EL PAPEL DEL OFICIAL DE PRIVACIDAD O DE PROTECCIÓN DE DATOS EN EL CUMPLIMIENTO DE LA NORMATIVA DE PROTECCIÓN DE DATOS

1. Introducción

La designación, de uno o varios oficiales de privacidad o de protección de datos, con adecuada cualificación, recursos y competencias suficientes para ejercer sus funciones de supervisión, se considera una medida muy adecuada de cara a promover el mejor cumplimiento de la normativa sobre protección de datos, tal y como se establece en la Directiva 95/46/CE de protección de datos.

En este sentido, los Estándares Internacionales sobre Protección de Datos Personales y Privacidad aprobados en la 31ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, celebrada en Madrid en noviembre de 2009, animaban a los Estados a adoptar medidas proactivas en el tratamiento de datos de carácter personal, tanto en el sector público como en el privado, mediante:

- El establecimiento de procedimientos destinados a prevenir y detectar infracciones, que podrán basarse en modelos estandarizados de gobierno y/o gestión de la seguridad de la información.
- La designación, de uno o varios oficiales de privacidad o de protección de datos.
- La realización periódica de programas de concienciación, educación y formación entre los miembros de la organización destinados al mejor conocimiento de la legislación que resulte aplicable en materia de protección de datos.
- La realización periódica de auditorías transparentes pro parte de sujetos cualificados y preferentemente independientes, que verifiquen el cumplimiento de la normativa de protección de datos que resulte de aplicación.
- La adaptación de aquellos sistemas y/o tecnologías de información destinados al tratamiento de datos de carácter personal a la normativa que resulte aplicable.
- La puesta en práctica de estudios de impacto sobre la privacidad previos a la implementación de nuevos sistemas y/o tecnologías de información.
- La adhesión a acuerdos de autorregulación cuya observancia resulte vinculante, que contengan elementos que permitan medir sus niveles de eficacia en cuanto al cumplimiento y grado de cumplimiento.
- La implementación de planes de contingencias que establezca unas pautas de actuación en caso de que se verifique un incumplimiento de la normativa de protección de datos que resulte aplicable.

La designación de un oficial de protección de datos en las diferentes denominaciones adoptadas por los Estados Miembros que han adoptado esta figura (data protection officer, personal data representatives, person responsable for the protection of personal data) se encuentra directamente relacionada con la simplificación o la excepción de la obligación de notificar los ficheros con datos de carácter personal a la Autoridad de Control.

Por su parte, en el ámbito de los Estados Unidos esta figura se encuentra relacionada con un nivel más alto de la organización, adoptando la denominación de Chief Privacy Officer (CPO), no implicando entre sus tareas la publicidad de los ficheros, tal y como establece la normativa europea.

La previsión de la designación del Oficial de Protección de Datos, como forma de excepcionar la obligación de notificar a la Agencia, no ha sido transpuesta a la normativa española.

2. Marco normativo español de protección de datos en relación con la designación de los oficiales de protección de datos.

La preocupación por la protección de datos en España aparece en la Constitución Española como un derecho fundamental que debe ser desarrollado por la normativa adecuada.

En 1992, el Parlamento español aprobó la primera Ley de Protección de Datos, la denominada LORTAD (Ley Orgánica reguladora de los tratamientos automatizados de datos), derogada por la actualmente vigente Ley Orgánica 15/1999, de 13 de diciembre de protección de datos de carácter personal.

Ya en la primera norma citada, en 1992, el Parlamento estableció las principales áreas que deberían ser abordadas en esta materia y que no han experimentado cambios sustanciales en la normativa en vigor:

- Defensa y concienciación de los derechos de los titulares de los datos.
- Cumplimiento de las obligaciones de los responsables de ficheros y de los encargados de tratamiento.
- Creación de una autoridad de control independiente con amplios poderes para velar por el cumplimiento de la normativa.

Teniendo en cuenta los aspectos relativos a la transparencia y la publicidad de los ficheros con datos de carácter personal, es necesario señalar que:

- En relación con el ejercicio de los derechos de los titulares de los datos, se estableció que cualquier persona podría consultar el Registro General de Protección de Datos, órgano incorporado en la Agencia Española de Protección de Datos.

- En relación con las obligaciones de los responsables, ambas normas establecían la obligación de notificar los ficheros con datos de carácter personal a la Agencia Española de Protección de Datos para su inscripción en el Registro General de Protección de Datos, con carácter previo al inicio del tratamiento.

- En consonancia, entre las funciones de la Agencia Española de Protección de Datos, se estableció la publicación del Catálogo de Ficheros inscritos en el Registro General de Protección de Datos para su consulta por cualquier persona.

Otro aspecto relevante, relacionado con las medidas de seguridad y, en cierta manera, con la figura del oficial de protección de datos, es la previsión de nombrar a un **responsable de seguridad** para aquellos ficheros o tratamientos que deban implantar las medidas catalogadas de nivel medio o alto al que se refiere el Título VIII del Reglamento de desarrollo de la LOPD. La designación del responsable de seguridad no representa una exención de la responsabilidad correspondiente al responsable del fichero o al encargado de tratamiento.

Además, también relacionado con los ficheros catalogados como de nivel medio o alto, el reglamento de desarrollo de la LOPD establece la obligación de realizar una auditoría de carácter interno o externo que verifique el cumplimiento de las

previsiones relativas a las medidas de seguridad que deban implantarse en los ficheros o tratamientos con datos de carácter personal.

3. Consecuencias del marco normativo español de protección de datos en la notificación de ficheros.

De acuerdo con la normativa española de protección de datos, la mayoría de los ficheros que incluyan datos de carácter personal deben ser notificados a la Agencia para su inscripción en el Registro General de Protección de Datos.

Es preciso tener en cuenta que la notificación de los ficheros tiene un carácter declarativo, por lo que no constituye una autorización sobre los tratamientos notificados, ni exime al responsable del cumplimiento de resto de las obligaciones establecidas en la normativa.

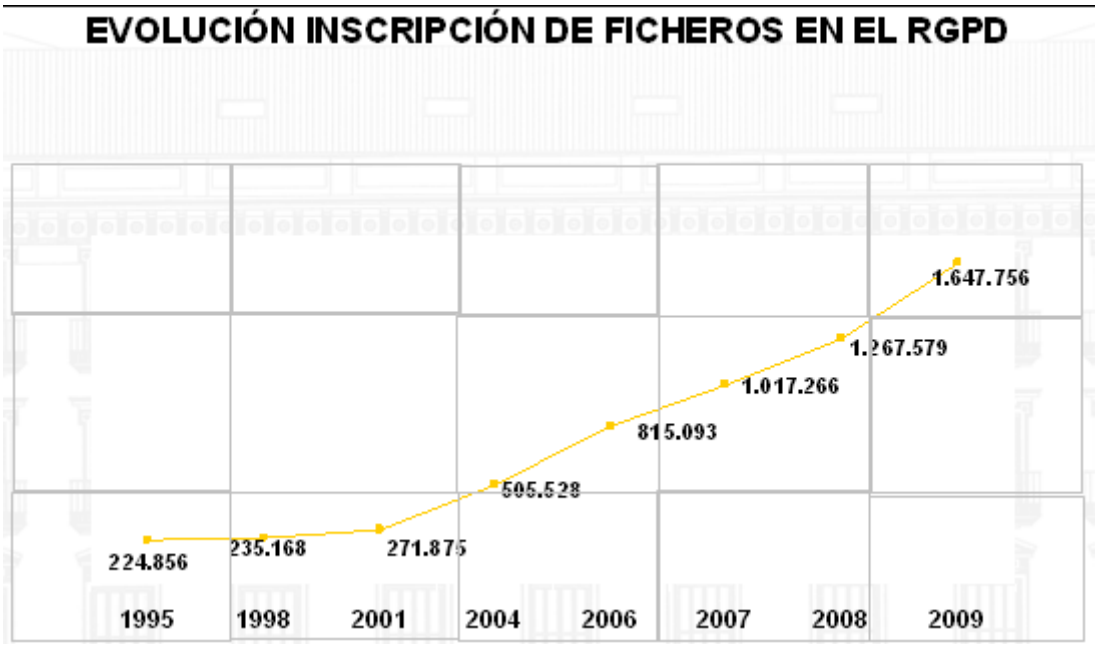
Teniendo en cuenta estas previsiones legales, la Agencia Española de Protección de Datos ha tenido que ir adaptando los procedimientos para atender los requerimientos derivados de las obligaciones de los responsables de ficheros. Estos procedimientos han tenido que evolucionar desde los primeros formularios a los actuales en los que se incluyen modelos simplificados así como procedimientos de administración electrónica (firma electrónica, notificación electrónica, seguimiento electrónico del estado de la tramitación, etc).

Además, se han tenido que adoptar medidas adecuadas para afrontar estos retos:

- Modelos de notificación simplificados para aquellos ficheros más habituales: clientes/proveedores, recursos humanos, nóminas, etc.
- Elaboración de guías para la notificación de ficheros.
- Elaboración de guía para la implantación de medidas de seguridad.
- Elaboración de guía para los responsables de ficheros.
- Herramienta EVALUA para la autoevaluación del cumplimiento de la normativa de protección de datos y las medidas de seguridad.

Como consecuente de la obligación de notificar los ficheros a la Agencia Española de Protección de Datos para su inscripción en el Registro General de Protección de Datos, al final de 2009, figuraban inscritos 1.647.000 ficheros correspondientes a 640.000 empresas y organismos públicos.

Es preciso señalar que la notificación de ficheros ha mantenido una tendencia constantemente creciente, tal y como figura en la figura siguiente, y que esta tendencia parece dar señales de mantenerse en el corto y medio plazo.



4. Relaciones con los responsable de ficheros.

Aunque, tal y como se ha señalado anteriormente, no se ha contado con una previsión específica para la designación de un oficial de protección de datos que pudiera ejercer de punto de contacto efectivo con los responsable de ficheros, una de las mayores preocupaciones de la Agencia Española de Protección de Datos ha sido establecer los canales de comunicación adecuados, ya sea directamente con los responsables de ficheros o a través de las distintas formas de representación adoptadas.

Entre las vías de comunicación utilizadas para lograr un efectivo cumplimiento de la normativa de protección de datos, se podrían citar:

- Elaboración de informes sobre las consultas planteadas por los responsables de ficheros, ya sea directamente o través de las personas o departamentos que tienen asignada la función de velar por el cumplimiento de la normativa de protección de datos en las entidades.
- Colaboración con los responsables de ficheros o sus representantes en temas relacionados con tratamientos de datos con riesgos en materia de protección de datos de carácter personal, transferencias internacionales de datos, reglas corporativas vinculantes, elaboración de códigos de conducta, etc.
- Emisión de informes jurídicos sobre los proyectos de normas reguladoras de creación, modificación o supresión de ficheros presentados por losdepartamentos de las Administraciones Públicas relacionados con el cumplimiento de la normativa de protección de datos.

Además, durante el tiempo de vigencia de la normativa de protección de datos, diversas iniciativas de carácter proactivo se han desarrollado, tanto por parte de los responsables, como por parte de la Agencia Española de Protección de Datos para facilitar el cumplimiento en materia de protección de datos y privacidad, tales como, la realización de inspecciones sectoriales, la elaboración de códigos de conducta, la firma de convenios y protocolos de colaboración con entidades públicas y privadas, así como el fortalecimiento de la relación con los consultores de protección de datos.

4.1.Inspecciones sectoriales

Desde su puesta en funcionamiento la Agencia Española de Protección de Datos ha tenido entre sus prioridades la realización de auditorías de protección de datos dirigidas tanto al sector público como al sector privado con el fin de evaluar el grado de cumplimiento del sector y poder emitir las recomendaciones derivadas de dichas auditorías.

Estas inspecciones sectoriales se han dirigido a distintos sectores como, entre otros:

- Administraciones Públicas.
- Selección de personal a través de Internet.
- Grandes superficies.
- Hoteles.
- Centros de enseñanza.
- Banca electrónica.
- Videovigilancia en Internet
- Instituciones sanitarias
- Sector asegurador.
- Mensajes comerciales SMS
- Transferencias internacionales relacionadas con un Call Center
- Solvencia patrimonial

4.2.Códigos de conducta

La Agencia Española de Protección de Datos, tal y como establece la LOPD y su reglamento de desarrollo, ha estimulado la adopción de Códigos de Conducta como forma de autorregulación en materia de protección de datos.

Los códigos de conducta son códigos éticos o de buenas prácticas profesionales y deben ser de cumplimiento obligatorio por las entidades adheridas a los mismos, debiendo contener reglas específicas o estándares que permitan la armonización de los tratamientos realizados por sus adheridos, facilitando el ejercicio de los derechos de los interesados y favoreciendo el cumplimiento de las previsiones de la normativa de protección de datos. Además, los códigos de conducta deben incluir procedimientos de control independientes que garanticen el cumplimiento de las obligaciones asumidas por las entidades adheridas, estableciendo un adecuado y eficaz régimen disciplinario en caso de incumplimiento.

Entre los Códigos de Conducta actualmente registrados en el Registro General de Protección de Datos, se pueden citar, entre otros:

- Farmaindustria.
- Asociación de Ayuntamientos del País Vasco.
- Universidades
- Organizaciones sectoriales del sector sanitario
- Comercio electrónico

4.3.Convenios de colaboración con entidades públicas y privadas.

Otra vía de colaboración con los responsables de ficheros ha sido la de promover la firma de convenios de colaboración con las entidades y asociaciones de representantes tanto del sector público como privado, así como asociaciones sin ánimo de lucro con el ánimo de promover el cumplimiento de la normativa de protección de datos.

Entre los convenios de colaboración firmados, se podrían citar:

- Instituciones educativas
- Asociación de entidades de seguridad privada
- Cámaras de Comercio.
- Asociación Española para el Sector Electrónico y de las Tecnologías de la Información y de las Comunicaciones (ASIMELEC)
- Instituto Nacional de Tecnologías de la Comunicación (INTECO)
- Federación de Municipios y Provincias

4.4. Consultores de protección de datos

Paralelamente al aumento de la concienciación en materia de protección de datos, la labor de consultoría en materia de protección de datos ha experimentado un auge permanente.

Los consultores en protección de datos ofrecen servicios relacionados con la implantación de las medidas tendentes a facilitar el cumplimiento de las obligaciones en materia de protección de datos. Estos servicios, dependiendo de las necesidades de los responsables, pueden llegar ir desde el cumplimiento de general de las previsiones en materia de protección de datos, a la implantación de las medidas técnicas y organizativas relacionadas con las medidas de seguridad.

También se pueden ofrecer servicios más especializados relacionados con las transferencias internacionales, las reglas corporativas vinculantes o los códigos de conducta.

Además, aquellos consultores que han desarrollado aplicaciones informáticas de protección de datos, utilizan las guías y los procedimientos que les permiten comunicarse con la Agencia de forma electrónica, manteniéndose una comunicación que permite resolver las incidencias técnicas.

5. Distintos escenarios para el cumplimiento en protección de datos

Tanto las organizaciones públicas como las entidades privadas, han adoptado distintos enfoques a la hora de afrontar el cumplimiento en materia de protección de datos, dependiendo de su tamaño, recursos disponibles así como de sus particularidades organizativas.

Las soluciones adoptadas pueden ser resumidas en las siguientes:

a) Entidades privadas pertenecientes al sector de la pequeña y mediana empresa en las que el cumplimiento se realiza por el propio responsable del fichero con los medios puestos a disposición de la Agencia Española de Protección de Datos y las Agencias Autonómicas.
b) Entidades que contratan, totalmente o parcialmente, con un tercero el cumplimiento en materia de protección de datos.
c) Entidades que afrontan el cumplimiento en materia de protección de datos desde los departamentos relacionados con la seguridad de la información.
d) Entidades que implantan el esquema de cumplimiento en materia de protección de datos de una forma global a través de un departamento o persona encargada del cumplimiento. Este enfoque, que representa un mayor grado de madurez organizacional, puede incluir además también el cumplimiento en relación con otras regulaciones (propiedad intelectual,

normativa específica del sector, Sarbanes-Oxley, administración electrónica, etc).

6. Funciones del oficial de protección de datos.

Con independencia que las funciones relacionadas con el cumplimiento en material de protección de datos sean coordinadas por una persona o por un departamento, deberá ser formalmente designado por el Responsable del fichero para coordinar, impulsar y supervisar el cumplimiento de la normativa de protección en relación con los tratamientos de datos de carácter personal.

Entre las principales funciones atribuidas a esta figura, se pueden citar:

- Establecer, mantener y supervisar el cumplimiento en materia de protección de datos y privacidad.
- Valorar el impacto sobre el marco de privacidad y la protección de los datos personales de nuevos proyectos o de normas que afecten a la organización.
- Centralizar la atención de los ejercicios de los derechos de los interesados.
- Centralizar la atención de las reclamaciones formuladas por los interesados.
- Centralizar las relaciones institucionales de forma interna con el todos los departamentos afectados por el cumplimiento: responsables internos de los distintos ficheros, Departamento de Recursos Humanos, Departamento de Tecnologías, Departamento de Seguridad, Departamento Legal, etc.
- Coordinar las relaciones con la Agencia Española de Protección de Datos y/o, en su caso, con la Agencia de Protección de Datos de la Comunidad Autónoma correspondiente.
- Supervisar y coordinar la notificación de ficheros.
- Supervisar la gestión de incidencias.
- Coordinar los planes de auditoría, ya sea de carácter interno o externo.
- Impulsar la adopción de medidas correctoras y de mejora para asegurar el cumplimiento de la normativa de protección de datos.
- Impulsar y promover buenas prácticas en protección de datos.
- Promover e impulsar la formación, educación y concienciación en protección de datos.

7. Conclusiones

a) La designación, de uno o varios oficiales de privacidad o de protección de datos, con adecuada cualificación, recursos y competencias suficientes para ejercer sus funciones de supervisión, se considera una medida muy adecuada y útil de cara a promover el mejor cumplimiento de la normativa sobre protección de datos, tal y como se establece en la Directiva 95/46/CE de protección de datos.

b) Los Estándares Internacionales sobre Protección de Datos Personales y Privacidad aprobados en la 31ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, celebrada en Madrid en noviembre de 2009, animaban a los Estados a adoptar medidas proactivas en el tratamiento de datos de carácter personal, tanto en el sector público como en el privado, entre las que se encuentra la designación de uno o varios oficiales de privacidad o de protección de datos.

c) En la normativa europea, la designación del oficial de protección de datos se encuentra directamente relacionado con la excepción en la obligación de notificación de los ficheros, en la medida en que la designación de estos oficiales conlleva que la publicidad de los ficheros de la organización queda asegurada por esta figura, pudiendo los interesados acudir a estos profesionales para consultar los ficheros que incluyen sus datos.

d) En la normativa española no se ha transpuesto la previsión de excepcionar la notificación de ficheros ligada a la designación de un oficial de protección de datos.

e) Sin embargo, la Agencia considera de gran valor la posibilidad de establecer canales de comunicación con las personas o departamentos que realicen esta labor relacionada con el cumplimiento en materia de protección de datos y privacidad.

f) En este sentido, durante el tiempo de vigencia de la normativa de protección de datos, diversas iniciativas de carácter proactivo se han desarrollado, tanto por parte de los responsables, como por parte de la Agencia Española de Protección de Datos para facilitar el cumplimiento en materia de protección de datos y privacidad.

g) El rol de oficial de protección de datos debe ser considerado desde una perspectiva más amplia que la centralización de las labores relacionadas con la notificación.

h) También debe ser considerada desde una perspectiva más amplia que la implantación de las medidas de seguridad. De hecho, desde un punto de vista ideal sería recomendable que la labor del oficial de protección de datos se independizará de las labores de seguridad, dado que pueden surgir conflictos de intereses entre un departamento y otro.

i) La labor del oficial de protección de datos tiene que contar con el respaldo decidido de la dirección de la organización asegurando su independencia.

j) Para desarrollar esta función se debe contar con los conocimientos adecuados en protección de datos, normativas relacionadas con el sector de actividad de la organización, conocimientos amplios de la organización, conocimientos de análisis y gestión de riesgos relacionados con los sistemas de información, entre otros.