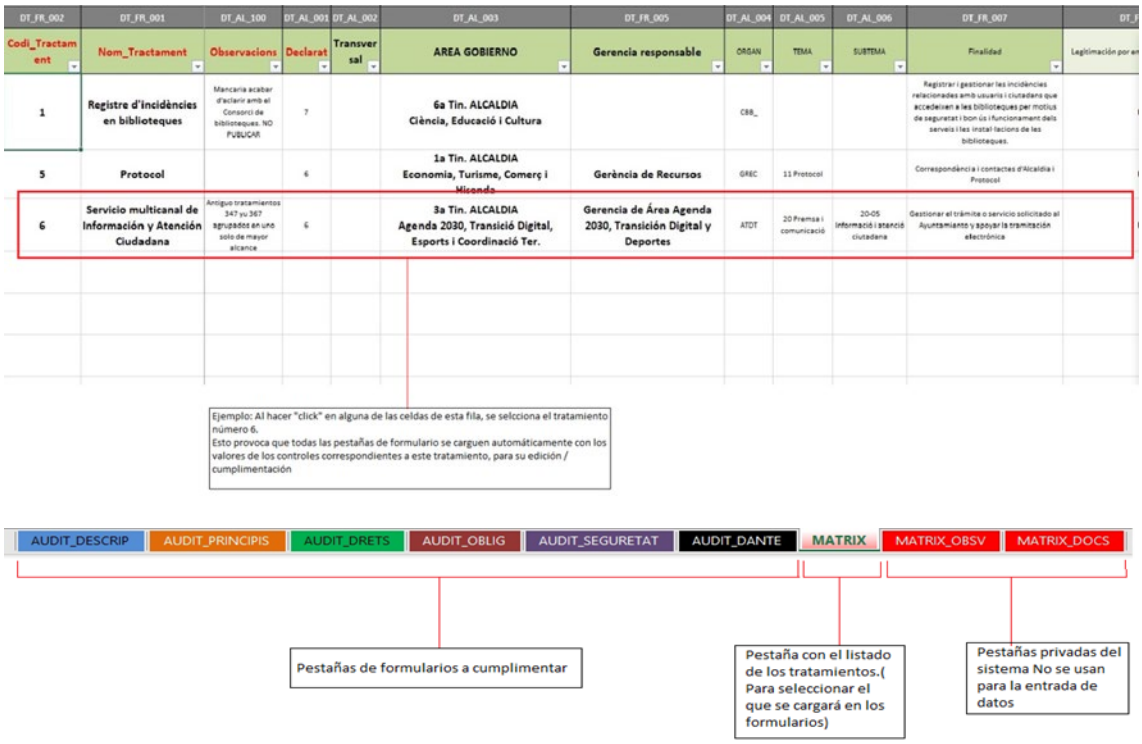


Figura3: selección de un tratamiento para acceder a su ficha de cumplimiento

Los controles están distribuidos en 5 bloques de cumplimiento (pestañas: AUDIT_DESCRIP hasta AUDIT_SEGURETAT) y agrupados en 35 apartados de cumplimiento.

El modelo de evaluación de riesgos calcula el riesgo individual inherente a cada control en función de su respuesta de acuerdo a su calificación en la guía *"Gestión del riesgo y evaluación de impacto en tratamientos de datos personales" de la AEPD*. Según dicha guía, el nivel de riesgo se cataloga en 4 niveles: "*bajo – medio – alto – muy alto"*.

En función de las respuestas, el formulario calcula el nivel de riesgo inicial para cada pregunta control y muestra también el riesgo máximo acumulado en cada uno de los 35 apartados de cumplimiento de la herramienta.

La siguiente figura muestra un ejemplo:

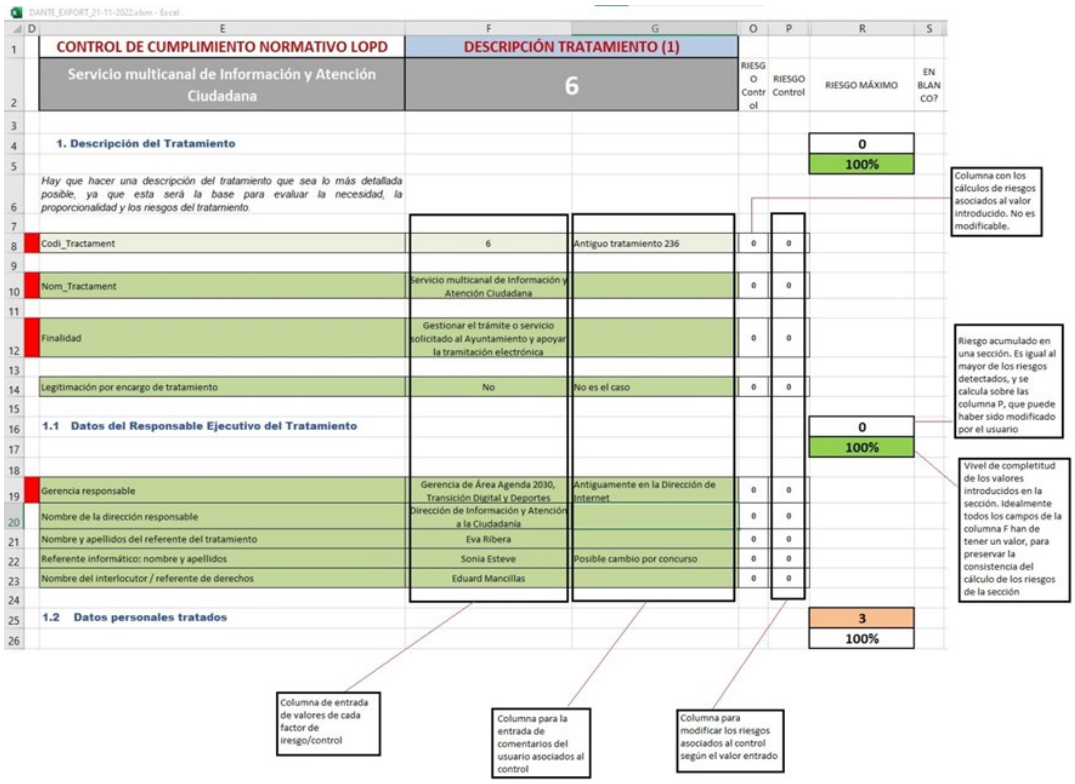


Figura 4: ejemplo de controles, apartados de cumplimiento y riesgos asociados

Los riesgos iniciales, pueden ser revisados por el personal especializado y ser modificados manualmente en función de circunstancias especiales del tratamiento en la corporación. En estos casos se deberán anotar las circunstancias que motivan la corrección del riesgo inicial calculado.

Será en todo caso el riesgo final modificado el que se utilice para la adopción de posibles medidas correctoras que, sin ser el objeto inicial de la herramienta, estaría preparada para asociar dicha tabla al módulo inicial.

Por último, incluye una función documental que permite asociar documentos a cualquier control del cuestionario, bien creando un repositorio integrado específico o integrando un link al documento correspondiente. La figura siguiente muestra el formulario de esta funcionalidad:

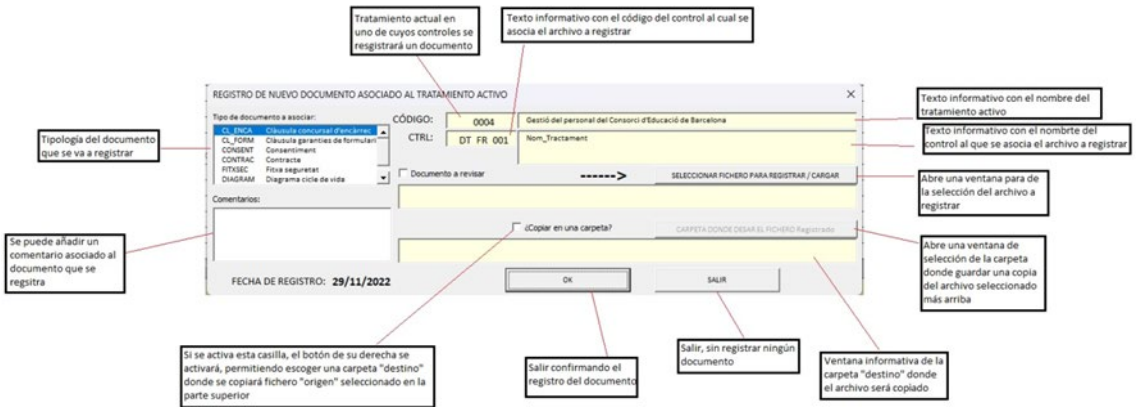


Figura 5: ilustrativa de la gestión documental ligada a un control

También integra un historial de movimientos que permitiría un análisis específico de la evolución (no incluido en la herramienta).

V. CONCLUSIONES

Cinco años después de la puesta en marcha efectiva del RGPD en 2018, las Administraciones públicas deben dar ejemplo de cumplimiento en esta materia reguladora de un derecho fundamental y que se erigirá en una cuestión clave en la transformación digital en la que todos estamos inmersos.

La actual transformación digital de los principales procesos en los que nos vemos envueltos todos los sectores (tanto público como privado) así como la ciudadanía, ha generado una economía global específica en el mundo de los datos digitales y que en el plano de los datos personales se encuentra seriamente amenazada. La asimetría normativa a nivel global, no se corresponde con la gestión globalizada de los datos y sus amenazas (ciberataques).

Es en este contexto, en el que la FEMP pone en marcha esta iniciativa que pretende ayudar a los ayuntamientos, en especial los de tipo medio, no sólo a cumplir sus obligaciones básicas en cuanto a la normativa de protección de datos, sino a **reforzar la cultura interna de protección de datos personales y hacer de la política de minimización de riesgos desde el diseño y por defecto, una constante de gestión**.

El modelo presentado y compuesto de un Registro de Actividades básicas de tratamiento para una entidad local (que incluye 60 tratamientos adaptados a las competencias de estas entidades locales) y un modelo de política de privacidad municipal tipo, sobre el que se desarrolla la herramienta abierta y adaptable de autoevaluación, pretende acompañar ese proceso, facilitando la evaluación de los riesgos normativos y técnicos en un entorno dirigido a las competencias municipales y que aunque nunca podrá hacer desaparecer por completo los riesgos para la privacidad, puede resultar un esfuerzo proporcionado para este tipo de entidades locales, en el camino del cumplimento de la normativa aplicable.

VI. BIBLIOGRAFÍA

CAMPOS ACUÑA, C. (Coord.). (2018) *Aplicación práctica y adaptación de la protección de datos en el ámbito local*, capítulo 7, Lluís Sanz Marco, Wolters Kluwer.

Jiménez Asensio, R. (2019). *Introducción al nuevo marco normativo de la protección de datos personales en el sector público*. Oñati: IVAP.

Jiménez Asensio, R. y Moro Cordero, A. (2018). *Manual-guía sobre impactos del Reglamento (UE) de protección de datos en los entes locales*. Barcelona: FMC y ACM.

Moro Cordero, M.A. (2020). *La nueva cultura de gestión de los datos personales y la incorporación de tecnologías disruptivas.* Revista La Ley Privacidad - Número 4 – Abril-Junio 2020. Madrid: Wolters Kluwer.

Moro Cordero, M.A. (Coord*.)*. (2019). *Especial Protección de Datos. La privacidad al servicio de la ciudadanía.* El Consultor de los Ayuntamientos. Madrid: Wolters Kluwer.

Povedano Alonso, D. (Coord.). (2019). *Guía para la adaptación de la protección de datos en las entidades locales.* El Consultor de los Ayuntamientos. Madrid: Wolters Kluwer.

Subirana de la Cruz, S. y Fortuny Cendra, M. (Coords.). (2020). *Compliance en el sector público.* Cizur Menor (Navarra): Aranzadi-Thomson Reuters.

Agencia Española de Protección de Datos (8/02/2023). *Cuándo hay que revisar las medidas de protección de datos*. Blog de la AEPD.