

Revista Internacional y Comparada de

**RELACIONES
LABORALES Y
DERECHO
DEL EMPLEO**

Escuela Internacional de Alta Formación en Relaciones Laborales y de Trabajo de ADAPT

Comité de Gestión Editorial

Alfredo Sánchez-Castañeda (*México*)

Michele Tiraboschi (*Italia*)

Directores Científicos

Mark S. Anner (*Estados Unidos*), Pablo Arellano Ortiz (*Chile*), Lance Compa (*Estados Unidos*), Jesús Cruz Villalón (*España*), Luis Enrique De la Villa Gil (*España*), Jordi Garcia Viña (*España*), Adrián Goldin (*Argentina*), Julio Armando Grisolia (*Argentina*), Óscar Hernández (*Venezuela*), María Patricia Kurczyn Villalobos (*México*), Lourdes Mella Méndez (*España*), Antonio Ojeda Avilés (*España*), Barbara Palli (*Francia*), Juan Raso Delgue (*Uruguay*), Carlos Reynoso Castillo (*México*), Raúl G. Saco Barrios (*Perú*), Alfredo Sánchez-Castañeda (*México*), Malcolm Sargeant (*Reino Unido*), Michele Tiraboschi (*Italia*), Anil Verma (*Canada*), Marcin Wujczyk (*Polonia*)

Comité Evaluador

Fernando Ballester Laguna (*España*), Francisco J. Barba (*España*), Ricardo Barona Betancourt (*Colombia*), Esther Carrizosa Prieto (*España*), M^a José Cervilla Garzón (*España*), Henar Álvarez Cuesta (*España*), Juan Escribano Gutiérrez (*España*), Rodrigo Garcia Schwarz (*Brasil*), José Luis Gil y Gil (*España*), Sandra Goldflus (*Uruguay*), Djamil Tony Kahale Carrillo (*España*), Gabriela Mendizábal Bermúdez (*México*), María Ascensión Morales (*México*), Juan Manuel Moreno Díaz (*España*), Pilar Núñez-Cortés Contreras (*España*), Eleonora G. Peliza (*Argentina*), Salvador Perán Quesada (*España*), María Salas Porras (*España*), José Sánchez Pérez (*España*), Esperanza Macarena Sierra Benítez (*España*)

Comité de Redacción

Omar Ernesto Castro Güiza (*Colombia*), María Alejandra Chacon Ospina (*Colombia*), Silvia Fernández Martínez (*España*), Paulina Galicia (*México*), Noemi Monroy (*México*), Juan Pablo Mugnolo (*Argentina*), Lavinia Serrani (*Italia*), Carmen Solís Prieto (*España*), Francesca Sperotti (*Italia*), Marcela Vigna (*Uruguay*)

Redactor Responsable de la Revisión final de la Revista

Alfredo Sánchez-Castañeda (*México*)

Redactor Responsable de la Gestión Digital

Tomaso Tiraboschi (*ADAPT Technologies*)

El delegado de protección de datos en la industria 4.0: funciones, competencias y las garantías esenciales de su estatuto jurídico

Esperanza Macarena SIERRA BENÍTEZ*

RESUMEN: El nuevo Reglamento (UE) 2016/679 relativo a la protección de las personas físicas respecto al tratamiento y circulación de datos personales regula la “nueva” figura del delegado de protección de datos (DPO por sus siglas en inglés). Aunque esta figura no es novedosa porque ya se instauró en el Reglamento 45/2001, la diferencia radica en que se instaura tanto en el ámbito del sector público como privado, exigiendo que el DPO tenga unos conocimientos especializados de la legislación y la práctica en materia de protección de datos, y que esté capacitado para ejecutar los cometidos del Reglamento. El nuevo reglamento tiene efectos directos y obliga a todos los Estados miembros a interpretar de forma similar la regulación en torno a la designación, posición y funciones del delegado de protección de datos, y exige que el DPO se designe atendiendo a sus cualidades profesionales y conocimientos especializados en la Industria 4.0. En este trabajo abordaremos además cuestiones laborales relacionadas con las funciones y competencias del delegado de protección de datos cuando se trate de una persona física: la dependencia jurídico-económica (en el caso de ser un trabajador interno) y la dependencia económica con el responsable del tratamiento (en el caso de ser DPO externo).

Palabras clave: Delegado de protección de datos, industria 4.0, dependencia jurídica y dependencia económica.

SUMARIO: 1. Nuevas profesiones y competencias digitales en la industria 4.0. 2. La “nueva” figura del *data protection officer* (DPO) en el Reglamento UE 2016/679. 2.1. La designación del delegado de protección de datos. 2.2. La cualificación y las competencias del delegado de protección de datos. 2.3. Funciones del DPO. 2.4. Posición del delegado de protección de datos. 3. Las garantías esenciales del estatuto jurídico del DPO, en especial la garantía de indemnidad. 4. Conclusiones. 5. Bibliografía.

* Profesora contratada Doctora de Derecho del Trabajo y de la Seguridad Social. Universidad de Sevilla (España).

The data protection officer in Industry 4.0: functions, competences and the essential guarantees of its legal status

ABSTRACT: The new Regulation (EU) 2016/679 on the protection of individuals regarding the processing and circulation of personal data regulates the “new” figure of the data protection officer (DPO). Although this job position is not new because it was already established in Regulation 45/2001, the difference now is that it affects both the public and private sector, requiring that the DPO has specialized knowledge of the legislation and practice in data protection matter, and is able to perform the tasks described in the Regulation. The new regulation has direct effects and obliges all Member States to interpret in a similar way matters regarding the designation, position and functions of the data protection officer, and requires that the DPO be designated according to their professional qualities and specialized knowledge in Industry 4.0. In this paper we will also address labor issues related to the functions and powers of the data protection officer when dealing with a natural person: the legal-economic dependence (in the case of an internal worker) and the economic dependence with the person responsible for the treatment (in the case of an external DPO).

Key Words: Data protection officer, industry 4.0, legal and economic dependence.

1. Nuevas profesiones y competencias digitales en la industria 4.0

La Unión Europea (en adelante UE) cuenta cada vez con un mayor número de graduados en ciencia, tecnología, ingeniería y matemáticas (19 titulados por cada mil personas de edad comprendida entre 20 y 30 años) y de especialistas en TIC en la población activa (3'5% en 2015 frente al 3'2% en 2012). No obstante, persisten las lagunas en las competencias digitales dado que casi la mitad de los europeos (44%) no posee todavía capacidades digitales básicas, como usar el correo electrónico, las herramientas de edición, o instalar nuevos dispositivos. En concreto, actualmente el 45% de los ciudadanos y el 37% de los trabajadores europeos tienen habilidades digitales insuficientes¹. En España el porcentaje de personas que han adquirido sus habilidades en materia TIC mediante una enseñanza reglada sólo alcanza el 20'5% frente al 27'6% de la Unión Europea, el 32'0% de Francia, el 37'6% de Reino Unido o el 28'5% de Alemania².

Por otro lado, la digitalización de la mayoría de sectores productivos y la Industria 4.0 abarcan mucho más que la tecnología. Las empresas deben estar preparadas para experimentar cambios radicales debido a diversos factores, entre los que se encuentra la necesidad de contar con competencias nuevas y actualizadas junto con nuevas formas de trabajar³. En España, según un reciente informe, la transformación digital ha despertado en las organizaciones la necesidad de alcanzar el nivel competitivo imprescindible en términos digitales y de innovación para adecuar el modelo de negocios a los nuevos hábitos de los consumidores y, por consiguiente, en la elaboración de programas de capacitación integral en innovación digital con el objetivo de formar a sus empleados y directivos⁴. Concretamente en el año 2016 el mercado de las Tecnologías de la Información (TI) creció un 3'3%, respecto al año anterior, alcanzando los 23.441 millones de euros. En lo que respecta al empleo en este mismo sector, el dato también es positivo con un aumento en la

¹ Comisión Europea. Comunicado de prensa, Bruselas, 3 de marzo de 2017, http://europa.eu/rapid/press-release_IP-17-347_es.htm.

² Ministerio de Industria, Energía y Turismo, *Informe Anual 2016 de la Agenda Digital para España*, julio 2016 en <http://www.agendadigital.gob.es/Seguimiento/InformesAnuales/Informes/2016/Informe-anual-ADpE-2016.pdf>.

³ Véase el Dictamen del Comité Económico y Social Europeo sobre el tema "Industria 4.0 y transformación digital: camino a seguir", [COM(2016) 180 final], DOUE de 21 de octubre 2016, C 389.

⁴ IEBS, Business School, *Transformación digital en las empresas* en <http://static.iebschool.com/17/pdf/estudio-transformacion-digital-IEBS.pdf>.

contratación de un 2'8%.

Con carácter general, los procesos de transformación digital en el ámbito de las empresas han sido los principales responsables del aumento de la actividad TI, y muy especialmente la de los Servicios TI (en concreto, los sectores de finanzas, energía e industria). En materia de empleo en ese mismo año la cifra de empleados directos superó los 200.000. El empleo en el sector TI mantiene sus características de calidad y estabilidad superior al del conjunto del tejido productivo, pero también los desequilibrios en algunos perfiles muy demandados por el sector para los que la oferta de profesionales es insuficiente⁵. En España se espera que en el año 2021 la aceleración digital impulsará un 3'6% el PIB, pero para ello serán necesarias actuaciones por parte de las empresas y las administraciones públicas a través de un programa centrado en tres palancas: talento, inversión en tecnología y aceleradores. En el primer caso es necesario generar talento digital en las universidades y capturarlo en las empresas (nuevas formas de trabajo, aumentar los equipos dedicados a la innovación, etc.)⁶; en el segundo caso, las línea de acción se centrarían en digitalizar la relación con el cliente, impulsar la colaboración en la empresa con herramientas digitales e incrementar la inversión en tecnologías como la nube (*cloud*), la analítica avanzada, la inteligencia artificial, IoT, movilidad o *social media*. Y, en el tercer caso, entre los aceleradores que impulsen la digitalización se citan el despliegue de una infraestructura de comunicaciones a la altura de los líderes digitales, la adaptación de la regulación a las nuevas tecnologías, nuevos modelos de negocio y modelos basados en la economía colaborativa, así como la potenciación

⁵ Comunicado de prensa 27 de marzo de 2017 de la Asociación Multisectorial de Empresas de la Electrónica, las Tecnologías de la Información y Comunicación, de las Telecomunicaciones y de los Contenidos Digitales (AMETIC), "El mercado de las Tecnologías de la Información en España creció un 3'3% en 2016".

⁶ En OECD, *Multilingual Summaries*, Education at a Glance 2017, OECD Indicators, Resumen en español, <http://www.oecd-ilibrary.org/docserver/download/7da6001b-es.pdf?expires=1510594243&id=id&accname=guest&checksum=8F3A95B5F6F74DA83AD0F8511BD3C0CD> según los indicadores de educación del 2017, los egresados de los campos científicos son los que tienen más posibilidades de conseguir empleo, aunque no en general. En la mayoría de los países de la OCDE los títulos universitarios más populares que ostentan los adultos son en las áreas de negocios, administración o derecho. En promedio, en la OCDE, el 23% de las personas de 25 a 64 años con educación superior tienen un título universitario en una de estas tres disciplinas en comparación, con 5% en ciencias naturales, estadísticas y matemáticas; 4% en tecnologías de la información y la comunicación; y 17% en ingeniería, manufactura y construcción. El interés en las ciencias, la tecnología y las matemáticas crece en los niveles de educación más altos. En 2015 egresó casi el doble del porcentaje de estudiantes de estos campos a nivel de doctorado que a nivel de licenciatura.

del uso de plataformas digitales y el fomento de nuevos negocios⁷.

Estos datos son importantes porque en la nueva economía, caracterizada por la digitalización del empleo (robotización, inteligencia artificial, impresión 3D, *big data*, etc.), se espera que el 90% de los puestos de trabajo requiera algún tipo de competencia digital⁸. El término *big data* hace referencia “al conjunto de tecnologías, algoritmos y sistemas empleados para recolectar datos a una escala y variedad no alcanzada hasta ahora y a la extracción de información de valor mediante sistemas analíticos avanzados soportados por computación en paralelo”⁹. Es un término que se puede definir “como un conjunto de tecnologías que permiten el almacenamiento de enormes cantidades de datos procedentes de fuentes no homogéneas en un formato no estructurado, y con un procesamiento con un elevado rendimiento”¹⁰. El concepto de *big data* “se aplica a toda la información que no puede ser procesada o analizada utilizando herramientas o procesos tradicionales. El desafío consiste en capturar, almacenar, buscar, compartir y agregar valor a los datos poco utilizados o inaccesibles hasta la fecha”¹¹.

Como señala el nuevo reglamento general sobre la protección de datos en la UE (en adelante, Reglamento 2016/679), la rápida evolución tecnológica y la globalización de la economía han planteado nuevos retos para la protección de los datos personales. La magnitud de la recogida y del intercambio de datos personales ha aumentado de manera significativa. La tecnología permite que tanto las empresas privadas como las autoridades públicas utilicen datos personales en una escala sin precedentes a la hora de realizar sus actividades. Las personas físicas difunden un volumen cada vez mayor de información personal a escala mundial. La tecnología ha transformado tanto la economía como la vida

⁷ Informe *Economía Digital. Una oportunidad para España* elaborado por Accenture Strategy para Mobile World Capital Barcelona en <http://ametic.es/es/prensa/la-aceleraci%C3%B3n-digital-impulsar%C3%ADa-un-36-el-pib-en-2021>.

⁸ Blog Fundación Europea para la Formación en el Empleo, *Competencias digitales para el futuro de Europa*, 9 de febrero 2017 en <https://blog.fundae.es/2017/02/09/competencias-digitales-para-el-futuro-de-europa/>.

⁹ Sáiz, C. (coord.), *Código de buenas prácticas en protección de datos para proyectos big data*, editado por la AEDP y ISMS Forum Spain en https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/2017/Guia_Big_Data_AEPD-ISMS_Forum.pdf, pág. 8.

¹⁰ Salgueiro, J.M., “Big Data, ¿amenaza u oportunidad para la gestión de la seguridad?”, *Red seguridad: revista especializada en seguridad informática, protección de datos y comunicaciones*, n. 78, 2017, p. 40.

¹¹ Gil, E., *Big data, privacidad y protección de datos*, Agencia Española de Protección de Datos, Agencia Estatal Boletín del Estado, Madrid, 2016, p. 18.

social, y ha de facilitar aún más la libre circulación de datos personales, pero garantizando al mismo tiempo un elevado nivel de protección de esos mismos datos.

Estos avances requieren un marco más sólido y coherente para la protección de datos en la UE, respaldado por una ejecución estricta, dada la importancia de generar la confianza que permita a la economía digital desarrollarse en todo el mercado interior. Las personas físicas deben tener el control de sus propios datos personales. Hay que reforzar la seguridad jurídica y práctica para las personas físicas, los operadores económicos y las entidades públicas. En este sentido, la normativa de la UE menciona que el responsable o el encargado del tratamiento deben contar con la ayuda de una persona con conocimientos especializados en Derecho y con experiencia práctica en materia de protección de datos si el tratamiento lo realiza una autoridad pública. En el sector privado, las actividades principales de un responsable están relacionadas con sus actividades primarias y no están relacionadas con el tratamiento de datos personales como actividades auxiliares. El nivel necesario de conocimientos especializados se debe determinar, en particular, en función de las operaciones de tratamiento de datos personales tratados por el responsable o el encargado. Tales delegados de protección de datos, sean o no empleados del responsable del tratamiento, deben estar en condiciones de desempeñar sus funciones y cometidos de manera independiente¹². En nuestro trabajo vamos a tratar las funciones y competencias de esta nueva figura: el delegado de protección de datos, designado por el responsable y el encargado de tratamientos de datos, regulada en el nuevo Reglamento 2016/679 de la UE. Esta norma de efecto directo, y que entra en vigor en mayo de 2018, tiene como objetivo principal la modernización de los principios de privacidad en la UE, reconociendo nuevos derechos como el derecho al olvido digital y la portabilidad de datos, así como la superación de la fragmentación de la normativa existente ocasionada por la transposición a las legislaciones nacionales sobre protección de datos de la Directiva de 1995¹³.

¹² Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a 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), DOUE 4 de mayo 2016, L 119. Considerandos 6, 7 y 97.

¹³ Díaz Díaz, E., “El «Data Protection Officer» (DPO) en el nuevo Reglamento General de Protección de Datos”, *El Derecho.com. Lefebvre. El Derecho*, 25 de abril de 2016, en http://tecnologia.elderecho.com/tecnologia/privacidad/Protection-Officer-DPO-Reglamento-Proteccion-Datos-UE_11_945055002.html.

Con ello se persigue reforzar el derecho fundamental a la protección de datos de acuerdo con las nuevas realidades tecnológicas. Sin embargo, “más que novedades introducidas por el Reglamento europeo se debería hablar de en qué forma se consiguen los objetivos perseguidos de uniformizar la normativa europea y reforzar el derecho fundamental a la protección de datos de los ciudadanos”¹⁴. El modelo que se incorpora es un modelo bien distinto “al que estábamos acostumbrados en España: una regulación bastante concreta y clara, con un listado bien definido de obligaciones jurídicas, organizativas y técnicas, así como un compendio taxativo de incumplimientos que nos permitían conocer específicamente las sanciones leves, graves o muy graves. Ahora pasamos a una nueva legislación más centrada en la persona y en que se garanticen resultados para su protección según la naturaleza del tratamiento” y a un régimen sancionador importante pero con márgenes muy amplios para su graduación¹⁵.

2. La “nueva” figura del *data protection officer* (DPO) en el Reglamento UE 2016/679

Como ha advertido la doctrina, la figura del DPO no es novedosa ya que se encontraba regulada en el Reglamento 45/2001 que contemplaba la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos¹⁶. Esta norma obliga a cada institución y organismo comunitario al nombramiento al menos de una persona para que actúe como responsable de la protección de datos, asesorando a los responsables del tratamiento en el ejercicio de sus obligaciones y debiendo velar por que el tratamiento no tenga efectos adversos sobre los derechos y las libertades de los interesados¹⁷. En realidad, la “novedad” de la figura

¹⁴ Davara Rodríguez, M.A., “El Delegado de Protección de Datos en los ficheros y/o tratamientos de la Administración en consonancia con el Reglamento Europeo de Protección de Datos”, *Actualidad Administrativa*, n. 1, 2017, La Ley 9650/2016, p. 3.

¹⁵ Judel Meléndrez, M.Mª, “La formación, clave para el DPD”, *Red seguridad. Revista especializada en seguridad de la información*, n. 76, 2017, p. 63.

¹⁶ Reglamento (CE) nº 45/2001 del Parlamento Europeo y del Consejo de 18 de diciembre de 2000 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos (DOCE L8 de 12.1.2001).

¹⁷ Davara Rodríguez, M.A., “El Delegado de Protección de Datos en los ficheros y/o tratamientos de la Administración en consonancia con el Reglamento Europeo de Protección de Datos”, *op. cit.*, p. 10. Esta norma se publica en el DOUE L núm. 8 de 12

del delegado de protección de datos es la obligatoriedad de su implantación en todos los Estados Miembros en un ámbito de aplicación más amplio que el de las instituciones y organismos de la UE como viene contemplado en el Reglamento 45/2001¹⁸.

En España nuestra normativa de protección de datos no contempló esta posibilidad como sí lo hicieron, por ejemplo, la Húngara y la Alemana puesto que la regulación europea, la derogada Directiva 95/46/CE¹⁹, no exigía su establecimiento a ninguna organización²⁰, por lo que en otros países como Holanda o Austria su nombramiento era opcional, y en otros como España no se exigía con anterioridad a la entrada en vigor del nuevo Reglamento UE 2016/679 de 25 de mayo de 2018²¹. No obstante, esta figura coincide funcionalmente con lo que la normativa española de desarrollo de la LO 15/1999, de 13 de diciembre, de protección de datos de carácter personal (LOPD de 1999) denominó “responsable de seguridad”, definido como la “persona o personas a las que el responsable del fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables” (art.5.2.i)²².

Como señala la doctrina, el problema que planteó esta regulación que desarrolló la LOPD es que no fue acompañada de una definición que incorporase un perfil profesional claro del responsable de seguridad ni las capacidades y las competencias teóricas necesarias o, en su caso, la titulación homologable exigible. La realidad es que no existía una

de enero 2016.

¹⁸ Recio Gayo, M., “Directrices del GT29 sobre el delegado de protección de datos. Figura clave para la responsabilidad «accountability»”, *Diario La Ley*, n. 2, 2017, La Ley 185/2017, p. 3.

¹⁹ Directiva 95/46/CE, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (DOUE n° L281 de 23 de noviembre de 1995. Esta figura venía contemplada para poder aplicar la simplificación o la omisión a la obligación de notificación de tratamientos o ficheros a la autoridad de control o supervisión.

²⁰ Grupo de Trabajo del artículo 29 sobre protección de datos, (16/EN GT 243), Directrices sobre los delegados de protección de datos (DPD), adoptado el 13 de diciembre de 2016. La figura apareció en Alemania, en 1977, con la Ley Federal de Protección de Datos.

²¹ Rodríguez Ballano, S. y Vidal, M., “Habemus nuevo Reglamento General de Protección de Datos”, *Actualidad Jurídica Aranzadi*, n. 919, 2016 parte Comentario, BIB 2016/3116, p. 1.

²² RD 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (BOE 19 enero de 2008, texto consolidado a 8 de marzo de 2012). En el art. 95 se prevé que en el Documento de seguridad deberán designarse uno o varios responsables de seguridad encargados de coordinar y controlar las medidas definidas en el documento de seguridad.

titulación curricularmente homologable al 100% (las más próxima eran las de diversas ramas de informática) y, pese a las solicitudes en ese sentido no se realizó una definición de la figura que incorporase un perfil profesional claro²³. Este dato es importante, porque precisamente la diferencia entre el responsable de seguridad y el DPO es que éste último tiene atribuida sus funciones en exclusividad. “El DPO ya no será, como hasta ahora, la persona que se designaba como Responsable de Seguridad ocurriendo que, sin apenas justificación, se elegía a profesionales sin la adecuada capacitación. El DPO será designado atendiendo a sus cualidades profesionales y, en particular, a *sus conocimientos especializados de la legislación y las prácticas en materia de protección de datos*, y a su capacidad para ejecutar los cometidos contemplados en el Reglamento”²⁴.

En la actualidad la Agencia Española de Protección de Datos (AEPD), en colaboración con la Entidad Nacional de Acreditación (ENAC) y la participación de un Comité Técnico de Expertos (representantes de sectores, asociaciones profesionales, empresariales, universidades y Administraciones Públicas), ha elaborado el Esquema de Certificación de Delegados de Protección de Datos basado en la norma ISO 17024 (requisitos generales para los organismos que realizan certificación de personas). Este sistema de certificación ofrece seguridad y fiabilidad a los profesionales de la privacidad, las empresas y entidades que incorporen esta figura a sus organizaciones, a través de un mecanismo que permite certificar que los Delegados reúnen la cualificación profesional y los conocimientos requeridos, si bien es cierto que esta certificación no es obligatoria para ejercer como Delegado²⁵. Esta obligatoriedad sólo se contempla en los supuestos regulados por el Reglamento, por lo que se debe entender que su implantación será voluntaria para el responsable y el encargado del tratamiento, que son los que designan a los DPO, con el fin de velar por el cumplimiento legal y técnico en las entidades²⁶.

Como hemos afirmado más arriba el DPO, según el Reglamento

²³ Rallo Lombarte, A. y García Mahamut, R., *Hacia un nuevo derecho europeo de protección de datos*, Tirant lo Blanch, Valencia, 2015, p. 560.

²⁴ Díaz Díaz, E., “El nuevo Reglamento de Protección de Datos de la Unión Europea y sus consecuencias jurídicas para las instituciones”, *Revista Aranzadi Doctrinal*, n. 6, 2016, parte estudio, BIB 2016/3067, p. 21; López Álvarez, L.F., *Protección de datos personales: adaptaciones necesarias al nuevo Reglamento europeo*, *op. cit.*, p. 47.

²⁵ AEPD, *Esquema de certificación de delegados de protección de datos de la Agencia Española de Protección de Datos (Esquema AEPD-DPD)*, redactado por la Unidad de Evaluación y Estudios Tecnológicos de la Agencia Española de Protección de Datos, 2 de octubre de 2017. Versión 1.1.

²⁶ Díaz Díaz, E., *El «Data Protection Officer» (DPO) en el nuevo Reglamento General de Protección de Datos*, *op. cit.*, p. 2.

2016/679, debe ejercer sus funciones con exclusividad, por lo que encontramos un elemento diferenciador importante con el responsable de seguridad. La nueva regulación exige que el DPO sea un profesional capacitado y que sea asignado en virtud de sus cualidades profesionales “y, en particular, a sus conocimientos especializados de la legislación y las prácticas en materia de protección de datos, y su capacidad para ejecutar los cometidos contemplados en el Reglamento”. (...) Por lo que “el DPO no será la persona designada como Responsable de Seguridad sin la adecuada capacitación²⁷”. Por este motivo no hay que confundir al Responsable de seguridad con el DPO, dado que supone un reforzamiento de aquél²⁸. Recientemente se ha presentado en España en el Congreso de los Diputados el Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal que recoge la figura del DPO en los mismos términos que el Reglamento (UE) 2016/679, en el sentido de que su designación puede tener carácter obligatorio o voluntario, estar o no integrado en la organización del responsable o encargado y ser tanto una persona física como una persona jurídica²⁹. Por último, llama la atención que la única definición del DPO no viene ni contemplada en el Reglamento UE 2016/679 ni el PLOPD, sino en un documento de trabajo sobre la evaluación de impacto relativo a la propuesta de Reglamento que lo define como “una persona responsable en el seno de un responsable o un encargado del tratamiento para supervisar y monitorear de una forma independiente la aplicación interna y el respecto de las normas sobre protección de datos. El DPO puede ser tanto un empleado como un consultor externo”³⁰.

A continuación vamos a ver los aspectos relacionados con la designación atendiendo a la regulación del Reglamento UE 2016/679, teniendo en cuenta que existen unas Directrices sobre los DPO adoptadas el 13 de diciembre de 2016 por el Grupo de trabajo sobre protección de datos del Artículo 29 (en adelante GT29) y que tienen como objetivo “aclarar las disposiciones del RGPD con el fin de ayudar a los responsables y encargados del tratamiento a cumplir con la legislación y también ayudar

²⁷ Díaz Díaz, E., *El «Data Protection Officer» (DPO) en el nuevo Reglamento General de Protección de Datos*, *op. cit.*, p. 5.

²⁸ Díaz Díaz, E., *El «Data Protection Officer» (DPO) en el nuevo Reglamento General de Protección de Datos*, *op. cit.*, p. 6.

²⁹ Exposición de motivos IV Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal (BOCG, Serie A, núm. 13-1 de 24 de noviembre de 2017).

³⁰ Recio Gayo, M., “Directrices del G29 sobre el delegado de protección de datos: figura clave para la responsabilidad («accountability»), *op. cit.*, p. 3, traducción literal de Commission Staff Working Paper, Impact Assessment, SEC (20129 72 final), Brussels.

al DPD en el desempeño de su labor³¹.

2.1. La designación del delegado de protección de datos

Como hemos visto, el DPO debe designarse en virtud de sus cualidades profesionales y conocimientos especializados de la legislación y las prácticas en materia de protección de datos. En España esta figura ha levantado muchas expectativas por la oportunidad de empleo de estos profesionales³², puesto que se espera que sea una de las profesiones más demandadas durante el año 2018³³. La designación del DPO corresponde al responsable y el encargado del tratamiento que deben de hacerlo siempre que: a) el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial; b) las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala; o c) las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales o de datos relativos a condenas e infracciones penales³⁴.

Algunas de las empresas que necesitarán contratar a un DPO son: colegios profesionales, centros docentes, empresas de seguridad privada, centros sanitarios, compañías de seguros, empresas de prestación de servicios de comunicaciones electrónicas y de la sociedad de la información, entidades financieras, empresas de inversión, distribuidores y comercialización de suministros energéticos, etc.³⁵. En concreto, todas aquellas entidades enumeradas en el Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal (en adelante PLOPD) de

³¹ 16/ES WP 243 rev.01 y revisadas por última vez y adoptadas el 5 de abril de 2017, p. 5.

³² López Álvarez, L.F., *Protección de datos personales: adaptaciones necesarias al nuevo Reglamento europeo*, Francis Lefebvre-El Derecho, S.A., Madrid, 2016, p. 147.

³³ Saracíbar, E., "Una profesión en alza", *Red seguridad: Revista especializada en seguridad de la Informática, protección de datos y comunicaciones*, n. 76, 2017.

³⁴ Art. 37.1 en relación con los art. 9.2 a) y 10 del Reglamento (UE) 2016/679. Estas entidades deben cumplir especiales requisitos como, por ejemplo, los relacionados con la información y el consentimiento de los interesados, que deberá ser claramente expreso y por tanto explícito.

³⁵ Blog Data, Consultoría especializada en Protección de Datos y Seguridad de la Información, *¿Qué es un DPO y quién puede contratarlo*, 4 de octubre de 2017 en <https://www.datax.es/blog-actualidad-proteccion-datos/es/dpo-quien-contratarlo/>.

conformidad con lo establecido en el Reglamento UE 2016/679. Debemos tener en cuenta que si la designación no fuera obligatoria “sería igualmente necesaria habida cuenta de la gran complejidad del nuevo escenario”, dado que “las empresas deben asumir la privacidad como piedra angular de sus negocios y adaptarse rápidamente”³⁶.

De todos modos, el propio Reglamento obliga a que exista un DPO en cada empresa u organización que emplee a más de 250 personas, a menos que el tratamiento que realice pueda entrañar un riesgo para los derechos y libertades de los interesados, no sea ocasional, o incluya categorías especiales o datos personales relativos a condenas e infracciones penales³⁷. En casos distintos a los anteriores, se podrá designar un DPO o deberá ser designado si así lo exige el Derecho de la Unión o de los Estados miembros. El DPO podrá actuar por cuenta de estas asociaciones y otros organismos que representen a responsables o encargados (art. 37.4 del Reglamento UE 2016/679)³⁸. En el supuesto de que el responsable o el encargado del tratamiento sea una autoridad u organismo público es posible designar un único DPO para varias de estas autoridades u organismos, teniendo en cuenta su tamaño y estructura organizativa. Igualmente, en el supuesto de un grupo empresarial también se puede nombrar un único DPO, siempre que sea fácilmente accesible desde cada establecimiento (arts. 37.2 y 3 Reglamento 2016/679). En este caso, la accesibilidad debe entenderse en un sentido amplio que incluya: a) la accesibilidad física para el propio personal del grupo; y b) la posibilidad de que los interesados contacten con el DPO en su lengua, aun cuando el DPO esté adscrito a un establecimiento en otro Estado Miembro³⁹. Por último, nos quedan por tratar aquellos aspectos de la designación en relación con la cualificación profesional exigida para el desempeño de las funciones que le vienen atribuidas por la norma.

³⁶ Judel Meléndrez, M.M^a, *La formación, clave para el DPD*, *op. cit.*, p. 63.

³⁷ Art. 30.5 Reglamento UE 2016/679 en relación con las obligaciones que corresponden al responsable del tratamiento y, en su caso, su representante en relación con el registro del nombre y los datos de contacto del DPO y, la del encargado y, en su caso, su representante en relación al registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de un responsable que contenga el nombre y los datos de contacto del DPO.

³⁸ El art. 37.4 delega esta designación también en las asociaciones y otros organismos que representen a categorías de responsables o encargados.

³⁹ AEPD, *Guía del Reglamento General de Protección de Datos para responsables de tratamiento*, p. 27
http://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/guia_rgpd.pdf

2.2. La cualificación y las competencias del delegado de protección de datos

El PLOPD establece que los requisitos en materia de cualificación del DPO, ya sea persona física o jurídica, podrán demostrarse, entre otros medios, a través de mecanismos voluntarios de certificación⁴⁰. La normativa no exige ninguna titulación específica, como la de Graduado en Derecho y/o otra de carácter técnico, porque la designación del candidato se realiza atendiendo a las cualidades profesionales, y en particular a los conocimientos especializados del Derecho, la práctica en materia de protección de datos y a la capacidad para desempeñar las funciones indicadas en el propio Reglamento 2016/679 (art. 37.5 Regl. 2016/679). Esto implica que “aunque no deba tener una titulación específica, en la medida en que entre las funciones del DPD se incluya el asesoramiento al responsable o encargado en todo lo relativo a la normativa sobre protección de datos, los conocimientos jurídicos en la materia son sin duda necesarios como también contar con conocimientos ajenos a lo estrictamente jurídico, como por ejemplo en materia de tecnología aplicada al tratamiento de datos o en relación con el ámbito de actividad de la organización en la que el DPD desempeña su tarea”⁴¹.

En todo caso, el nivel de conocimientos especializados necesario se debe determinar en función de las operaciones de tratamiento de datos que se realicen y de la protección exigida para los datos personales tratados⁴². En la Industria 4.0 hay una demanda de perfiles por parte de las empresas que están desarrollando las nuevas tecnologías a las que hicimos referencia más arriba (Inteligencia Artificial, IoT, *Big Data*, etc.). En el primer semestre de 2017 se ha experimentado un incremento del 50% en las ofertas de especialistas en tecnologías aplicadas a la automatización industrial dado el alto nivel de automatización de las “fábricas inteligentes”⁴³. En la Industria 4.0 se están demandando unos perfiles profesionales que no se ajustan a la preparación y/o cualificación de los candidatos para cubrir esos puestos necesarios en el mercado laboral

⁴⁰ AEPD, *Esquema de certificación de delegados de protección de datos de la agencia española de protección de datos (esquema AEPD-DPD)*, Madrid, 2 de octubre de 2017 en http://www.agpd.es/portalwebAGPD/temas/certificacion/common/pdf/ESQUEMA_AEPD_DPD.pdf.

⁴¹ AEDPD, *Guía del Reglamento General de Protección de Datos para Responsables de Tratamiento*, *op. cit.*, p. 26.

⁴² Considerando 97 del Reglamento 2017/679.

⁴³ Martín, O., “Se dispara la demanda de perfiles en la Industria 4.0”, *RRHHDigital*, 24 de noviembre de 2017.

digital⁴⁴. En el período comprendido entre los años 2015 y 2017 los puestos más solicitados en diferentes áreas han sido: estrategia digital y contenido, *social media*, *big data*, *e-commerce*, ciberseguridad y marketing. Según los expertos, los perfiles más buscados serán “los *Knowledge Workers* capaces de moverse tanto *on line* y *off line* y que fundamentalmente se diferencian de los otros por tener capacidades que los convierten en prácticamente únicos en el mercado laboral, que sean capaces de resolver problemas no rutinarios, innovar y tener pensamiento crítico”⁴⁵. En realidad, en la Industria 4.0 el DPO debería tener las siguientes cualidades profesionales: grado universitario más doctorado o máster, certificaciones reconocidas, alto nivel de inglés, experiencia en protección de datos y conocimientos especializados en derecho y conocimiento TIC (*strong skills*). Y con carácter adicional a las anteriores: pro-actividad, creatividad, asertividad, visión global, capacidad de impacto e influencia, análisis, planificación, formación continua, trabajo en equipo, accesibilidad, transversalidad, empatía y habilidades de comunicación (*soft skills*)⁴⁶.

Lo cierto es que en la actualidad son escasas las universidades y escuelas de negocios que ofertan programas formativos en Derecho y Tecnología de datos que proporcionen las competencias personales y profesionales adecuadas para el desempeño de los puestos necesarios en la Industria 4.0⁴⁷. En lo que respecta al DPO, las Directrices sobre delegados de protección de datos (DPD) del GT29⁴⁸, indican que el nivel de conocimiento debe ser acorde con la sensibilidad, complejidad y cantidad de datos que una organización trata. Por lo tanto, debe ser elegido con cuidado, teniendo debidamente en cuenta las cuestiones relativas a la protección de datos que surjan en la organización. En lo que respecta a las

⁴⁴ Por ejemplo, en materia Seguridad los CSO/Responsables de Ciberseguridad, administradores de seguridad de red, administradores de sistemas de seguridad, arquitectos de seguridad TI, responsables de seguridad y *hacking* ético, expertos en seguridad informática, consultores de seguridad en el análisis de riesgos (con cometidos específicos y competencias parecidas), en Fuentes, P., “IV. Perfiles más demandados en la actualidad (1)”, en Gil Casares, M. y Fuentes, P., *Digitalización, empleo y futuro*, Wolters Kluwer, Madrid, 2017, p. 319.

⁴⁵ *Idem*.

⁴⁶ Saracíbar, E., “Una profesión en alza”, *Red seguridad: revista especializada en seguridad de la Información*, n. 76, 2017, p. 62.

⁴⁷ La Universidad Pontificia Comillas ICAI-ICADE oferta un programa bilingüe E-3 Analytics, que combina el Grado en Análisis de negocios y el de Derecho y que ofrece la formación para el análisis de datos en la toma de decisiones en cualquier ámbito empresarial, <http://www.comillas.edu/es/grados/doble-grado-en-business-analytics-economics-and-finance-y-derecho-e-3>.

⁴⁸ Adoptadas el 13 de diciembre de 2016. Revisadas por última vez y adoptadas el 5 de abril de 2017 (16/ES WP 243 rev.01).

cualidades profesionales, un factor importante es que tenga conocimiento sobre legislación y prácticas nacionales y europeas en materia de protección de datos y una profunda comprensión del Reglamento 2016/279, del sector empresarial y de la organización del responsable del tratamiento, y un buen conocimiento de las operaciones de tratamiento y protección de datos del responsable del tratamiento.

La doctrina ha advertido que si se trata de un DPO perteneciente a “organizaciones del sector privado, además del sector de negocio, el DPO debe tener, en particular, un conocimiento profundo del modelo de negocio de la organización cuando se base en el tratamiento de datos personales para facilitar también la innovación y la competitividad de la organización al mismo tiempo que se asegura el derecho fundamental a la protección de datos personales”⁴⁹. En el caso de una autoridad u organismo público, el DPO debe también poseer un conocimiento sólido de las normas y procedimientos administrativos de la organización. En relación con la capacidad para desempeñar las funciones del DPO, las mismas Directrices del GT 29 establecen que aquélla debe interpretarse tanto en referencia a sus cualidades personales y conocimientos (como, por ejemplo, la integridad y un elevado nivel de ética profesional) como a su puesto dentro de la organización. El DPO debe posibilitar el cumplimiento del Reglamento 2016/679.

Como señalan las directrices, el DPO desempeña un papel fundamental en la promoción de una cultura de protección de datos dentro de la organización y contribuye a la aplicación de los elementos esenciales del Reglamento 2016/679, como los principios relativos al tratamiento de datos (capítulo II), los derechos de los interesados (capítulo III), la protección de los datos desde el diseño y por defecto (art. 25), el registro de las actividades de tratamiento (art.30) y la notificación y comunicación de las violaciones de la seguridad de los datos (arts. 33 y 34). En cuanto a las competencias y conocimientos específicos las Directrices incluyen: a) conocimientos especializados sobre la legislación y prácticas nacionales y europeas en materia de protección de datos y una profunda comprensión del Reglamento 2016/679; b) comprensión de las operaciones de tratamiento que se llevan a cabo; c) comprensión de las tecnologías de la información y de la organización; y d) capacidad para fomentar una cultura de protección de datos dentro de la organización⁵⁰.

En definitiva, se trata de competencias específicas que hay que sumar a la

⁴⁹ Recio Gayo, M., “Directrices del G29 sobre el delegado de protección de datos: figura clave de la responsabilidad «accountability»”, *op. cit.*, p. 6.

⁵⁰ Grupo de Trabajo sobre Protección de Datos del Artículo 29, *Directrices sobre los delegados de protección de datos (DPO)*, *op. cit.*, pp. 12, 13 y 25.

denominada competencia digital, es decir, “aquella que implica el uso creativo, crítico y seguro de las tecnologías de la información y comunicación para alcanzar los objetivos relacionados con el trabajo, la empleabilidad, el aprendizaje, el uso del tiempo libre, la inclusión y la participación en la sociedad”. En ese sentido se requieren conocimientos relacionados con el lenguaje específico básico (textual, numérico, icónico, etc.) y de las principales aplicaciones informáticas que le permitan el acceso a las fuentes y el procesamiento de la información, y el conocimiento de los derechos y las libertades que asisten a las personas en el mundo digital. Como también el desarrollo de diversas destrezas relacionadas con el acceso a la información, el procesamiento y uso para la comunicación, la creación de contenidos, la seguridad⁵¹.

2.3. Funciones del DPO

El PLOPD no contempla la regulación de las funciones del DPO en los mismos términos del art. 39 del Reglamento 2016/679, estableciendo un contenido mínimo de las funciones que corresponden al DPO (información, asesoramiento y supervisión del cumplimiento con el Reglamento así como el papel del propio delegado), art. 39.2 Reglamento 2017/679. Las directrices del GT29 están en relación con las funciones asignadas por el Reglamento: a) supervisión de la observación de Reglamento 2016/679; b) el papel de DPO en una evaluación de impacto relativa a la protección de datos; la cooperación con la autoridad de control y actuación como punto de contacto; c) enfoque basado en el riesgo; y, por último, d) el papel del DPO en el mantenimiento de registros. Como afirma el GT29 se trata de una lista de tareas mínimas de que debe encargarse el DPO, por lo que “nada impide que el responsable o el encargado del tratamiento asignen al DPO la tarea de mantener un registro de las operaciones de tratamiento bajo la responsabilidad del responsable o del encargado del tratamiento”. A fin de cuentas “el registro debe considerarse una de las herramientas que permiten al DPD realizar sus funciones de supervisión de la observancia de las normas y de información y asesoramiento al responsable o al encargado del tratamiento”⁵². Por último, como hemos indicado el PLOPD no enumera

⁵¹ Ministerio de Educación y cultura <https://www.mecd.gob.es/educacion/mc/lomce/el-curriculo/curriculo-primaria-eso-bachillerato/competencias-clave/competencias-clave/digital.html>.

⁵² Grupo de Trabajo sobre Protección de Datos del Artículo 29, *Directrices sobre los delegados de protección de datos (DPO)*, *op. cit.*, p. 21.

este listado mínimo de funciones, sino que se limita a estipular que el DPO “actuará como interlocutor del responsable o encargado del tratamiento ante la Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos” (art. 36.1). Y es que los responsables y encargados del tratamiento deben comunicar a la AEPD o, en su caso a las autoridades autonómicas de protección de datos, las designaciones, nombramientos y ceses de los DPO tanto si su designación es obligada como voluntaria (art. 34.4).

Por último, es de destacar que el responsable y el encargado del tratamiento deben facilitar los recursos necesarios para el desempeño de dichas funciones y el acceso a los datos personales y a las operaciones de tratamiento, y para el mantenimiento de sus conocimientos especializados (por ejemplo apoyo activo a la labor del DPO; tiempo suficiente para que cumpla con sus funciones; apoyo financiero, de infraestructura y de personal; comunicación oficial de la designación a todo el personal; acceso necesario a otros servicios como, por ejemplo, recursos humanos y departamento jurídico, TI, seguridad; formación continua y, en función del tamaño y estructura de la organización, puede ser necesario establecer un equipo de DPO (un DP y su personal). Estas funciones y la necesidad de dotación de recursos son elementos que tenemos que valorar a la hora de abordar las posibles responsabilidades laborales del DPO, porque como veremos a continuación el delegado no puede ser removido ni sancionado, salvo que incurra en dolo o negligencia grave en el ejercicio de sus funciones⁵³. En el caso de que sea despedido como consecuencia del desempeño de sus funciones entendemos que el despido puede declararse nulo, por vulnerar derechos fundamentales como la libertad de expresión y la garantía de indemnidad⁵⁴.

2.4. Posición del delegado de protección de datos

El art. 38.1 del Reglamento 2016/769 contempla que “el responsable y el encargado del tratamiento garantizarán que el DPO participe de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales”. El PLOPD configura la posición del DPO “como interlocutor del responsable o encargado del tratamiento

⁵³ Grupo de Trabajo sobre Protección de Datos del Artículo 29, *Directrices sobre los delegados de protección de datos (DPO)*, *op. cit.*, pp. 15 y 16.

⁵⁴ Ayuda Ley de Protección de Datos en https://ayudaleyprotecciondatos.es/2016/06/27/delegado-proteccion-datos/#Es_responsable_el_DPO_del_incumplimiento_de_la_normativa.

ante la Agencia Española de Protección de Datos y la autoridades autonómicas de protección de datos” (art. 36.1). Como se ha afirmado es una figura que “pivota” entre diferentes departamentos de la empresa como los de Recursos Humanos, Seguridad Corporativa, Legal, Marketing, Comercio electrónico, Financiero o Auditoría⁵⁵.

La posición del DPO ha sido tratada en una de las Directrices del Grupo de Trabajo sobre Protección de Datos del Artículo 29 (en adelante GT29) donde se hace hincapié en que es fundamental que el DPO, o su equipo, participen desde la etapa más temprana posible en todas las cuestiones relativas a la protección de los datos. El GT29 introduce una “directriz transcendental, que es la relativa a que, para facilitar el objetivo de cumplimiento («compliance») con el Reglamento y asegurar la aproximación de la privacidad desde el diseño, las organizaciones deben incorporar como parte de su gobernanza el procedimiento relativo a informar y consulta al DPO”⁵⁶. El G29 ofrece unos ejemplos de medidas que deben asegurar la participación del DPO, y finalmente recomienda que el responsable o el encargado elaboren unas directrices o programas sobre la protección de datos que determinen cuándo debe consultarse al DPO⁵⁷. Por otro lado, el PLOPD establece que en el ejercicio de sus funciones el DPO tendrá acceso a los datos personales y procesos de tratamiento, no pudiendo oponer a este acceso el responsable o el encargado del tratamiento la existencia de cualquier deber de confidencialidad o secreto (art. 36.3). En este sentido, si el DPO aprecia la existencia de una vulneración relevante en materia de protección de datos debe comunicarlo inmediatamente a los órganos de administración y dirección del responsable o el encargado del tratamiento (art. 36.4). Por último, nos queda por tratar otra serie de garantías esenciales en relación con el desempeño de sus funciones de “manera independiente” y la prohibición de destitución y sanción por el desempeño de las mismas (art 38.3).

⁵⁵ Velázquez, R., “El delegado de protección de datos en el entorno de la empresa”, *Red seguridad: Revista especializada en seguridad de la información*, n. 76, 2017, p. 58.

⁵⁶ Recio Gayo, M., *Directrices del G29 sobre el Delegado de protección de datos: figura clave para la responsabilidad («accountability»)*, *op. cit.*, p. 7.

⁵⁷ Grupo de Trabajo sobre Protección de Datos del Artículo 29, *Directrices sobre los delegados de protección de datos (DPD)*, *op. cit.*, p. 15.

3. Las garantías esenciales del estatuto jurídico del DPO, en especial la garantía de indemnidad

El DPO puede formar parte de la plantilla del responsable o del encargado del tratamiento o puede desempeñar sus funciones en el marco de un contrato de servicios (art. 37.6 Reglamento 2016/679). El Reglamento contempla que para que el Delegado participe de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales contará con el respaldo del responsable y del encargado del tratamiento de datos, que garantizarán que el Delegado no reciba ninguna instrucción en lo que respecta al desempeño de sus funciones ni sea destituido o sancionado por desempeñarlas, por lo que rendirá cuentas directamente al más alto nivel jerárquico del responsable o encargado⁵⁸. En el ejercicio de sus funciones estará obligado a mantener el secreto o la confidencialidad en lo que respecta al desempeño de sus funciones, de conformidad con el Derecho de la Unión o de los Estados miembros (art. 38 Reglamento UE). Como afirma el PLOPD la figura del DPO podrá estar o no integrado en la organización del responsable o del encargado y ser tanto persona física como una persona jurídica⁵⁹. En este sentido se ha afirmado que en el caso de las pequeñas empresas que necesiten designar el DPO o cuyo negocio no esté basado en los datos, el cargo puede ser externo. Por el contrario en las empresas multinacionales, en muchos casos va a suceder que el DPO radique en el país en que tengan su sede. Incluso hay quien afirma que es mejor que se trate de una persona que esté situada dentro de la empresa, pero sin responsabilidad en la gestión presupuestaria de la misma⁶⁰.

Estas recomendaciones no están en consonancia con la realidad de la Industria 4.0, puesto que en España en el año 2016 el 59'16% de las empresas utilizaba proveedores externos para dar servicios de seguridad y protección de datos. Entre los porcentajes más bajos se encontraban, por

⁵⁸ En AEDP, *Guía del Reglamento General de Protección de Datos para Responsables de Tratamientos*, p. 13, los encargados tienen obligaciones propias establecidas por el Reglamento 2016/379 como, por ejemplo, la designación del DPO en los casos contemplados en el art. 37 que no se circunscriben al ámbito del contrato que los une al responsable, y que pueden ser supervisadas separadamente por las autoridades de protección de datos.

⁵⁹ Exposición de Motivos IV, Proyecto de Ley de Protección de Datos de Carácter Personal (BOCG, núm. 13-1 de 24 de noviembre de 2017).

⁶⁰ Fernández, C.B., “El DPO es un cargo complejo que requiere difíciles competencias”, *Diario La Ley*, 2 de noviembre de 2017, p. 4 en <http://diariolaley.laley.es/home/NE0001445022/20171102/El-DPO-es-un-cargo-complejo-que-requiere-dificiles-competencias>.

ejemplo, las empresas cuya seguridad y protección de datos fue realizada principalmente por empleados propios (25'93%)⁶¹.

Como hemos afirmado más arriba, el DPO debe ejercer sus funciones con independencia, siendo obligada su designación tanto en el sector público como privado siempre que se cumplan los requisitos del Reglamento y de la norma nacional. En el ámbito de las Administraciones Públicas la implantación del DPO va a requerir⁶²: 1) conocer y revisar la normativa administrativa y técnica aplicable; 2) revisar el régimen competencial; y 3) decidir la organización administrativa del DPO. En este último punto incluye decidir si se comparte un DPO entre varios organismos o no⁶³, si se cubre con personal propio o con personal contratado externo, revisar el régimen de la función pública (si debe ser un funcionario o personal laboral a tiempo completo o a tiempo parcial); si se crea un puesto de trabajo o una unidad administrativa, revisar el régimen de provisión de la plaza (por concurso o por designación descartándose la libre designación para evitar posteriores conflictos), el carácter preceptivo o facultativo de sus informes y el carácter vinculante o no de los mismos y la conveniencia de dotarle de un seguro de responsabilidad civil⁶⁴.

En todo caso, si el DPO es una persona física -bien como un trabajador interno o como trabajador externo- en ambos casos hay una dependencia económica con el responsable o el encargado del tratamiento. Y, como es obvio, tratándose de un trabajador con un contrato de trabajo la dependencia es de tipo jurídico-económica⁶⁵. Si se trata de un DPO externo su función puede ejercerse sobre la base de un contrato de servicios suscrito con una persona física o una organización⁶⁶. Si la

⁶¹ Fuente INE, *Encuesta de Uso de TIC y Comercio Electrónico en las empresas*, 2016 publicada en <http://www.ontsi.red.es/ontsi/es/indicador/empresas-con-especialistas-tic-por-funciones>.

⁶² Hay que tener en cuenta que si el tratamiento lo lleva a cabo una autoridad u organismo público con independencia el tipo de datos que se traten la designación es obligatoria.

⁶³ Las directrices del GT 24 sobre los delegados de protección de datos (DPD) afirman que se podrán designar para varias autoridades u organismos públicos, teniendo en cuenta su estructura organizativa y tamaño, obra cit., p. 24.

⁶⁴ En Fernández, C.B., *El DPO es un cargo complejo que requiere difíciles competencias*, op. cit., p. 5 en <http://diariolaley.laley.es/home/NE0001445022/20171102/El-DPO-es-un-cargo-complejo-que-requiere-dificiles-competencias>.

⁶⁵ Davara Rodríguez, M.A., *El Delegado de Protección de Datos en los ficheros y/o tratamientos de la Administración en consonancia con el Reglamento Europeo de Protección de Datos*, op. cit., p. 10 y el mismo autor en "Delegado de Protección de Datos en las entidades locales", *El Consultor de los Ayuntamientos*, n. 3, 2013, La Ley 103372013, p. 2.

⁶⁶ Grupo de Trabajo sobre Protección de Datos del Artículo 29, *Directrices sobre los delegados de datos (DPD)*, op. cit., p. 25.

función del DPO la ejerce un proveedor de servicios externo, las directrices del GT24 afirman que “un grupo de personas que trabaje para dicha entidad podrá desempeñar efectivamente las funciones de DPD como equipo, bajo la responsabilidad de un contacto principal designado como persona «a cargo» del cliente”. En ese caso, es fundamental que cada miembro de la organización que ejerza las funciones de DPD cumpla todos los requisitos aplicables del RGPD⁶⁷. En definitiva, toda 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 Control⁶⁸. Una de las características de la implantación de un DPO en las organizaciones es la creación de este nuevo puesto con unas funciones y peculiaridades inherentes al sujeto realizadas con independencia del vínculo o título jurídico que tenga con su empleadora: a) total autonomía en el ejercicio de sus funciones; b) necesidad de que se relacione con el nivel superior de la dirección; c) obligación de que el responsable o el encargado faciliten al DPO todos los recursos necesarios para desarrollar su actividad. No obstante, “ya esté integrado o forme parte de la empresa o Administración pública o ya sea un profesional jurídico-técnico externo (...) en todo caso va a tener una enorme responsabilidad, como es prevenir y evitar las conductas que pueden terminar con una sanción administrativa tan desproporcionada” (10 o 20 millones de euros) y “todo ello *al margen de la responsabilidad civil* pertinente que se superpondría a esta sanción administrativa”.

En materia de responsabilidad laboral, cuando el DPO sea persona física integrada en una organización del responsable o encargado del tratamiento, el DPO no podrá ser removido ni sancionado por el responsable o el encargado por desempeñar sus funciones salvo que incurriera en dolo o negligencia grave en su ejercicio. Y, por lo tanto, el despido podría tener la consideración de un despido nulo en parecidos términos a lo contemplado en art. 68.1 c) ET cuando el despido o sanción se base en la acción del trabajador- DPO en el ejercicio de sus funciones y la sanción se conecte con el ejercicio de derechos fundamentales, como la

⁶⁷ Grupo de Trabajo sobre Protección de Datos del Artículo 29, *Directrices sobre los delegados de datos (DPD)*, *op. cit.*, p. 25.

⁶⁸ AEPD, *Guía para el cumplimiento del deber de informar*, p. 2 en <https://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/modeloclausulainformativa.pdf>.

libertad de expresión y la garantía de indemnidad⁶⁹.

4. Conclusiones

El DPO no es una figura propiamente novedosa, aunque se presenta como novedad en el Reglamento UE 2016/679. La novedad radica precisamente en la designación obligatoria de un DPO por el responsable y encargado del tratamiento en los casos tasados en el propio Reglamento, y su carácter voluntario en el resto. El Reglamento general de protección de datos ofrece un marco que permite reforzar el derecho fundamental a la protección de datos de carácter personal, puesto que es de aplicación directa y, por lo tanto, de regulación uniforme en los Estados miembros de la UE. Es una norma que además actualiza la protección de datos atendiendo al impacto de la evolución tecnológica y de la globalización y los retos que ello supone para la protección de los datos personales de los trabajadores y de los ciudadanos en el marco de la Industria 4.0, donde las personas físicas deben tener el control de sus propios datos.

Por lo tanto, la novedad del Reglamento es la implantación de un DPO en las organizaciones con la creación de un nuevo puesto con unas funciones y peculiaridades inherentes al sujeto que las lleva a cabo con independencia del vínculo o título jurídico que tenga con la persona que lo contrata: a) total autonomía en el ejercicio de sus funciones; b) necesidad de que se relacione con el nivel superior de la dirección; y c) obligación de que el responsable o el encargado faciliten al DPO todos los recursos necesarios para desarrollar su actividad.

Como garantía adicional cabe señalar la no responsabilidad personal del incumplimiento de los requisitos de protección de datos. La responsabilidad recae sobre el responsable o el encargado del tratamiento que es el que está obligado a garantizar y ser capaz de demostrar que el tratamiento se realiza de conformidad con el Reglamento 2016/679 porque, como han indicado las directrices del GT 29 conforme a la regulación reglamentaria, el cumplimiento de las normas en materia de protección de datos es responsabilidad del responsable del tratamiento.

⁶⁹ Durán López, F. y Sáez Lara, C., “Representación y participación de los trabajadores en la empresa”, en AA.VV., *Las transformaciones del derecho del trabajo en el marco de la Constitución Española*, Editorial La Ley, Madrid, 2006, La Ley 5484/2007, pp. 10 se dice “la garantía frente al despido prohíbe el despido-sanción de las funciones representativas, pero no prohíbe el despido fundado en actuaciones del representante protagonizadas en el desarrollo de su actividad sindical en la empresa”.

En este sentido, otra de las garantías que contempla el Reglamento 2016/679 es que el DPO no será destituido ni sancionado por el responsable o el encargado por desempeñar sus funciones.

En definitiva, una garantía adicional que atañe al DPO como persona física que esté integrada en la organización del responsable o encargado del tratamiento, puesto que no puede ser removido ni sancionado por el responsable o el encargado por el desempeño de sus funciones, salvo que incurriera en dolo o negligencia grave en su ejercicio. Por lo tanto, el despido que se produzca en el ejercicio de sus funciones debe entenderse nulo de pleno derecho (garantía de indemnidad) salvo que, como en el caso de los representantes de los trabajadores, se trate de un despido disciplinario conforme a lo previsto en el art. 54 del ET.

5. Bibliografía

- Davara Rodríguez, M.A., “El Delegado de Protección de Datos en los ficheros y/o tratamientos de la Administración en consonancia con el Reglamento Europeo de Protección de Datos”, *Actualidad Administrativa*, n. 1, 2017, La Ley 9650/2016.
- Davara Rodríguez, M.A., “Delegado de Protección de Datos en las entidades locales”, *El Consultor de los Ayuntamientos*, n. 3, 2013, La Ley 1033/2013.
- Díaz Díaz, E., “El «Data Protection Officer» (DPO) en el nuevo Reglamento General de Protección de Datos”, *El Derecho.com. Lefebvre. El Derecho*, 25 de abril de 2016, en http://tecnologia.elderecho.com/tecnologia/privacidad/Protection-Officer-DPO-Reglamento-Proteccion-Datos-UE_11_945055002.html.
- Díaz Díaz, E., “El nuevo Reglamento de Protección de Datos de la Unión Europea y sus consecuencias jurídicas para las instituciones”, *Revista Aranzadi Doctrinal*, n. 6, 2016, parte estudio, BIB 2016/3067.
- Durán López, F. y Sáez Lara, C., “Representación y participación de los trabajadores en la empresa”, en AA.VV., *Las transformaciones del derecho del trabajo en el marco de la Constitución Española*, Editorial La Ley, Madrid, 2006, La Ley 5484/2007.
- Fernández, C.B., “El DPO es un cargo complejo que requiere difíciles competencias”, *Diario La Ley*, 2 de noviembre de 2017, en <http://diariolaley.laley.es/home/NE0001445022/20171102/El-DPO-es-un-cargo-complejo-que-requiere-dificiles-competencias>.
- Fuentes, P., “IV. Perfiles más demandados en la actualidad (1)”, en Gil Casares, M. y Fuentes, P., *Digitalización, empleo y futuro*, Wolters Kluwer, Madrid, 2017.

- Gil, E., *Big data, privacidad y protección de datos*, Agencia Española de Protección de Datos, Agencia Estatal Boletín del Estado, Madrid, 2016.
- Judel Meléndrez, M.M^a, “La formación, clave para el DPD”, *Red seguridad. Revista especializada en seguridad de la información*, n. 76, 2017.
- López Álvarez, L.F., *Protección de datos personales: adaptaciones necesarias al nuevo Reglamento europeo*, Francis Lefebvre-El Derecho, S.A., Madrid, 2016.
- Martín, O., “Se dispara la demanda de perfiles en la Industria 4.0”, *RRHHDigital*, 24 de noviembre de 2017.
- Rallo Lombarte, A. y García Mahamut, R., *Hacia un nuevo derecho europeo de protección de datos*, Tirant lo Blanch, Valencia, 2015.
- Recio Gayo, M., “Directrices del GT29 sobre el delegado de protección de datos. Figura clave para la responsabilidad («accountability»)", *Diario La Ley*, n. 2, 2017, La Ley 185/2017.
- Rodríguez Ballano, S. y Vidal, M., “Habemus nuevo Reglamento General de Protección de Datos”, *Actualidad Jurídica Aranzadi*, n. 919, 2016 parte Comentario, BIB 2016/3116.
- Sáiz, C. (coord.), *Código de buenas prácticas en protección de datos para proyectos big data*, editado por la AEDP y ISMS Forum Spain en https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guías/2017/Guía_Big_Data_AEPD-ISMS_Forum.pdf.
- Salgueiro, J.M., “Big Data, ¿amenaza u oportunidad para la gestión de la seguridad?”, *Red seguridad: revista especializada en seguridad informática, protección de datos y comunicaciones*, n. 78, 2017.
- Saracíbar, E., “Una profesión en alza”, *Red seguridad: revista especializada en seguridad de la Informática, protección de datos y comunicaciones*, n. 76, 2017.
- Velázquez, R., “El delegado de protección de datos en el entorno de la empresa”, *Red seguridad: Revista especializada en seguridad de la información*, n. 76, 2017.

Web sites

- http://europa.eu/rapid/press-release_IP-17-347_es.htm.
- <http://www.agendadigital.gob.es/Seguimiento/Informes anuales/Informes/2016/Informe-anual-ADpE-2016.pdf>.
- <http://static.iebschool.com/17/pdf/estudio-transformacion-digital-IEBS.pdf>.
- <http://www.oecd-ilibrary.org/docserver/download/7da6001b-es.pdf?expires=1510594243&id=id&accname=guest&checksum=8F3A95B5F6F74DA83AD0F8511BD3C0CD>.

<http://ametic.es/es/prensa/la-aceleraci%C3%B3n-digital-impulsar%C3%ADa-un-36-el-pib-en-2021>.

<https://blog.fundae.es/2017/02/09/competencias-digitales-para-el-futuro-de-europa/>.

https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guías/2017/Guia_Big_Data_AEPD-ISMS_Forum.pdf, pág. 8.

http://tecnologia.elderecho.com/tecnologia/privacidad/Protection-Officer-DPO-Reglamento-Proteccion-Datos-UE_11_945055002.html.

<https://www.datax.es/blog-actualidad-proteccion-datos/es/dpo-quien-contratarlo/>.

http://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/guia_r_gpd.pdf.

http://www.agpd.es/portalwebAGPD/temas/certificacion/common/pdf/ESQ_UEMA_AEPD_DPD.pdf.

<http://www.comillas.edu/es/grados/doble-grado-en-business-analytics-economics-and-finance-y-derecho-e-3>.

<https://www.mecd.gob.es/educacion/mc/lomce/el-curriculo/curriculo-primaria-eso-bachillerato/competencias-clave/competencias-clave/digital.html>.

https://ayudaleyprotecciondatos.es/2016/06/27/delegado-proteccion-datos/#Es_responsable_el_DPO_del_incumplimiento_de_la_normativa.

<http://diariolaley.laley.es/home/NE0001445022/20171102/El-DPO-es-un-cargo-complejo-que-requiere-dificiles-competencias>.

<http://www.ontsi.red.es/ontsi/es/indicador/empresas-con-especialistas-tic-por-funciones>.

<http://diariolaley.laley.es/home/NE0001445022/20171102/El-DPO-es-un-cargo-complejo-que-requiere-dificiles-competencias>.

Red Internacional de ADAPT



ADAPT es una Asociación italiana sin ánimo de lucro fundada por Marco Biagi en el año 2000 para promover, desde una perspectiva internacional y comparada, estudios e investigaciones en el campo del derecho del trabajo y las relaciones laborales con el fin de fomentar una nueva forma de “hacer universidad”. Estableciendo relaciones estables e intercambios entre centros de enseñanza superior, asociaciones civiles, fundaciones, instituciones, sindicatos y empresas. En colaboración con el DEAL – Centro de Estudios Internacionales y Comparados del Departamento de Economía Marco Biagi (Universidad de Módena y Reggio Emilia, Italia), ADAPT ha promovido la institución de una Escuela de Alta formación en Relaciones Laborales y de Trabajo, hoy acreditada a nivel internacional como centro de excelencia para la investigación, el estudio y la formación en el área de las relaciones laborales y el trabajo. Informaciones adicionales en el sitio www.adapt.it.

Para más informaciones sobre la Revista Electrónica y para presentar un artículo, envíe un correo a redaccion@adaptinternacional.it



ADAPTInternacional.it

Construyendo juntos el futuro del trabajo