El Delegado de Protección de Datos en las Administraciones Públicas

Manual práctico para cumplir con el Reglamento General de Protección de Datos

Virginia Guasp Martínez

EL CONSULTOR DE LOS AYUNTAMIENTOS

ÍNDICE SISTEMÁTICO

II.
PROPUESTA DE UN MODELO DE DELEGADO DE PROTECCIÓN DE DATOS EN LAS ADMINISTRACIONES PÚBLICAS

PRÓLOGO

La obra que tengo el honor de prologar tiene su origen en la tesis doctoral que su autora defendió 25 de abril de 2025 en el Salón de Grados de la Facultad de Derecho de la Universidad de Valladolid. Con una brillante exposición puso punto final a un trabajo de investigación de 9 años que mereció la máxima calificación académica.

Confieso que me siento muy orgulloso de figurar como codirector y prologuista de un trabajo tan sólido, tan consistente, que habla por sí solo de la solvencia, la inteligencia y el rigor científico de su autora. Pero lo cierto es que no puedo atribuirme ningún mérito en esta historia. Ni siquiera en la elección del tema, que es un acierto imputable por entero, como todo lo demás, a la doctoranda. Me he limitado a leer y comentar las sucesivas versiones del trabajo. Aunque mi aportación como presunto orientador del mismo ha sido irrelevante, he sido testigo del pundonor y la tenacidad de Virginia y puedo dar fe de su coraje, de su empeño por analizarlo todo, absolutamente todo, a fondo, sin concesiones a la pereza o la cómoda mediocridad, contra viento y marea, sacrificando su escaso tiempo libre. No advertí nunca una señal de desaliento en ese arduo y solitario proceso de gestación. Sólo con esa determinación y esa perseverancia a prueba de bombas puede uno emprender una carrera de fondo, como es la elaboración de una tesis doctoral, y cruzar la meta sin perecer en el intento.

Nuestra flamante doctora tiene mucho mérito y es justo consignarlo aquí. Porque, como otros doctorandos que se ganan la vida fuera del ecosistema universitario y no aspiran a cursar una carrera académica, ha tenido que compatibilizar su paciente labor investigadora con una intensa actividad profesional. Ha sido letrada jefe de la Consejería de la Presidencia de la Junta de Castilla y León y Delegada de Protección de Datos de la misma. Desde 2022 es vocal asesora en la Subdirección de Inspección de la Agencia Española de Protección de Datos, una responsabilidad que denota su vocación de servicio público y su compromiso con la defensa de los derechos y libertades constitucionales. Un compromiso que viene avalado también por un amplio repertorio de publicaciones sobre cuestiones que no se circunscriben al objeto de su investigación doctoral. Su repleto curriculum es muy revelador: no se ha tomado un respiro.

Ha dedicado buena parte de su dilatada trayectoria como servidora pública a visibilizar y fortalecer las garantías de ese derecho en los múltiples frentes que se van abriendo como consecuencia de las incesantes innovaciones tecnológicas (el tratamiento de datos biométricos para el control de presencia, el reconocimiento facial, el tratamiento de datos personales a través de la inteligencia artificial, la videovigilancia, la geolocalización, la suplantación de identidad, los sistemas de información crediticia...).

Pero eso no es todo. Virginia Guasp ha formado a cientos de empleados públicos en materias relacionadas con la protección de datos de carácter personal desde el año 2013, organizando jornadas o cursos e impartiendo ponencias dirigidas a quienes trabajan en sectores específicos como el sanitario o el educativo y al personal que presta sus servicios en todo tipo de Administraciones. Yo mismo he podido comprobar su extraordinaria capacidad didáctica, su elocuencia, en varias conferencias impartidas a los alumnos de nuestra Facultad. Trasmite un entusiasmo contagioso, porque cree firmemente en lo que dice y esa íntima convicción se aprecia incluso en cualquier conversación informal que termine desembocando en sus dominios, en un terreno en el que ella no solo se mueve como pez en el agua, sino que lo hace de forma vehemente, con incontenible pasión. Porque para Virginia la tutela efectiva de los derechos de todas las personas, y muy particularmente de las más vulnerables, frente a las amenazas derivadas de la vertiginosa digitalización y el tratamiento masivo de datos no es un simple trabajo retribuido ni un sugestivo reto intelectual, es mucho más que eso, es una causa, una causa justa, una misión que activa su natural empatía y moviliza toda su energía.

Ella ha explicado alguna vez que asumir el encargo de formar a quienes esperan que les ilustres con tus acreditados conocimientos en una determinada materia te obliga a sentarte a pensar, a no dar nada por sentado, a formularte nuevas preguntas, a estudiar y caer en la cuenta, a no conformarte con aproximaciones superficiales, a desarrollar un pensamiento crítico. Y es esa inagotable curiosidad, esas ganas de aprender y ahondar en los problemas para desentrañar todas las claves, las que le llevaron a dar el paso de elaborar una tesis doctoral, pero no una tesis para presumir, para colgar el título en la pared y colmar la legítima vanidad de quien ha invertido un enorme esfuerzo para coronar con éxito su gesta, sino una tesis útil, que sirva para algo, que no sea un alarde de erudición y dé cumplida respuesta a un problema real. Un ensayo rigurosamente original que sirva, entre otras cosas, para mitigar la incertidumbre y la soledad de los Delegados de Protección de Datos (DPD), una soledad que ella ha padecido en primera persona.

La excelente factura del libro revela que estamos en presencia de una jurista senior, madura, con talento y oficio para llevar a buen puerto un trabajo de

investigación, que se mueve con soltura, con criterio, en todos los frentes. Es una obra cocinada a fuego lento, sin prisas, construida a base de razonamientos bien trabados y rematada con unas atinadas conclusiones que, en lo esencial al menos, no puedo sino compartir.

Por lo que concierne a los aspectos formales y metodológicos, el lector comprobará enseguida que es una obra bien escrita, con extrema precisión y pulcritud. Y bien ordenada e hilvanada. La autora se interna en un territorio árido y apenas explorado, pero no pierde en ningún momento el rumbo. Hay un hilo conductor que no es otro que el rol que puede jugar el DPD para reforzar la vigencia efectiva del derecho fundamental a la protección de datos de carácter personal en un entorno tan peculiar como el de las Administraciones Públicas. Un ámbito en el que la presencia de esta figura es obligatoria porque se llevan a cabo tratamientos de datos a gran escala, con cantidades ingentes de datos personales de todo tipo, muchos de ellos especialmente sensibles. Pues bien, cuando uno se adentra en la lectura de sus páginas, se agradece mucho no sólo esa coherencia interna, sino también la claridad expositiva, una claridad que es reflejo de una mente ordenada, bien amueblada. Por lo demás, la bibliografía es sencillamente abrumadora y está actualizada. Hace gala de un dominio completo de la literatura especializada.

Al indiscutible valor añadido de la obra contribuye no sólo el minucioso análisis crítico de normas y prácticas administrativas, sino también la batería de propuestas *de lege ferenda* que formula la autora. Son un buen testimonio de su honesta preocupación por el rendimiento de esta novedosa figura, que le lleva a poner el foco en los imperativos de la práctica, de la cruda realidad, con un enfoque muy pegado al terreno. Porque Virginia no es una fundamentalista, una talibana, conoce esas dificultades perfectamente, mejor que nadie. Por eso, sus propuestas no son un brindis al sol, son sensatas y factibles.

En la primera parte de la monografía se estudia la naturaleza y la evolución del derecho fundamental a la protección de datos de carácter personal, un derecho autónomo, con entidad propia, aunque de proyección transversal, de cuyo alcance e impacto en nuestras vidas y en nuestras libertades no somos aun plenamente conscientes. Es una aproximación de carácter instrumental (no procedía un examen exhaustivo) para centrarse luego en la regulación y las funciones del DPD. Este capítulo introductorio tiene calado dogmático, porque ofrece una visión innovadora del derecho a la autodeterminación informativa, que pone el énfasis en la necesidad de una actuación preventiva y proactiva, no meramente reactiva o represiva, y una detección y evaluación temprana de los riesgos, antes de que se consumen los daños. No se trata sólo de resarcir los perjuicios ya producidos y restablecer al afectado en sus derechos (garantías ex post), sino de anticiparse a los problemas y neutralizar las posibles amenazas (garantías ex

ante). Esta nueva perspectiva (un cambio de paradigma, llega a decir la autora) es la que inspira el Reglamento General de Protección de Datos (RGPD) de la Unión Europea y da sentido a la figura del DPD como garante del derecho en un escenario cada vez más complejo e incierto.

La doctora Guasp no alberga la menor duda sobre el acierto del legislador europeo al incorporar esta nueva garantía y su virtualidad para asegurar el cumplimiento efectivo de las múltiples obligaciones establecidas en el RGPD, una norma de aplicación directa que no requiere la transposición de sus disposiciones al ordenamiento interno de cada Estado miembro de la UE. Pero esa potencial funcionalidad depende de su encaje dentro del sistema de gestión del cumplimiento normativo diseñado en el Reglamento y de una adecuada articulación de sus competencias con las asignadas al responsable y al encargado del tratamiento. Como experto en la materia, el DPD asesora a este, supervisa su gestión y le presta la ayuda necesaria para aplicar de la forma más correcta y cabal posible el Reglamento y la normativa complementaria. Al fin y al cabo, el cumplimiento de las obligaciones impuestas por el RGPD (garantizar el ejercicio de los derechos de los interesados, implantar la privacidad desde el diseño y por defecto, identificar y evaluar riesgos, gestionar brechas de datos personales; velar por la transparencia, formar y concienciar a directivos y empleados, realizar auditorías...) es una responsabilidad que recae directamente en el responsable del tratamiento (art. 5.2).

En cuanto al estatuto jurídico y el diagrama organizativo del DPD contamos con las previsiones del RGPD y la LOPDGDD, que apenas han sido objeto de concreción o desarrollo normativo por parte de la Administración General del Estado o las Administraciones autonómicas en el marco de sus respectivas competencias. En este capítulo se pasa revista a los diferentes modelos de designación y organización existentes en las administraciones públicas, y las garantías que se le otorgan en el ejercicio de esas funciones. En el marco esbozado por el RGPD, cada Estado y cada administración, en función de sus dimensiones y sus características, tiene que encontrar la fórmula que mejor se ajuste a sus peculiaridades, con el fin de garantizar de manera integral y efectiva el derecho fundamental a la protección de datos de carácter personal. En todo caso, su inserción en la estructura administrativa ya supone por sí misma una reducción de los riesgos, una apuesta decidida por la terapia preventiva, porque el DPD va a participar activamente en todo tipo de análisis, estudios o conflictos relacionados de algún modo con la protección de los datos de carácter personal dentro de la organización.

Al examinar el cuadro completo de tareas encomendadas al DPD la autora destaca su posición de bisagra, porque, por un lado, ha de atender las preguntas y denuncias formuladas por los interesados en relación con el tratamiento de sus

datos personales, pero, por otro, actúa como interlocutor de las autoridades de control, elevando consultas y colaborando con ellas en sus investigaciones o en la ejecución de sus resoluciones.

Se suele decir, con razón, que un derecho vale lo que valen sus garantías. Como letrada y gestora experimentada, Virginia es muy consciente de que la finalidad perseguida con esta figura puede malograrse si no se blinda su independencia con las necesarias garantías. Es en este punto donde se juega realmente la partida, el éxito o el fracaso de este instituto. Es esa preocupación la que le lleva a plantearse cómo pueden trasplantarse al ámbito de las administraciones públicas las garantías conferidas al DPD por el RGPD. Fruto de esa indagación es un estudio pormenorizado de los requisitos exigibles para su correcta implementación.

En primer lugar, su perfil profesional. Ha de ser lógicamente un experto en protección de datos, que no sólo conozca a fondo la normativa nacional y europea que regula específicamente esa materia y la que, con carácter general, regula la estructura y el funcionamiento de la Administración en nuestro país, sino que esté también capacitado para descifrar y comprender el entramado tecnológico que sirve de soporte al espacio digital. Con un perfil tan singular, no parece disparatada su sugerencia de que se cree un cuerpo funcionarial especial o una escala dentro de alguno de los existentes para cubrir este puesto. Pero no basta con una cualificación profesional adecuada para desempeñar de manera eficaz sus funciones. Han de ponderarse igualmente las cualidades personales y la autora destaca algunas en particular: integridad moral, motivación y compromiso; capacidad de trabajo y de resolución de problemas y conflictos; capacidad de comunicación, de negociación, de mediación y de gestión de equipos; empatía y sensibilidad por la problemática de los interesados; y, sobre todo, sentido común.

En cuanto a la posición que ocupa el DPD en el organigrama administrativo, el responsable del tratamiento puede optar por un DPD interno o un DPD externo, y en ambos supuestos puede elegir entre designar un único DPD, que puede ser una persona física o jurídica, o varios. Si se decanta por un DPD interno, integrado en la propia organización, caben distintas alternativas: se puede crear un puesto de trabajo o un órgano ad hoc, o se pueden acumular sus funciones a un puesto ya existente en la RPT, y se puede prestar esa función a tiempo completo o a tiempo parcial. Cada una tiene sus ventajas e inconvenientes. Lo que realmente importa es que, cualquiera que sea su dependencia orgánica, se garantice su independencia funcional, lo que excluye la sujeción a instrucciones del responsable del tratamiento, el encargado del tratamiento o un tercero. Una cosa es que deba rendir cuentas de su actuación ante ellos y otra muy distinta que estos se entrometan o inter-

fieran en el ejercicio de sus competencias. La independencia del DPD frente a todo tipo de presiones o injerencias se ve reforzada sin duda cuando se dota de estabilidad al puesto de trabajo. Sólo así podrá actuar con objetividad e imparcialidad, con libertad de criterio, sin temor a recriminaciones o represalias. Y aquí entra en juego la garantía de indemnidad, que impide que pueda ser destituido o sancionado directa o indirectamente por el responsable del tratamiento. Nuestra LOPDGDD sólo contempla una excepción: la posibilidad de ser removido o sancionado si incurre en dolo o negligencia grave en el desempeño de sus funciones.

En este terreno, a nadie se le escapa que una de las claves para el buen funcionamiento de esta institución en el sector público es el procedimiento previsto para su designación. Y lógicamente la autora presta mucha atención a esta cuestión, que no puede concebirse como una simple formalidad administrativa. No se trata de nombrar un DPD para cubrir el expediente, como un trámite preceptivo para cumplir la ley. Si el DPD es interno y se elige a un funcionario de carrera, son varias las formas de provisión a las que se puede recurrir, pero entiende que la más adecuada es la convocatoria de un concurso específico, en el que además de valorarse los méritos previos de los aspirantes, éstos se someten a una serie de pruebas con el fin de verificar si reúnen las cualidades profesionales que exige el RGPD. Si, por el contrario, el DPD es externo, su designación puede llevarse a cabo a través de cualquier fórmula jurídica (normalmente, un contrato o un convenio administrativo).

Es obvio que por impecable que fuese el procedimiento de designación del DPD y por potentes que fuese las garantías destinadas a blindar su posición, de poco serviría si no se le dota de los medios necesarios para poder cumplir su misión. La autora sabe perfectamente de lo que habla y por eso sale al paso de una práctica muy extendida que consiste en escatimar los recursos que se ponen a disposición del DPD. De ahí su insistencia en que ha de tener acceso a los datos personales, a las operaciones de tratamiento y a toda la información que precise; y contar con los medios personales (un equipo multidisciplinar que le ayude en su cometido) y materiales (un espacio físico apropiado, recursos informáticos, un correo electrónico y un teléfono de contacto...) que sean indispensables.

El libro que el lector tiene en sus manos no sólo contiene un análisis crítico de la regulación vigente y su deficiente aplicación, sino que incluye una propuesta específica para reglamentar y articular este nuevo organismo en la Administración General de la Comunidad Autónoma de Castilla y León. Una propuesta que por su grado de concreción y detalle podría implementarse automáticamente, tal y como está diseñada. Y replicada en su caso en otras Comunidades Autónomas.

No es desde luego una ocurrencia improvisada. Virginia explica que en julio de 2019, ostentando el cargo de DPD de la Consejería de la Presidencia se la presentó al Vicepresidente de la Junta de Castilla y León. La idea consistía en crear la Oficina del Delegado de Protección de Datos, como una estructura permanente y transversal que sirviera para visibilizar la relevancia del derecho fundamental a la protección de datos personales en el marco de la Administración pública y contribuir a su tutela efectiva. Sería un órgano administrativo adscrito orgánicamente a la Consejería que tuviera atribuidas las competencias en materia de protección de datos, pero con la autonomía funcional que garantiza el RGPD (incluyendo la elaboración de un presupuesto propio). En esta Oficina se integraría un DPD coordinador, como titular del órgano, y tantos DPD sectoriales como consejerías y organismos autónomos tuviera la Administración autonómica. Al DPD coordinador le correspondería la formulación de criterios y recomendaciones comunes para toda la Administración autonómica, lo que redunda en una mayor eficacia y seguridad jurídica, al minimizarse las posibles discrepancias entre los distintos DPDs y responsables del tratamiento a la hora de interpretar y aplicar la normativa. En cualquier caso, ese objetivo de una mínima uniformidad no puede alcanzarse a costa de la independencia funcional del resto de los DPDs.

De acuerdo con esta propuesta, la Oficina del Delegado de Protección de Datos debería regularse mediante un Decreto de la Junta de Castilla y León, que debería precisar la naturaleza jurídica del órgano, su adscripción, sus funciones y su estructura, que tendría que incluir necesariamente un equipo multidisciplinar de apoyo compuesto de personal cualificado (juristas, ingenieros informáticos o de telecomunicaciones, archiveros...). Por lo que respecta al nombramiento de los DPDs, el correspondiente acuerdo de la Junta debería ir precedido de un procedimiento caracterizado por las notas de concurrencia competitiva, mérito y capacidad, publicidad y transparencia.

Este capítulo se cierra con una cita muy pertinente de Rafael Jiménez Asensio, que no me resisto a reproducir: «Los problemas —y no descubro nada nuevo— son los de siempre: la rigidez enorme (y absoluto desfase) de nuestro sistema normativo de función pública y su clara y evidente obsolescencia para dar respuesta a estas nuevas necesidades que ya comienzan a emerger de forma clara en el sector público …Reformar los sistemas de provisión de puestos de trabajo requiere una Ley, pero adaptar esos sistemas a las enormes singularidades que ofrece esta figura del Delegado de Protección de Datos (preludio tal vez de otras muchas figuras o puestos de trabajo de especial factura que, en el campo de la digitalización y Big Data, se puedan dar en los años venideros, también en el sector público) requiere sin duda dosis de ingenio, propuestas creativas e innovadoras, adaptabilidad, flexibilidad en el diseño y una línea de trabajo sostenida que haga avanzar a la administración pública por el camino de la profesionali-

zación, la tecnificación y la apertura a la sociedad, en consonancia con el Gobierno Abierto y la Gobernanza Pública».

La doctora Guasp ha tomado buena nota de esa exhortación y este libro es la prueba de que se la ha tomado muy en serio. Porque es mucho más que un manual de instrucciones de indudable utilidad para los servidores públicos que han asumido o van a asumir la responsabilidad de ocupar el cargo de Delegado de Protección de Datos (en ese sentido, es evidente que marca un antes y un después y es ya la obra de referencia, de obligada consulta). Encierra también interés para cualquier persona preocupada por los desafíos que plantea la circulación masiva de datos de carácter personal y su utilización y comercialización a gran escala. En este aspecto, creo que contribuye a apuntalar una cultura de respeto a la privacidad demasiado débil todavía entre nosotros. Por todo ello, debo felicitar de nuevo a su autora y recomendar por supuesto su lectura. Me daré por satisfecho si estas notas sirven para despertar la curiosidad por una obra que vale la pena leer atentamente.

Juan María Bilbao Ubillos

INTRODUCCIÓN

La figura del delegado de protección de datos me fascinó desde la primera lectura del Reglamento General de Protección de Datos. Por vez primera se instauraba para toda la Unión Europea, dentro de las organizaciones, un defensor directo del ciudadano respecto del derecho fundamental a la protección de datos de carácter personal. Una figura prácticamente nueva en el derecho español, sin que existiera una de similares características con la que compararse.

Así, se configura el delegado de protección de datos como un instrumento auxiliador y asesor para responsables y encargados del tratamiento, en relación con la aplicación del Reglamento General de Protección de Datos. Y ello a los efectos de evitar que los riesgos en los derechos y libertades de los interesados presentes en los tratamientos de datos personales se materialicen en daños para estos. Además de asesorar sobre la gestión del cumplimiento normativo previsto en el Reglamento General de Protección de Datos, entre otras funciones, el delegado de protección de datos constituye un punto de contacto con las autoridades de control y atiende a los interesados.

Me sedujeron las inmensas posibilidades de lo que, con esta figura, que podría calificarse como un factótum, podría lograrse en relación con la garantía de este derecho fundamental, cuyo impacto en la vida de todos nosotros en la actualidad es evidente, especialmente dentro de una organización administrativa. Tan solo calibrar cómo podría calar el delegado de protección de datos en las administraciones públicas suponía ya un desafío importante.

En este contexto, y al inicio de la aplicación del Reglamento General de Protección de Datos, tuve la oportunidad de trabajar como delegada de protección de datos en la Consejería de la Presidencia de la Junta de Castilla y León.

Cuando nada estaba construido y todo estaba por hacer, las dificultades y los obstáculos con los que me encontré, de todo tipo, fueron muchos, desde la invisibilidad del derecho fundamental, pasando por la pasividad, la dejadez o la incomprensión, hasta el rechazo absoluto de la figura y sus funciones. Nada muy diferente o alejado de la problemática a la que se enfrentaron mis compañeros delegados de protección de datos, especialmente en las administraciones públicas.

No sería justo decir que todo fue indiferencia y falta de colaboración. Muchos funcionarios, mis compañeros, a los que estoy inmensamente agradecida, mostraron su interés por hacer bien las cosas, facilitando sobremanera el desempeño de mis funciones.

Mas, sobre este escenario de dificultades, mi inicial entusiasmo tornó en escepticismo sobre si realmente la figura servía como yo la percibía, esto es, como un verdadero garante del derecho fundamental.

Empecé a preguntarme si las administraciones públicas y el sistema español estaban preparados para acoger esta figura. A cuestionarme si las normas jurídicas existentes daban cobertura a su implantación y cómo, si no, habría que diseñar o mejorar el sistema, con qué herramientas e instrumentos. Y ello para que efectivamente la figura del delegado de protección de datos funcionara, aun contando con las resistencias naturales del propio sistema, sirviendo para lograr la finalidad pretendida por el Reglamento General de Protección de Datos con su implementación, esto es, lograr la protección efectiva de las personas físicas.

La cuestión es si el Derecho soportaba o, mejor dicho, daba soporte a esta nueva figura.

Consideré que podría ser necesario, incluso imprescindible, construir, desde una visión eminentemente práctica y sobre las bases jurídicas con las que se contaba, un modelo tipo, un sistema integral, que fuera una herramienta que pudiera ser utilizada por cualquier administración pública que tuviera dificultades respecto de la integración de la figura en la estructura de una organización administrativa.

Y ello porque la figura no es circunstancial, sino permanente, definitiva. El delegado de protección de datos ha venido para quedarse y precisa de una respuesta concluyente que solvente la imprevisibilidad inicial. La solución ha de ser, además, mucho más contundente en las administraciones públicas que ejercen potestades públicas, que están al servicio de los ciudadanos y donde el nombramiento del delegado de protección de datos es obligatorio.

Es obvio que muchas administraciones públicas desconocen cómo afrontar el reto de cumplir con la obligación de designar al delegado de protección de datos, resultando que ni la normativa de aplicación ni la jurisprudencia les muestran de modo tangible, claro y sencillo la forma legal de cumplir con estas obligaciones dentro de sus organizaciones, ajustándolas a la idiosincrasia y características de estas.

Cuestiones tan concretas como de qué forma, jurídicamente hablando, ha de nombrarse el delegado de protección de datos o qué tipo de personal puede desempeñar estas funciones o cómo contratar a un delegado de protección de

datos externo a la administración pública son habituales y no cuentan con una respuesta directa ni en el Reglamento General de Datos ni en la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales.

La tarea no es sencilla, como se verá a lo largo de este libro, puesto que el Reglamento General de Protección de Datos exige, particularmente, pensar mucho antes de comenzar a actuar.

Acostumbrados a supuestos de hecho tasados con consecuencias jurídicas concretas, en el Reglamento General de Protección de Datos no se delimitan qué tratamientos concretos y con qué condiciones pueden efectuarse.

El Reglamento General de Protección de Datos cuenta con una innegable complejidad, por su enfoque eminentemente garantista, preventivo, proactivo y flexible, que evita la obsolescencia de la norma jurídica, pero que implica una transformación radical en la mentalidad del jurista.

El Reglamento General de Protección de Datos demanda saber Derecho, con mayúsculas, contar con conocimientos técnicos y tener una visión abierta y amplia que permita la comprensión integral del derecho fundamental a la protección de datos. Es una norma jurídica que, como la lluvia fina, cala lentamente.

De esta forma comencé a pensar en un intento de aligerar esta tarea de componer un modelo tipo, que he desarrollado a través de este manual.

Con ello he pretendido, en primer lugar, realizar una prueba de resistencia para comprobar si el ordenamiento jurídico español soporta o da soporte a la figura del delegado de protección de datos sobre la base establecida por el Reglamento General de Protección de Datos.

Segundo, y desde un enfoque eminentemente práctico y global, he tratado de establecer reglas dentro de un modelo tipo que sea susceptible de adaptarse a la organización e idiosincrasia de cualquier administración pública, que, desde las obligaciones fijadas en el Reglamento General de Protección de Datos, descienda a problemas habituales y recurrentes de las administraciones públicas ofreciendo soluciones concretas para solventarlos.

Se pretende auxiliar a las administraciones públicas de forma inmediata a escoger, nombrar e incorporar debidamente al delegado de protección de datos en su estructura y organización, cumpliendo efectivamente con la normativa de protección de datos de carácter personal, y, en concreto, con sus obligaciones de responsabilidad proactiva, para garantizar el derecho fundamental a la protección de datos de carácter personal en el ejercicio de sus competencias y funciones.

En tercer lugar, he aspirado también visibilizar el valor de este nuevo actor en el escenario de la protección de datos, que a su vez muestra la importancia cada vez mayor de este derecho fundamental.

Y, además, por último, ayudar al delegado de protección de datos a ser consciente de la importancia de su trabajo, de cuál debería ser su posición en la organización administrativa y de cuáles son sus derechos en el ejercicio de sus funciones.

Mediante esta obra he pretendido aligerar esta tarea que han de realizar las administraciones públicas, pensando por ellas, elaborando un modelo tipo de cumplimiento normativo que sea susceptible de aplicarse inmediatamente y adaptarse a las necesidades de las administraciones públicas. Es, por tanto, un instrumento que dota de herramientas prácticas para designar y posicionar, cumpliendo con el Reglamento General de Protección de Datos, al delegado de protección de datos en las administraciones públicas.

Y a partir de aquí, desde la experiencia de todos, abiertos a nuevas ideas y a críticas constructivas, comenzar a construir algo nuevo.

Espero que sea de utilidad.

3. POSICIÓN DEL DELEGADO DE PROTECCIÓN DE DATOS EN LA ESTRUCTURA DE LAS ADMINISTRACIONES PÚBLICAS: MODELOS ORGANIZATIVOS DE DELEGADO DE PROTECCIÓN DE DATOS

3.1. Elección del sistema adecuado: responsabilidad proactiva

El responsable del tratamiento debe decidir de manera activa, consciente y proactiva qué tipo de sistema implanta en su organización en aras a establecer la figura del DPD. Puede elegir entre un DPD interno o un DPD externo y entre designar a un único DPD o a varios. Todos los sistemas tienen ventajas e inconvenientes, resultando que lo que son ventajas en uno de ellos tornan en desventajas en el otro sistema. Mas, lo determinante es que el sistema que se elija sea apropiado para que el DPD preste eficazmente sus funciones y sirva al cumplimiento del RGPD por parte del responsable del tratamiento. Como vamos a comprobar, no existe una fórmula mágica. Lo que para una organización puede resultar idóneo, para otra puede constituir un fracaso. No existen, por tanto, sistemas buenos o malos en términos absolutos, sino sistemas adecuados o inadecuados para la organización del responsable del tratamiento.

Así, PUYOL MONTERO manifiesta que los pros del nombramiento de un DPD externo son aquellos relacionados con la reducción de costes (pudiéndose asignar recursos en función de necesidades puntuales, a través de un contrato de servicios), el poder dotarse de profesionales con amplios conocimientos en todos los ámbitos necesarios en cuanto a protección de datos y la reducción del conflicto de intereses; determina como aspectos negativos el menor conocimiento de la organización y del sector, la dificultad de participar en todas las cuestiones de la organización relacionadas con la protección de datos y el riesgo de pérdida de independencia(242).

Sobre tal particular debemos objetar que la reducción de costes es algo relativo, puesto que en el ámbito administrativo no tiene por qué ser más económico externalizar un servicio que tenerlo internalizado, máxime cuando en muchas administraciones públicas se han nombrado DPDs a coste cero (acumulando las funciones del DPD a las que ya desempeñaba un empleado público) y que el nombramiento de DPD en las administraciones públicas no es una obligación puntual sino permanente.

Amén de que lo que se ha de buscar es un DPD competente, efectivo en sus funciones y resolutivo, donde si bien el coste debe tenerse en consideración (los recursos públicos no son ilimitados) no ha de ser el único elemento, ni mucho menos a considerar, y ello bajo el axioma de que «lo barato sale caro». El coste debe ser el adecuado para prestación profesional del servicio de DPD.

(242) PUYOL MONTERO, Javier (2020), *La figura del delegado de protección de datos (DPD) adaptado al reglamento (UE) 2016/679 (RGPD) a la LO 3/2018, de 5 de diciembre (LOPDGDD) y al esquema de certificación de la Agencia Española de Protección de Datos,* Aferré Editores, págs. 44 y 45.

Asimismo, y en relación con el conflicto de intereses, si está bien protocolizado en el ámbito administrativo, como se verá posteriormente, no tiene por qué generar más problemas en un DPD interno que en un DPD externo.

En todo caso, antes de efectuar la elección debe abordar el examen pormenorizado de su situación, sus necesidades y las de su organización, para valorar qué fórmula se adapta mejor, a los efectos de cumplir con el RGPD y LOPDGDD. Es claro que *«ha de ser el responsable el que valore la procedencia de designar uno o varios DPD, así como si el mismo ha de pertenecer o no a su propia estructura, garantizando en todo momento su independencia y disponibilidad»*, tal y como dispone el Informe 0100/2019 del Gabinete Jurídico de la AEPD, de 17 de febrero de 2020, sobre la designación de DPD en el Ministerio de Defensa.

No hemos de olvidar que, en el ámbito de las administraciones públicas especialmente, conforme apostilla el Informe 0037/2020, de 17 de febrero de 2020, del Gabinete Jurídico de la AEPD, *«la fórmula adoptada para el nombramiento de DPD dependerá de la decisión adoptada por la entidad en la que desempeñe sus funciones, como consecuencia de su autonomía organizativa»*.

En relación con lo anterior, el Gabinete Jurídico de la AEPD matiza en su Informe 0011/2019, sobre diversas cuestiones relativas a la figura del DPD, que *«con independencia del criterio organizativo seguido en el ámbito de una determinada Administración pública, así como del nombramiento único o múltiple de varios DPD, en ningún caso la fórmula adoptada podrá suponer una excusa para el debido cumplimiento del conjunto de las obligaciones dimanantes de la normativa a la que se ha hecho mención, contenida en la Sección 4 del CAPÍTULO IV, del RGPD, y en el CAPÍTULO III del TÍTULO V de la LOPDGDD —artículos 34 a 37—»*.

No es una decisión baladí ni que pueda realizarse a la ligera, sino que ha de ser fruto de la reflexión pausada, en pos de lograr el efectivo respeto al derecho fundamental a la protección de datos de carácter personal[243]. Ello no impide que, adoptada una decisión, esta no pueda adaptarse o mudarse si se observa que el sistema no sirve o no es adecuado para acometer la finalidad pretendida.

3.2. Planteamiento general: sistema de delegado de protección de datos interno o externo

Ahora bien, para empezar, contamos con dos posibilidades permitidas por el ordenamiento jurídico, un sistema de DPD interno, en el que el DPD forma parte de la propia organización, o un sistema de DPD externo, en el que el DPD es

(243) Así, en el Informe 0100/2019 del Gabinete Jurídico de la AEPD, de 17 de febrero de 2020, sobre la designación de DPD en el Ministerio de Defensa se asevera que *«esta Agencia debe incidir, una vez más, en la importancia que la figura del DPD tiene en el nuevo modelo instaurado por el RGPD y que pivota sobre la base de la responsabilidad proactiva del responsable»*.

ajeno a la organización. La decisión no puede verse influida por la protección laboral dispensada a los DPDs internos(244).

Debemos partir del artículo 37.6 del RGPD que permite que el DPD forme parte de la plantilla del responsable o del encargado del tratamiento o desempeñe sus funciones el marco de un contrato de servicios.

Tanto el sistema de DPD interno como el de DPD externo cuentan con múltiples variantes que pueden ser estudiadas, para estimar por parte del responsable del tratamiento cuál puede ser más idónea para su organización.

3.3. Planteamiento general: persona física o persona jurídica

Del RGPD parece deducirse *a priori* que el DPD es una persona física(245). Así se induce cuando el considerando 97 se refiere a personas que pueden ser o no empleados del responsable del tratamiento. También, en el artículo 30 del RGPD se indica que en el registro de actividades de tratamiento debe constar *«el nombre y los datos de… del delegado de protección de datos»;* de igual forma en las notificaciones de violaciones de la seguridad de los datos personales, artículo 33.2.b) del RGPD, se requiere la comunicación del nombre y datos de contacto del DPD; o la mención específica de la prohibición o destitución del DPD por el cumplimiento de sus funciones hace de nuevo rememorar a una persona física.

Esta visión se refuerza con la referencia que el Grupo de Trabajo del Artículo 29 realiza a las «cualidades personales» que debe ostentar el DPD, cuando menciona que deben incluirse *«la integridad y un nivel elevado de ética profesional»*(246), que son privativas de las personas físicas.

Mas esta cuestión es claramente controvertida, ya que, por otro lado, es cierto que la referencia es genérica a una «persona», sin diferenciar sobre su naturaleza jurídica.

El propio Grupo de Trabajo del Artículo 29 nos despista de nuevo al matizar que también puede serlo una persona jurídica, al afirmar que *«la función del DPD puede ejercerse también en el marco de un contrato de servicios suscrito*

(244) *«The choice between an internal or external DPO shall not be influenced by the employment protection of internal DPOs» —«La elección entre un DPD interno o externo no puede verse influida por el sistema de protección de los DPDs internos»* (la traducción es nuestra)—, CONFEDERATION OF EUROPEAN DATA PROTECTION ORGANISATIONS (2017), CEDPO position on the DPO in the GDPR, 15 de febrero de 2017, pág. 1.

(245) ROMEO RUIZ, Aritz (2020), «La Responsabilidad Proactiva de las Administraciones Públicas en la Protección de Datos Personales», en *Revista Vasca de Gestión de Personas y Organizaciones Públicas,* núm. 18/2020, Instituto Vasco de Administración Pública, pág. 149.

(246) GRUPO DE TRABAJO DEL ARTÍCULO 29, *Directrices sobre los Delegados de Protección de Datos, WP243 rev. 01, adoptadas el 13 de diciembre de 2016, revisadas por última vez y adoptadas 5 de abril de 2017,* pág. 13.

con una persona física o con una organización ajena a la organización del responsable o del encargado del tratamiento»[247].

Y, en el mismo sentido, el artículo 35 de la LOPDGDD determina que el DPD puede ser una persona física o jurídica, cuando en referencia al artículo 37.5 del RGPD menciona las necesarias cualidades profesionales que debe ostentar.

La AEPD, tanto en su documento «El Delegado de Protección de Datos en las Administraciones Públicas» como en la Guía de Protección de Datos y Administración Local, admite la eventualidad *«de que se pueda prestar por entidades privadas especializadas»,* que, obviamente, tendrán la forma de personas jurídicas.

Eso sí, la AEPD en sus preguntas frecuentes matiza que, cuando se preste por entidades privadas especializadas *«es fundamental que cada miembro de la organización que ejerza las funciones de DPD cumpla todos los requisitos aplicables de la sección 4 del RGPD* y que se combinen *capacidades y puntos fuertes individuales para que varios individuos que trabajen en equipo puedan servir a sus clientes de forma más eficaz»*[248].

Así, todos los miembros del equipo de esa organización que ejercen las funciones de DPD deben cumplir con todos los requisitos previstos en el RGPD en cuanto a la cualificación profesional y capacidades personales suficientes, en los términos prescritos por el RGPD, aun cuando combinen *«capacidades y puntos fuertes»*.

Entre esas capacidades deben incluirse también las personales, tales como *«la integridad y un nivel elevado de ética profesional»,* las citadas por el Grupo de Trabajo del Artículo 29.

De la lectura detallada y de la reflexión deducimos que la finalidad última pretendida es dar cobertura al sistema que se establezca, cumpliendo con los requisitos del RGPD, para cobijar las funciones propias de la figura del DPD, de la manera más efectiva y eficaz para garantizar el derecho fundamental.

No es tanto la vía o la estructura elegida, sino visibilizar un conjunto variopinto de posibilidades, que permitan auxiliar al responsable del tratamiento nombrar a un DPD procurando el cumplimiento efectivo de la normativa de protección de datos.

(247) GRUPO DE TRABAJO DEL ARTÍCULO 29, *Directrices sobre los Delegados de Protección de Datos, WP243 rev. 01, adoptadas el 13 de diciembre de 2016, revisadas por última vez y adoptadas 5 de abril de 2017,* pág. 13.

(248) Preguntas frecuentes de la AEPD, recuperado el 15 de noviembre de 2020 de https://sedeagpd.gob.es/sede-electronica-web/vistas/infoSede/detallePreguntaFAQ.jsf?idPregunta=FAQ%2F00064
GRUPO DE TRABAJO DEL ARTÍCULO 29, *Directrices sobre los Delegados de Protección de Datos, WP243 rev. 01, adoptadas el 13 de diciembre de 2016, revisadas por última vez y adoptadas 5 de abril de 2017,* pág. 13.

4.3.11. Funciones en relación con las violaciones de la seguridad de los datos personales

Una de las funciones nuevas y esenciales del DPD es la contribución en la gestión de las violaciones de la seguridad de los datos personales o brechas de datos personales(661).

Comprende su participación en todo el proceso que se desarrolle al efecto, incluyendo su colaboración respecto del registro documental de las incidencias, en la notificación a las autoridades de control y en la eventual comunicación a los interesados.

El DPD deberá estar implicado tanto en los procesos iniciales de detección y categorización de la brecha, a través de sus actividades de asesoramiento y supervisión, como en el proceso de respuesta y contención de la brecha de datos personales, así como en la notificación a las autoridades de control y la comunicación a los interesados, en su caso(662).

Deberá coordinarse con el responsable del tratamiento y con el encargado del tratamiento, en su caso, así como con otras figuras que tengan responsabilidad atribuida en la gestión de las brechas de datos personales, como, por ejemplo, los responsables de la seguridad del ENS(663).

---

(661) El DPD se encarga solo de las violaciones de la seguridad de los datos personales que incumban a datos de carácter personal. En este sentido, la Guía para la notificación de brechas de datos personales de la AEPD, aclara que no todos los incidentes de seguridad son violaciones de la seguridad de los datos personales; asimismo determina que una brecha de datos personales: *«El RGPD define, de un modo amplio, las "brechas de datos personales" como "todas aquellas violaciones de la seguridad que ocasionen la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos". No tendrán consideración de brecha de datos personales sujetas a los artículos 33 y 34 del RGPD aquellos incidentes que: — No afecten a datos personales, es decir, a datos que no sean de personas físicas identificadas o identificables. — No afecten a tratamientos de datos personales llevados a cabo por un responsable o un encargado. — Ocurran en tratamientos llevados a cabo por una persona física en el ámbito doméstico. Por lo tanto, no todos los incidentes de seguridad son necesariamente brechas de datos personales y no solo los ciberincidentes pueden ser brechas de datos personales. A su vez, no toda acción que suponga una vulneración de la normativa de protección de datos puede ser considerada una brecha de datos personales»,* pág. 8.

(662) *«Estos factores significan que el DPD debe desempeñar un papel clave a la hora de ayudar a prevenir una violación o a prepararse proporcionando asesoramiento y supervisión del cumplimiento, así como durante una violación (es decir, cuando se notifica a la autoridad de control) y durante cualquier investigación posterior por parte de la autoridad de control. En este sentido, el CEPD recomienda que el DPD sea informado con rapidez de la existencia de una violación y que participe en todo el proceso de gestión y de notificación de la misma»,* Directrices 9/2022 del CEPD, sobre la notificación de las violaciones de la seguridad de los datos personales en el marco del RGPD, Versión 2.0, adoptadas el 28 de marzo de 2023, pág. 31

(663) La gestión de las brechas de datos personales requiere la intervención del DPD y de los responsables de la seguridad, quienes actuarán conjuntamente y coordinados, cada uno realizando sus respectivas funciones: *«El delegado de protección de datos tiene el papel*

Resulta clave que el responsable del tratamiento ponga las brechas de datos personales en conocimiento de todos los órganos ante quien corresponda(664), incluyendo, en su caso, a las autoridades de control en los términos de los artículos 33 y 34 del RGPD; mas lo que a nosotros atañe es la intervención en tal proceso del DPD. La responsabilidad recae, por tanto, en el responsable del tratamiento y no en el DPD.

En este contexto, la concienciación de lo que constituye una violación de la seguridad de los datos personales, constituye el paso obligado para evitarla, fomentando la prevención. Y ello en atención a las consecuencias que el considerando 85 del RGPD dispone respecto de las brechas de datos personales si no se adoptan las medidas apropiadas, en relación con la materialización de los riesgos previstos en el considerando 75 del RGPD.

Tal labor debe desarrollarla el DPD de manera conjunta con el responsable o encargado del tratamiento. Máxime, cuando, al hablarse de violaciones de la seguridad de los datos personales, siempre se considera a las relacionadas con las tecnologías de la información y las telecomunicaciones(665), y en raras ocasiones se asocia con otro tipo de violaciones relacionadas con brechas físicas (por ejemplo, robo en instalaciones administrativas de expedientes en papel que contengan datos personales). También en esas últimas debe hacer hincapié el DPD.

En relación con la gestión de las brechas de datos personales, obligatoria es la mención a la política de protección de datos que debe desarrollarse a través de otros instrumentos que contengan medidas concretas de evitación, detección y contención de las violaciones de la seguridad de los datos personales.

En las administraciones públicas es preciso desarrollarlo elaborando lo que se denomina como «procedimiento de respuesta a incidentes». Tanto la política de protección de datos, la política de seguridad de la información, como el procedimiento de respuesta a violaciones de la seguridad de los datos personales que para cada tratamiento se aprueben, deben conocerse oportunamente por el DPD, por los responsables de seguridad y por el resto de los empleados públicos que puedan verse implicados en la brecha de datos personales, pues de su conocimiento se infiere la correcta detección y gestión de la brecha.

---

de*supervisar la licitud de los tratamientos informando y asesorando al responsable; por su parte el responsable de seguridad es la persona encargada de supervisar los controles necesarios para proteger los datos y controlar su eficacia*». En tal sentido se manifiesta en la Guía para la gestión y notificación de brechas de seguridad de la AEPD, INCIBE y CCN-CERT, págs. 9 y 10.

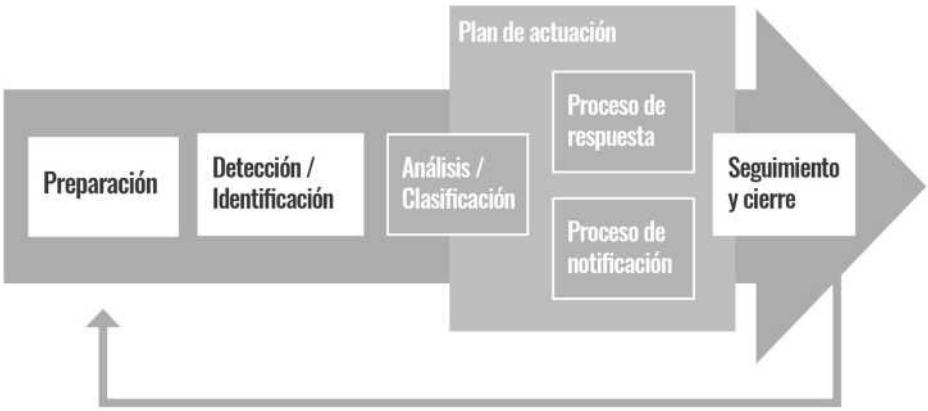
(664) La gestión y notificación de las violaciones de la seguridad de los datos personales es más compleja de lo que aparenta. El marco normativo existente no se limita a imponer obligaciones en relación con la AEPD, sino que comprende otro tipo de actuaciones que involucran a otros organismos como el CCN-CERT.

(665) AEPD (2020), *Brechas de seguridad: el correo electrónico y las plataformas de productividad online*, en Blog de la AEPD.

El procedimiento de respuesta a brechas de datos personales está relacionado de forma directa con el análisis de riesgos y, en su caso, con la EIPD y las conclusiones que de tal análisis se deriven, las cuales impongan la adopción de medidas adecuadas y eficaces en relación con el tratamiento de los datos personales, incluyendo lo relativo a la seguridad de los datos personales.

Lo primero que debemos definir son las fases que conforman el proceso de gestión de las brechas de datos personales.

La Guía para la gestión y notificación de brechas de seguridad de la AEPD, en la que ha colaborado el INCIBE y el CCN-CERT, mostró la estructura temporal más usual en el proceso de administración de estas. Así, del proceso de gestión de brechas de seguridad es un ciclo cerrado que comprende la preparación del propio proceso de gestión, la detección e identificación de la incidencia y su posterior análisis y clasificación, la posterior respuesta y notificación y el cierre y posterior seguimiento de la incidencia que se engarza con la actualización y preparación del proceso de gestión(666).



Fases de actuación en una brecha de datos personales(667).

Hemos de considerar que el DPD actúa en todas las fases antedichas, desde la detección de violaciones de la seguridad de los datos personales, pasando por su análisis, por la respuesta y las medidas de contención, hasta la determinación de la obligatoriedad de su notificación a la autoridad de control y, en su caso, la comunicación a los interesados; sin olvidarnos de las recomendaciones sobre

(666) Estas fases son comunes para la gestión de todo tipo de incidentes: preparación; detección, análisis y notificación; contención, erradicación y recuperación; actividad posterior. Así se consigna, por ejemplo, para la gestión de ciberdelincuentes, en la *Guía de Seguridad de las TIC CCN-STIC 817 sobre Esquema Nacional de Seguridad Gestión de Ciberdelincuentes del CCN-CERT,* pág. 10.

(667) AEPD, INCIBE y CCN-CERT (2018), *Guía para la gestión y notificación de brechas de seguridad, de 22 de junio de 2018*, pág. 11.

la adopción de las medidas técnicas y organizativas apropiadas de todo tipo, incluyendo las de seguridad, precisas para restaurar, corregir la situación y evitar que no vuelva a acontecer, que deben estar alineadas con los requisitos de seguridad precisos para procurar la seguridad de los derechos y libertades de los ciudadanos.

Centrémonos ahora en una fase previa y de preparación no citada en el ciclo anterior.

No podemos dejar de indicar que la mejor violación de la seguridad de los datos personales es la que nunca llega a producirse. La prevención en protección de datos es la clave absoluta de todo, requiriéndose para su consecución involucrar a todo el personal de la organización. De nuevo hemos de traer a colación el enfoque de riesgos y la protección de datos desde el diseño que extienden su onda expansiva también en el ámbito de la seguridad de los datos.

Por eso, la primera «fase» de una violación de la seguridad de los datos personales es preventiva, de concienciación, de formación y de implicación activa del responsable del tratamiento, y, por ende, de sus empleados.

Una violación de la seguridad de los datos personales empieza a evitarse y corregirse antes de que se produzca.

Tengamos en consideración que cuando se piensa en riesgos y en brechas de datos personales se suele asociar a riesgos externos, debiendo observarse también los internos de la organización.

Durante la vigencia de la LOPD y del RLOPD las medidas de seguridad establecidas para un fichero se contenían en el documento de seguridad, en los términos que preveía el artículo 88 y siguientes del RLOPD.

Este documento debía ser puesto en conocimiento de los empleados por parte del entonces responsable del fichero a los efectos de que supieran qué hacer y qué no hacer en relación con las medidas de seguridad impuestas y cómo reaccionar ante una vulneración de la seguridad. Mas la realidad contrastada en las administraciones públicas era que, salvo contados y muy excepcionales ejemplos, no solo el contenido del documento de seguridad elaborado era desconocido por los empleados de la organización, sino también la existencia del documento mismo. De esa manera resultaba imposible implementar la prevención y gestionar cualquier vulneración de la seguridad. Y todo ello amén de que, en la mayoría de los supuestos, dado que el sistema era prescriptivo y basado en la tipología de datos personales y no en el nivel de riesgo del tratamiento, amén de que solo contemplaba medidas de seguridad estandarizadas (y no medidas de todo tipo como ahora), se limitaban a transcribir las medidas de seguridad previstas en el RLOPD, de tal forma que lo que tenía que ser un sistema de mínimos se convirtió en un sistema de máximos con dispar funcionalidad.

Manual práctico para designar e integrar al delegado de protección de datos en cualquier administración pública a través de un modelo tipo que puede adaptarse a la organización, la idiosincrasia y las necesidades específicas de cualquiera de ellas.

Partiendo de las obligaciones fijadas en el Reglamento General de Protección de Datos la obra trasciende de la teoría para descender a problemas reales, habituales y recurrentes de las administraciones públicas ofreciendo soluciones concretas, susceptibles de ser aplicadas de forma inmediata, para solventarlos.

Destinada a todo tipo de administraciones públicas y extrapolable tanto al sector público como al privado, expone la nueva visión del derecho fundamental a la protección de datos de carácter personal desde la perspectiva del delegado de protección de datos. Centrándose en el nuevo enfoque del Reglamento General de Protección de Datos, facilita, además, la comprensión y el cumplimiento efectivo de esta norma en su conjunto al responsable y al encargado del tratamiento.

ISBN: 979-13-990682-4-5

EL CONSULTOR DE LOS AYUNTAMIENTOS