EL DELEGADO/A DE PROTECCIÓN DE DATOS Y LA GOBERNANZA DE LA PRIVACIDAD EN PEQUEÑOS MUNICIPIOS. EL PAPEL DE LAS DIPUTACIONES PROVINCIALES

Pilar VÉLEZ CALERO

Área de Concertación Municipal . Diputación de Huelva

Trabajo de evaluación presentado para el Curso: Transparencia y Protección de Datos Personales en las Administraciones Locales. CEMCI.

SUMARIO:

1. INTRODUCCIÓN

Con la aprobación del 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 (en adelante RGPD), el legislador europeo establece las normas relativas a la libre circulación de los datos personales dentro de la UE, garantizando al mismo tiempo un elevado nivel de protección de los datos personales…" (Considerando 6º del RGPD). Y lo hace, mediante la implantación de un nuevo paradigma que deja atrás un modelo reactivo para dar paso a uno proactivo (responsabilidad proactiva del artículo 5.2 del RGPD), que se focaliza en la gestión del riesgo.

Se traslada a la Protección de Datos la técnica del "compliance" o cumplimiento normativo, dimensión preventiva o anticipadora que nos lleva a estar siempre vigilantes, a través de una serie de medidas técnicas y organizativas, entre las que destacan el incremento de las medidas de seguridad del artículo 32 del RGDP, el establecimiento de protocolos para hacer frente a posibles violaciones de seguridad y la consiguiente notificación tanto a las autoridades de control como a los afectados (artículos. 33 y 34 del RGDP), la evaluación de los posibles impactos del tratamiento de los datos (artículo 35 del RGDP,) las auditorias de protección de datos, o la designación de un delegado/a de protección de datos (en adelante DPD). En estos últimos aspectos, el RGPD fortalece el

papel de las autoridades de control tanto a nivel externo, a través de la Agencia Española de Protección de Datos (en adelante AEPD) y las autoridades de control autonómicas en el caso de España, como a nivel interno dentro de la propia organización a través de la ahora obligatoria[1] figura del DPD que asume el doble papel de asesor y auditor interno.

En este escenario, las Administraciones Públicas, que por su propia naturaleza tratan grandes cantidades de datos de personas físicas, deben poder garantizar los derechos de estas y entre ellos, el Derecho Fundamental a la protección de datos personales, del artículo 18.4 de la CE: *"4. La Ley limitará el uso de la informática para garantizar el derecho al honor y a la intimidad…"*[2]

Es el propio RGPD el que en su artículo 37.1 obliga a las Entidades Públicas a nombrar un delegado/a de protección de datos, obligación que puede resultar de difícil cumplimiento para los municipios de menor tamaño dada la escasez de recursos humanos y económicos de que estas entidades suelen disponer.

Si bien es cierto que las personas titulares de las secretarías municipales parecen ser las candidatas perfectas para ocupar la figura del delegado/a de protección de datos, dado su perfil jurídico, su conocimiento del funcionamiento de toda la institución y su posición dentro de la estructura municipal, y puesto que Ley Orgánica 3/2018 de 5 de diciembre de Protección de Datos Personales y Garantías de Derechos Digitales (en adelante LOPDGDD) en su artículo 34.5 permite establecer la dedicación del delegado/a a tiempo parcial, en función del volumen de los tratamientos, las categorías especiales de los datos tratados o de los riesgos para los derechos o libertades de los interesados, parece que designar al secretario o secretaria municipal como DPD es una opción más que razonable

Sin embargo, situándonos en la realidad de las corporaciones locales y en la de este cuerpo que en los municipios de menor población suelen ostentar también la intervención municipal, el ingente paquete de medidas a las que las personas titulares de las secretarías municipales, deben dar cumplimento para adaptar la corporación a las nuevas realidades jurídicas, la responsabilidad proactiva introducida por la normativa de Protección de Datos Personales que requiere de la ya mencionada permanente vigilancia, hace difícil que este cuerpo pueda encargarse también de la tareas encomendadas al delegado/a de protección de datos (y que veremos más adelante). Todo ello sin obviar que la figura del DPD requiere de una "posición" en la que no converjan conflictos de intereses, posición que según nuestra opinión, no siempre será posible en el caso de quien ocupa la secretaría municipal.

---

1 La Figura del DPD no es una novedad en la normativa europea en materia de protección de datos, en cuanto que ya se regulaba en la derogada Directiva 95/46/CE , que en su artículo 18.2 permitía a los Estados miembros legislar, o no, sobre el DPD y por la que se le atribuían funciones de control interno así como llevar el registro de los tratamientos efectuados por el responsable. En España, no se había regulado esta figura sin embargo, en Alemania por ejemplo era obligatoria. El nuevo RGPD pone fin a esta asimetría entre Estados miembros, regulando una serie de supuestos en los que el nombramiento de la figura del DPD es de obligado cumplimiento para todos los EM .

2 El Tribunal Constitucional ha reconocido el derecho a la protección de datos como un derecho fundamental en sí mismo y no como un derecho derivado del derecho a la intimidad

Es en este punto dónde las alcaldías de los municipios de pequeño tamaño miran a las diputaciones provinciales en busca del auxilio que, en base al artículo 36 de la Ley 7/1985 de 2 de abril Reguladora de las Bases del Régimen Local, deben prestar estas entidades supramunicipales para asistir a los municipios de menor capacidad económica y de gestión, reforzando sus servicios de asistencia técnica.

Concretamente el artículo 36, en la letra b) de su número 1, atribuye a las diputaciones *"La asistencia y cooperación jurídica, económica y técnica a los Municipios, especialmente los de menor capacidad económica y de gestión"*. El apoyo para una correcta aplicación de la normativa de protección de datos, ejerciendo las tareas que se atribuyen legalmente a los delegados/as de protección de datos, entra de lleno en esa cooperación técnica.

Esta obligación viene reforzada en los artículos 11 a 14 de la Ley 5/2010, de 11 de junio, de Autonomía Local de Andalucía, que además de insistir en esa asistencia y cooperación técnica, habla de implantación de la tecnología de la información y comunicaciones, y de formación del personal y de los representantes locales.

A continuación haremos un breve recorrido por una propuesta de procedimiento de nombramiento de delegado/a de protección de datos por parte de una diputación provincial para prestar servicios en varios municipios de pequeño tamaño y con reducida capacidad económica y de gestión, así como por sus funciones, no sin antes mencionar algunas de las normas que complementan al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos y Garantías de Derechos Digitales y que deben tenerse en cuenta en el día a día de los ayuntamientos para garantizar el derecho a la protección de datos personales a la ciudadanía.

2. LEGISLACIÓN APLICABLE

Con 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 (Reglamento general de protección de datos, RGPD), se da luz verde al nuevo marco jurídico en materia de protección de datos personales a fin de garantizar y homogeneizar este derecho en todos los Estados miembros así como a facilitar la libre circulación de datos en la Unión Europea.

Y lo hacen, como vemos, a través de un Reglamento, medida que no necesita transposición por parte de los Estados miembros ya que es de aplicación directa. Esta norma preveía un periodo de 2 años para adaptarse a su cumplimiento. Meses después de estos dos años, España, siguiendo la senda del RGPD, aprueba su Ley Orgánica 3/2018 de 5 de diciembre de Protección de Datos Personales y Garantías de derechos digitales (LPDGDD), para regular aquellos aspectos en los que el Reglamento deja vía libre a los Estados miembros (como por ejemplo la edad a la que los menores pueden prestar el consentimiento). La Ley Española hace continuas "llamadas" al RGPD así como

remisiones a la normativa sectorial, en la que se regulan determinados aspectos en el funcionamiento de los entes locales.

Por dejar constancia del alcance del nuevo marco jurídico en materia de PDP y sin intención de hacer un recorrido exhaustivo de la normativa a tener en cuenta para garantizar el derecho fundamental a la protección de datos de la ciudadanía por parte de las Administraciones Locales, creemos importante hacer indicación de aquellas de mayor impacto que o bien han sido directamente modificadas por la LOPDGDD ,o bien se ven especialmente afectadas por el ejercicio de los derechos que recoge su Título X: Garantías de Derechos Digitales. (artículos 79 a 97):

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE
- Ley Orgánica 3/2018 de 5 de diciembre de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD)
- Real Decreto-ley 14/2019 de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones (que introduce los mandatos de la normativa de protección de datos en otras normas sectoriales)
- Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración electrónica. Que es llamado por la Disposición Adicional Primera a incorporar medidas de seguridad conforme a lo establecido en el artículo 32 del RGPD
- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica (Véase el considerado 68 del RGPD , relativo a la interoperabilidad, la portabilidad y la base jurídica del tratamiento de datos)
- Ley 39/2015 de 1 de octubre de Procedimiento Administrativo Común de las Administraciones Púbicas. *(Modificado en su artículo 28.2 y 28.3 por la Disposición Final Duodécima de la LOPDGDD y llamando a su artículo 44 por la Disposición Adicional Séptima a la adecuada identificación de los interesados en la publicación de notificaciones por medios de anuncios. El Real Decreto -ley 14/2019 introduce asimismo cambios en los artículos 9 y 10 para someter esta Ley al RGPD)*

- Ley 40/2015 de 1 de octubre de Régimen Jurídico del Sector Público (modificado en su artículo 155, para actualizar las Transmisiones de datos entre Administraciones Públicas conforme al RGPD e incorporado el artículo 46-bis, ambos vía Real Decreto -ley 14/2019)
- Ley 9/2017 de 8 de noviembre de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014. (Que se ha visto modificada en sus artículos 35.1d) , 39.2.h), 116.1, 122.2, 202.1, y 215.4 por Real Decreto-ley 14/2019 de 31 de octubre para incorporar los mandatos del RGPD)
- Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público (EBEP). (Modificado en su artículo14 por la disposición adicional décimo cuarta de la LOPDGDD al adicionar el artículo14.j-bis)
- Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores. (Incorpora el artículo 20 bis por la Disposición Final Decimotercera de la LOPDGDD)
- Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa (modificada en sus artículos 10, 11 ,12 y 122 por la Disposición Final Sexta de LPDGDD).
- Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno. (Modificada en su artículo 15.1 e incorporado el artículo 6 bis, por la Disposición Adicional Segunda de la Ley Orgánica 3/2018, de 5 de diciembre de Protección de Datos Personales y garantías de derechos digitales).
- Ley Orgánica 2/2006, de 3 de mayo, de Educación (que incorpora la letra I en su artículo 2.1, por la Disposición Adicional Décima Ley Orgánica 3/2018, de 5 de diciembre).
- Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General.(Modificada en su artículo 39.3 e incorporado el artículo 58 bis por la Disposición Final Tercera de la Ley Orgánica 3/2018 de 5 de diciembre.)

También habrá de estarse a lo dispuesto en la normativa en materia de Régimen Local, Haciendas Locales, Reglamento de Medio Ambiente, Tributos, Tráfico, Urbanismo, Transporte público, Salud, Seguridad Social, Policía Local, Padrón, Vídeo Vigilancia, Seguridad.....etc. a la hora de ponderar la prevalencia del derecho a la protección de datos y la garantía de derechos digitales respecto de otros derechos.

3. LOS PERFILES EN LA PROTECCIÓN DE DATOS

Tres son las principales figuras que deben tenerse en cuenta a la hora de considerar la responsabilidad en materia de protección de datos personales en las entidades locales

Responsable :

Persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento. En nuestro caso, el Responsable sería el ayuntamiento. No la alcaldía, lo que no significa que como responsable de la entidad no deba garantizar que se provea de los medios técnicos y organizativos para dar cumplimiento a la normativa

Encargado:

Persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento (artículo 33 LOPDGDD) . En el caso de los ayuntamientos , entre los encargados del tratamiento podemos encontrar personal del propio ayuntamiento, como por ejemplo la persona que gestiona o accede al padrón municipal (la consulta de datos es un tratamiento de datos y en el caso del padrón municipal se trata de datos confidenciales). Podemos también citar a las diputaciones provinciales como encargadas del tratamiento de datos de los municipios, por ejemplo en materia de servicios sociales lo que supone el tratamiento de datos especialmente protegidos, o los servicios delegados en temas de recaudación. Serán también encargados de tratamiento las Mutuas de Salud, las empresas de formación, o cualquier prestador de servicio que tenga subcontratado el ayuntamiento y que necesite tratar datos de carácter personal.

Delegado/a de Protección de Datos:

Persona física o jurídica, empleado en plantilla o mediante contrato de servicio, que informa y asesora al Responsable, al Encargado y a otros empleados sobre las obligaciones del RGPD y supervisa su cumplimiento, cooperando y actuando como punto de contacto con las Autoridades de Control (artículos 37 a 39 RGPD) . Una entidad puede tener más de un DPD, atendiendo a su tamaño y organización. Por ejemplo, la Junta de Andalucía tiene distintos DPD con ámbito competencial diferenciado por consejerías e incluso por servicios. En un pequeño ayuntamiento no procedería el nombramiento de más de un DPD.

4. RECOMENDACIONES PARA REGULAR LA FIGURA DE DELEGADO/A DE PROTECCIÓN DE DATOS NOMBRADO POR UNA DIPUTACIÓN PROVINCIAL PARA PRESTAR SERVICIO EN VARIOS AYUNTAMIENTOS.

Para dar cumplimento a la nueva normativa, los ayuntamientos deben seguir un procedimiento que se inicia con el nombramiento del DPD. Cuando no le sea posible nombrar una persona de su plantilla o contratar el servicio de manera externa, pueden solicitar el apoyo de las diputaciones provinciales para que sean estas quienes nombren a su costa, un delegado/a de protección de datos para el ente local.

Cabe recordar aquí que la figura del DPD es obligatoria para todas las AAPP y que el RGPD prevé que pueda nombrarse un mismo DPD para varias autoridades u organismos público atendiendo a su tamaño y su estructura organizativa.

A continuación centramos nuestro trabajo en esta figura y en el proceso de su nombramiento paso a paso.

Planteemos por ejemplo la siguiente hipótesis: varios municipios de pequeño tamaño solicitan a la Diputación Provincial que nombre DPD para sus corporaciones. Desde la diputación en cuestión, entendemos que deben tomarse las siguientes medidas:

1. Identificar las unidades en que se habrá de "integrar" el DPD dentro de cada ayuntamiento y en la propia Diputación.

2. Aclarar su posición en la estructura administrativa y los mecanismos para asegurar que reúne los requisitos de cualificación y competencia establecidos por el RGPD

3. Definir su configuración para asegurar su criterio independiente y en ausencia de conflictos de intereses

4. Seleccionar a la persona que ocupara el puesto de DPD teniendo en cuenta que**:**

- No se exige que deba ser un jurista, pero sí que cuente con ese conocimiento en materia de protección de datos
- El DPD podrá ser interno o externo, persona física o persona jurídica especializada en esta materia . Desde nuestro punto de vista la opción menos deseable, aunque permitida por la normativa, sería contratar con una empresa externa la figura del delegado/a de protección de datos ya que, en nuestra opinión, se interferiría con uno de los principios que sostiene a esta figura; la independencia. Si la continuidad del contrato del servicio del DPD depende de lo rígido o flexible que este sea con la normativa, es posible que se apueste por la flexibilidad en vez de por la vigilancia y la proactividad. Por otro lado sería más difícil encontrar una empresa externa que conozca el funcionamiento de una entidad local mejor que el personal funcionario, sin obviar que la persona que ostente la responsabilidad de DPD tendrá acceso a toda la información de la

entidad, lo que obliga forzosamente a firmar acuerdos de confidencialidad que deben perdurar más allá de la vigencia del contrato de prestación del servicio de delegado/a de protección de datos. Tampoco es baladí la cuestión de la "libre competencia" ya que la empresa contratada para proveer al ente local de un DPD, tendría acceso a cualquier información de la entidad lo que puede suponer, acceso a información privilegiada de cara a otros posibles contratos con diferentes objetos. Entendemos por tanto que el papel de las empresas externas supondrá para el DPD un gran apoyo en materia de asesoramiento, apoyo legal y tecnológico pero sin ese acceso universal a la información que requiere la figura del DPD. Apostamos por tanto, por un DPD que forme parte de la plantilla de la diputación en cuestión, que podría, eso sí, tener el apoyo de un asesor externo que sea DPD certificado, pero sin ya sin el acceso a esa información privilegiada.

- La AEPD ha desarrollado un Esquema de certificación de DPD, que si bien no es obligatorio para ejercer como DPD y se puede ejercer la profesión sin estar certificado bajo éste o cualquier otro esquema, aquel permite certificar que los DPD reúnen la cualificación profesional y los conocimientos requeridos para ejercer la profesión. Creemos que dada la posición del DPD, sería más conveniente que la persona designada se certificase conforme al Esquema de Certificación que puede descargase en: https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/delegado-de-proteccion-de-datos/certificacion

5. Nombrar al DPD por parte de la diputación provincial en respuesta a la petición formal por parte del ayuntamiento. Recomendamos que se firme un convenio entre las partes o bien que la alcaldía firme el acuerdo de nombramiento, lo que indicará su aceptación del DPD que ha sido nombrado. (Cualquier acto administrativo sería valido) – Para una mejor gestión de los nombramientos y su seguimiento en el futuro, sería bueno un nombramiento por cada Ayuntamiento. Convendría firmar un acuerdo en el que se recordase tanto el artículo 38.1 del RGPD que establece que el responsable y el encargado del tratamiento garantizarán que el delegado/a de protección de datos participe de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales como que recoja también un acuerdo de confidencialidad de los DPD.

6. Crear una dirección de correo electrónico tipo: dpd@ayto.es

Los artículos 13.1.b y el 14.1.b del RGPD recogen que la información que debe facilitarse a los interesados incluye: "los datos de contacto del delegado/a de protección de datos" .

7. Comunicar la designación a las autoridades de control (artículo 37.7 del RGPD) (en caso de municipios andaluces el Consejo de Transparencia y Protección de datos de Andalucía o a la Agencia Española de Protección de datos en aquellas Comunidades Autónomas donde no exista Autoridad de Control Autonómica) en el plazo de 10 días hábiles desde su nombramiento (artículo 34.3 de la LOPDGDD). Cabe señalar aquí que el artículo 74.p de la LOPDGDD considera como infracción leve *" No publicar los datos de contacto del delegado de protección de datos, o no comunicarlos a la autoridad de protección de datos, cuando su nombramiento sea exigible de acuerdo con el artículo 37 del Reglamento (UE) 2016/679 y el artículo 34 de esta ley orgánica."*

8. Notificar su nombramiento al personal del ayuntamiento: el nombramiento del DPD debe ser notificado a todo el personal ya que a la hora de realizar sus labores de asesoramiento y supervisión del cumplimiento puede ser necesario requerir información a las áreas y servicios que realizan tratamientos de datos personales.

9. Publicar la dirección de correo electrónico del DPD (Ej.dpd@ayto.es) en la web del ayuntamiento. El artículo 37.7 del RGPD recoge: "El responsable o el encargado del tratamiento publicarán los datos de contacto del delegado/a de protección de datos y los comunicarán a la autoridad de control."

10. Recordar que posteriormente la dirección dpd@ayto.es debe ser incorporada en todas las cláusulas de información y en la política de privacidad justo a continuación de los datos del responsable del tratamiento. Aunque atendiendo al artículo 11 de la LOPDGDD esa información no requiere ir en la primera capa de información, recomendamos su inclusión para que a primera vista el interesado conozca de la existencia de un DPD y sus datos de contacto.

5. FUNCIONES DEL DELEGADO/A DE PROTECCIÓN DE DATOS:

El RGPD establece en su artículo 39, que el DPD tendrá como mínimo las siguientes funciones:

- Informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del presente Reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros

- Supervisar el cumplimiento de lo dispuesto en el propio Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes

- Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35 del RGPD

- Cooperar con la autoridad de control

- Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36 del RGPD, y realizar consultas, en su caso, sobre cualquier otro asunto.

El **Esquema de Certificación** del DPD de la Agencia Española de Protección de Datos y la Entidad Nacional de Acreditación (ENAC), amplía el detalle de estás funciones en los siguientes términos :

1. Cumplimiento de principios relativos al tratamiento, como los de limitación de finalidad, minimización o exactitud de los datos.

2. Identificación de las bases jurídicas de los tratamientos.

3. Valoración de compatibilidad de finalidades distintas de las que originaron la recogida inicial de los datos.

4. Identificación de la existencia de normativa sectorial que pueda determinar condiciones de tratamiento específicas distintas de las establecidas por la normativa general de protección de datos.

5. Diseño e implantación de medidas de información a los afectados por los tratamientos de datos.

6. Establecimiento de mecanismos de recepción y gestión de las solicitudes de ejercicio de derechos por parte de los interesados.

7. Valoración de las solicitudes de ejercicio de derechos por parte de los interesados

8. Asesoramiento en la contratación de encargados de tratamiento, incluido el contenido de los contratos o actos jurídicos que regulen la relación responsable- encargado.

9. Identificación de los instrumentos de transferencia internacional de datos adecuados a las necesidades y características de la organización y de las razones que justifiquen la transferencia.

10. Diseño e implantación de políticas de protección de datos.

11. Auditoría de protección de datos.

12. Establecimiento y gestión de los registros de actividades de tratamiento.

13. Análisis de riesgo de los tratamientos realizados.

14. Implantación de las medidas de protección de datos desde el diseño y protección de datos por defecto adecuadas a los riesgos y naturaleza de los tratamientos.

15. Implantación de las medidas de seguridad adecuadas a los riesgos y naturaleza de los tratamientos.

16. Establecimiento de procedimientos de gestión de violaciones de seguridad de los datos, incluida la evaluación del riesgo para los derechos y libertades de los afectados y los procedimientos de notificación a las autoridades de supervisión y a los afectados.

17. Determinación de la necesidad de realización de evaluaciones de impacto sobre la protección de datos.

18. Realización de evaluaciones de impacto sobre la protección de datos.

19. Relaciones con las autoridades de supervisión.

20. Implantación de programas de formación y sensibilización del personal en materia de protección de datos.

Por su parte, las Directrices del GT29 (Grupo de Trabajo del Artículo 29) sobre DPD parten de la base que este puede tener un papel relevante en la realización de Evaluaciones de impacto en protección de datos. Por ello proponen que se le solicite asesoramiento en las siguientes cuestiones:

1. Si se debe llevar a cabo o no una evaluación de impacto de la protección de datos

2. Qué metodología debe seguirse al efectuar una evaluación de impacto de la protección de datos

3. Si se debe llevar a cabo la evaluación de impacto de la protección de datos con recursos propios o con contratación externa

4. Qué salvaguardas (incluidas medidas técnicas y organizativas) aplicar para mitigar cualquier riesgo para los derechos e intereses de los afectados

5. Si se ha llevado a cabo correctamente o no la evaluación de impacto de la protección de datos y si sus conclusiones (si seguir adelante o no con el tratamiento y qué salvaguardas aplicar) son conformes con el RGPD.

6. Si el responsable del tratamiento está en desacuerdo con el consejo expresado por el DPD, la documentación de la evaluación de impacto de la protección de datos deberá justificar específicamente por escrito por qué el consejo no se ha tenido en cuenta.

Si ha llegado hasta aquí, ¡enhorabuena! ha dado el primer paso para el cumplimiento de la normativa en materia de protección de datos: Nombrar el delegado/a de protección de datos, ubicarlo en la estructura de la corporación y atribuirle las

funciones que le permitirán ir cumpliendo los objetivos que acerquen a la corporación al cumplimento de la normativa.

Continua el camino, ahora de la mano del DPD; con el resto de las actuaciones que nos marca la normativa; la creación del Registro interno de actividades y su publicación en la web municipal (el RAT) , la identificación de los principios sobre los que se fundamenta el tratamiento realizado (la legitimación del tratamiento), la revisión de la validez de los tratamientos basados en el consentimiento , dado que en la nueva normativa ya no es válido el consentimiento tácito sino expreso, el cumplimiento del principio de transparencia; la identificación de los contratos concertados que impliquen tratamiento de datos para adaptarlos en su caso al RGPD; la implementación de los circuitos para atender el ejercicio de derechos por parte de los ciudadanos que supondrá por ejemplo la redefinición de los formularios en los que se recogen datos personales de forma que aparezcan en ellos los nuevos elementos (como el contacto del DPD) y los nuevos derechos (como el de portabilidad), la realización de evaluaciones de impacto sobre los tratamientos realizados en los que se aprecien riesgos; la revisión constante de las medidas de seguridad implantadas; La cooperación con la autoridad de control y guardar las evidencias de todo lo anterior, es decir estar en disposición de facilitar, en cualquier momento, evidencias del cumplimiento del Reglamento.

Vemos que la tarea no es simple y que requerirá de toda la corporación para alcanzar los objetivos, pero es sin duda un reto que merece la pena afrontar.