Prevención en la protección de datos personales: funciones del Compliance Officer y del Data Protection Officer

TRABAJO FINAL DE GRADO.
GRADO DE CRIMINOLOGÍA Y SEGURIDAD 2017/2018

ALUMNA: **Catalina Radu**
TUTOR: **Félix Serrano Gallardo**

ÍNDICE:

Abreviaturas

AEPD	Agencia Española de Protección de Datos
CE	Constitución Española
CP	Código Penal
CO	Compliance Officer
DPO	Data Protection Officer
INE	Instituto Nacional de Estadística
LECrim	Ley de Enjuiciamiento Criminal
LOPD	Ley Orgánica de protección de datos de carácter personal
RGPD	Reglamento General de Protección de Datos (UE)
RLOPD	Reglamento de desarrollo de la Ley Orgánica de protección de datos de carácter personal
STC	Sentencia del Tribunal Constitucional
TC	Tribunal Constitucional
TIC	Tecnologías de la Información y la Comunicación
TJUE	Tribunal de Justicia de la Unión Europea
UE	Unión Europea

Extended summary

The protection of personal data has it´s basis since the mid-sixties. Although it is minimal, because at the time the technological advances were little or with no progress. Among the existing regulations at European level in terms of data protection, stands out:

- The European Convention on Human Rights signed in Rome on November 4, 1950 and published in Spain in the BOE on October 10, 1979;

- The Charter of Fundamental Rights of the European Union (2000/C 364/01);
- Convention No. 108 of the Council of Europe, of January 28, 1981;

- Directive 95/46 / EC of the European Parliament and of the Council of 24 October 1995 on the protection of natural persons with regard to the processing of personal data and the free circulation of such data;

- Directive 97/66 / EC of the European Parliament and of the Council of 15 December 1997;

- Directive 2002/58 / EC of the European Parliament and of the Council of 12 July 2002 on the processing of personal data and the protection of privacy in the field of electrical communications (directive on privacy and electronic communications;

- Regulation of the European Union 2016/679, of April 27, 2016.

At national level, the EC does not include any article that makes special reference to any data protection, it's the STS 254/1993 who deserves special recognition since, and through it "computer freedom" is mentioned for the first time in Spain the right to privacy (Article 18.1 CE) and dignity of persons (Article 10.1). It manages to connect the articles from the Constitution with the right to privacy and the right to protection of personal data.

The rules in this field can be extended and the ones worthy of note are: The Organic Law of Protection of Personal Data, of December 15, 1999; Royal Decree 1720/2007, which approves the Regulation for the development of the Organic Law 15/1999, of December 13 and currently, the Draft Organic Law for the Protection of Personal Data.

The main novelties of the general regulatory system, highlights the discipline and rigor with which technique is applied. Standards have been tightened up, and new rights and principles introduced, such as the ARCO rights. They have extended it by adding the right of cancellation (right to forget), which is the right to have unnecessary personal data removed within a period of day. Also, the limitation of data transmission for the respect of the right to privacy. Additionally, we are also part of the Accountability principle, which is a system for regular and routine exchange of notifications and other information. Another important novelty is the introduction of the DPO figure.
Regarding the principles and rights, we would highlight the:

1. Principles:
    - Principles of legality, loyalty and transparency;
    - Principle of determination of treatment;
    - Principle of adequacy, conservation and accuracy of data;
    - Information duty;
    - Principle of consent, in usual or general treatments;
    - Principle of accountability.

2. Rights of data subject:
    - Right of access by data subject,
    - Right to rectification;
    - Right to erasure (´right to be forgotten´);
    - Right to restriction of processing;
    - Notification obligation regarding rectification or erasure of personal data or restriction of processing;
    - Right to data portability.

The following section describes the two figures in charge of risk prevention. On the one hand we have the data protection delegate that is the great novelty of the RGPD. It's characterized by being the person in charge of the regulatory Compliance of data

protection in organizations. This figure must have knowledge in national and European laws, and extensive skills and knowledge in the area of data protection. Its main functions are:

- Inform and advise the responsible and employees on the treatment,
- Supervise Compliance with the policies of the Regulation,
- Offer advice on impact evaluation,
- Cooperate and act as a point of contact for the supervisory authority.

On the other hand, we have the Compliance officer, who is the person responsible for providing or coordinating the continuous training of regulatory Compliance, as well as the figure that can be supported in case of doubts, according to the UNE-ISO 19601: 2017 Standard.

Its main functions are:

- Management of the preventive model
- Information and training on the prevention model
- Review and modification of the prevention model
- Management of the reporting channel and internal investigations

The responsibility of legal persons is another relevant principle since, with the reform of CP 1/2015, the introduction of management system would lead to system improvements, as the requirements of article the 31 bis of the Código Penal and the comparison of the Office of the Prosecutor and the UNE-ISO 19601: 2017.

Regarding the criminal responsibility of the CO and the DPO, the CO, may incur in criminal acts in the cases of an active coexistence in the criminal action, as necessary inductor or co-operator. In his advisory role, he does not incur criminal liability since he does not have a guarantor position.
The DPO does not have the position of guarantor; therefore, it can`t commit criminal acts, which can`t be imputed. This does not rule out that he can be fired for his bad practice in the performance of his factions.

The prevention of personal data protection will take into account the impact evaluation, consequence of the treatment of personal data that is a function of the DPO and the risk maps of the Compliance management system, made by the DPO. The prevention is made

in relation of an act of crime by the discovering and revelation of the secrets established in the second part in article 197 in the Código Penal.

Risk maps will be established in relation to the impact and frequency evaluation, in addition to the analysis of the risk prevention matrix, with its respective supervision map after the implementation of the system in the organization.

Finally, the figure of the criminologist is analysed, as a future professional in the field of data protection and management of the prevention system.
The profile that a CO must have is the following:

- Legal profile,
- Knowledge in criminal law and other branches of the legal system,
- Demonstrable knowledge of national, European and international regulations,
- Neutrality,
- Integrity,
- Communication and coordination skills.

On the other hand, the DPO also has to have a legal profile, powers in terms of data protection. He also has to have at least two years of professional experience in data protection and training courses. The Spanish Data Protection Agency has established a mechanism to open a way for anyone wishing to work on this, through a certification.

In conclusion, this work deals with the European and national regulations, with their respective analysis in relation to the novelties introduced on the rights principles and the new figure of the DPO. It also deals with the effectiveness of the Compliance Officers and the delegates, the legal responsibility in which they may incur both the general and the specific level.

Lastly, from a criminology-based perspective, the possibility or not of working, in these two areas mentioned above, general data protection and the prevention, detection and investigation of criminal offences.

Resumen: La era de la información ha traído consigo numerosos beneficios que han dado lugar a una vida más cómoda y plena de oportunidades, pero también ha conllevado un incremento de los riesgos de que Derechos Fundamentales sufran vulneraciones. Por tal razón, tanto a nivel nacional como europeo, la normativa ha ido evolucionando para prevenir y reaccionar ante tal vulnerabilidad. Determinados cargos en la dirección de las personas jurídicas como los Delegados de Protección de Datos y los Oficiales de Cumplimiento normativo han cobrado un papel importante en materia de protección de datos y prevención de riesgos delictivos, respectivamente. Las similitudes y diferencias entre estas dos funciones y las responsabilidades en que pueden incurrir surgen como cuestiones de interés. Por último, tras el análisis de la prevención en materia de protección de datos personales, se estudiará si un criminólogo cumple con los requisitos establecidos para insertarse en el mercado laboral, llevando a cabo las actividades de alguna de estas dos figuras.

Palabras clave: Oficial de Cumplimiento, Responsabilidad penal, Programa de Cumplimiento Normativo, Delegado de Protección de Datos, Protección de Datos.

Abstract: The information age has brought numerous benefits that had led to a more comfortable and full of opportunities life, but it has also entailed an increase in the risks of Fundamental Rights suffering violations. For this reason, both at national and European level, regulations have evolved to prevent such vulnerability. Certain positions in the management of legal persons such as Data Protection Officers and Compliance Officers have gained an important role in data protection and crime prevention, respectively. The similarities and differences between these two functions and the responsibilities they may incur arise as matters of interest. Finally, after analysing the prevention of personal data protection, it will be studied if a criminologist complies with the requirements established to work, carrying out the activities of one of these two figures.

Keywords: Compliance Officer, Criminal Liability, Data Protection Officer, Corporate Compliance, Data protection Officer.

I Introducción

El presente trabajo tiene como objeto realizar un análisis sobre la evolución de la prevención en materia de protección de los datos de carácter personal. Los avances informáticos han contribuido a enormes y vertiginosos cambios en esta materia. Así, el Derecho no puede mantenerse ajeno a la presente "Era de la Información"[1], y se han desarrollado normas para proteger las violaciones de derechos tanto para las personas físicas como para las personas jurídicas, a nivel europeo y nacional. Internet y su llegada "se ha infiltrado" en las vidas de las personas y ha dado paso a vulneraciones de la intimidad y la vida privada. La Red ha pasado a ser "el tejido de nuestras vidas, que constituye, actualmente, la base tecnológica de la forma organizativa que caracteriza la era de la información"[2]. Las nuevas tecnologías generan sensaciones de inseguridad social en relación con la privacidad de las personas.[3] Según los estudios estadísticos de la AEPD los ciudadanos están cada vez más preocupados por la utilización de sus datos personales, *"las consultas recibidas en el área de Atención al Ciudadano han superado las 236.000, un incremento del 8% que se suma al 10% que ya se había producido en 2015 sobre 2014"*[4].

El Ministerio de Interior, en sus "Estudios sobre la cibercriminalidad, infraestructuras críticas y ciberseguridad"[5], analiza los siguientes incidentes: "robos de información", "virus, troyanos, gusanos, spyware", "SPAM", "escaneo de red", "fraude", "denegación de servicios", "acceso no autorizado" con un total de 36005 incidentes gestionados en el año 2016. Frente a este número tan elevado de incidentes que afectan a la seguridad de los datos, se ha creado un canal de respuesta, denominado CERTSI[6]_ en virtud del cual las grandes empresas han empezado a firmar acuerdos de confidencialidad.

---

[1] NOAIN SÁNCHEZ, Amaya, La protección de la intimidad y vida privada en internet: la integridad contextual y los flujos de información en las redes sociales (2004-2014), XIX Edición del Premio Protección de Datos Personales de Investigación de la Agencia Española de Protección de Datos. Agencia Estatal Boletín Oficial del Estado Madrid, 2016, pp. 41 y ss.

[2] CASTELLS, Manuel. (2001) La galaxia Internet, Barcelona: Areté, p.15.

[3] ZALDÍVAR ROBLES, Javier La protección penal del derecho a la intimidad(19/2016) Fecha de publicación, 06/2016 www.tirantonline.com [Fecha de consulta: 23/04/2018]

[4] ESPAÑA MARTÍ, Mar, Memoria_AEPD, http://www.agpd.es/ portalwebAGPD /LaAgencia/informacion_institucional/common/memorias/2016/Memoria_AEPD_2016.pdf [Fecha de consulta: 30/04/2018]

[5] Estudios sobre la Cibercriminalidad en España, 2016; Ministerio del Interior http://www.interior.gob.es/documents/10180/5791067/Estudio+Cibercriminalidad+2016.pdf/456576b2-9ce8-4f3c-bbcc-ca0dbf3bb3cf [Fecha de consulta: 30/04/2018]

[6] CERTSI_ Capacidad de Respuesta a incidentes de Seguridad de la Información del Ministerio de Energía, Turismo y Agenda Digital y del Ministerio del Interior.

Tras la presente introducción, el TFG analizará el marco normativo de referencia en cuanto a la protección de datos personales a nivel europeo y nacional, haciendo hincapié en el recorrido y las novedades en dicho ámbito. Se hará un exhaustivo recorrido por tales normas, y en especial por el nuevo Reglamento General de Protección de Datos (RGPD) europeo, vigente de manera uniforme y homogénea en el espacio europeo desde el 25 de mayo de este año. A nivel europeo, en la mayoría de los países la responsabilidad penal de las personas jurídicas no es una novedad, pero si lo es, la introducción de la figura del Delegado de Protección de Datos, que viene recogido explícitamente en el *Reglamento 2016/679 del Parlamento Europeo y del Consejo de 27 de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos*. De esta manera, España mediante al novedoso Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal[7], lo que quiere conseguir es adoptar la normativa española a nivel europeo (RGPD).

A su vez, se tratará de la ampliación del marco normativo en lo referente a los derechos ARCO, pasando a contemplar tres novedosos derechos: el derecho al olvido, el derecho de limitación y el derecho de portabilidad de los datos.

El tercer capítulo se dedicará al estudio de las figuras que pueden prevenir las infracciones sobre protección de datos, en el caso de personas jurídicas que utilicen masivamente este tipo de datos. En concreto se examinan el Delegado de Protección de Datos (DPO del inglés Data Protection Officer) y el Delegado de Cumplimiento (o, del mismo modo, CO ó Compliance Officer), sus funciones, el modo de intervenir en cuanto al tratamiento de datos y la prevención de riesgos respectivamente.

En ese mismo capítulo III se partirá de la introducción en nuestro ordenamiento jurídico de la responsabilidad criminal de las personas jurídicas, al haberse quebrado la regla que recoge el aforismo "*societas delinquiere non protest*" y la introducción del artículo 31 bis, del Código Penal, con la implantación de un sistema de gestión de riesgos "Corporate Compliance", para eximirle o en su caso, atenuarle, de la posible responsabilidad criminal. Todo ello para relacionarlo con las posibles infracciones penales en protección de datos de carácter personal por parte de las personas jurídicas, y su prevención.

[7] Proyecto de Ley Orgánica en tramitación parlamentaria habiendo superado la fase de enmiendas en el Congreso: http://congreso.es [última consulta efectuada el 22 de mayo de 2018]

Se compara la Circular de la Fiscalía General de Estado[8] sobre dicho artículo 31 bis CP con la norma UNE-ISO 19601:2017 sobre sistemas de gestión de Compliance Penal, buscando en todo momento la perspectiva de la prevención. También, se introducirá la propia responsabilidad penal en la que pueden incurrir los Delegados de Protección de Datos y los Oficiales de Cumplimiento, y sus intervenciones en materia de prevención de riesgos.

El capítulo III desembocará en la prevención criminal en materia de protección de datos, lo que se realizará mediante la aplicación de la citada norma UNE-ISO 19601:2017 al artículo 197 CP sobre descubrimiento y revelación de secretos. La realización previa de prácticas externas de la autora del presente TFG en el Ilustre Colegio Oficial de Criminólogos de la Comunidad Valenciana (Valencia) sobre "Compliance" y la norma UNE-ISO 19601:2017 le facilitó esta labor, que a su vez incluirá el estudio del mapa de riesgos que sobre protección de datos pueden existir en ámbito penal en el día a día de las personas jurídicas.

En el último apartado se hará una aproximación crítica a la eventual empleabilidad como Delegado de Protección de Datos o como Compliance Officer de un futuro egresado en el Grado de Criminología y Seguridad.

Las conclusiones extraídas se referirán a las novedades normativas que diseñan un verdadero espacio europeo de protección de datos para los ciudadanos, sobre todo en materia de principios y de nuevos derechos; a la eficacia de los Delegados de Protección de Datos y Oficiales de Cumplimiento para prevenir las vulneraciones en esta cuestión y las responsabilidades subsiguientes; a la idoneidad de las normas UNE-ISO para la elaboración de mapas de riesgo sobre protección de datos tomando como referencia lo que prescribe la Circular de la FGE; así como si se abren o no posibilidades de trabajo en este campo para los criminólogos.

[8] Circular FGE 1/2016, sobre la Responsabilidad Penal de las Personas Jurídicas conforme a la Reforma del Código Penal efectuada por la Ley Orgánica 1/2015.

II Marco normativo

1. Regulación europea sobre protección de datos

La protección de los datos de carácter personal alcanza sus bases normativas desde mediados de los años sesenta, aun así era mínima, porque en esa época los avances tecnológicos eran escasos y no había tantas facilidades para la libre circulación de los datos. No se contaba con vulneraciones de derechos fundamentales en este ámbito, aun así la legislación no es reprochable, pero poco amplia. En el ámbito europeo destacan:

a) El Convenio Europeo de Derechos Humanos[9] regula en su artículo 8 el derecho a la vida privada y familiar, el domicilio y de su correspondencia. Así como, defiende la protección de los datos personales y expone los requisitos donde las autoridades públicas pueden hacer injerencia.

b) La Carta de los Derechos Fundamentales de la Unión Europea, abarca en su artículo 8, la protección de los datos de carácter personal.

c) El Convenio nº 108 del Consejo de Europa, de 28 de enero de 1981[10], es la primera norma amplia sobre la protección de datos. Tiene como finalidad extender la protección de datos en relación con el tratamiento automatizado (principio finalista, pertinencia de datos, principio de utilización no abusiva, principio de derecho de olvido, principio de lealtad, principio de exactitud, principio de publicidad, principio de acceso individual y principio de seguridad).

d) Directiva 95/46/CE[11], contemplaba un marco normativo general en la Unión Europea. Fue una de los pilares básicos, con dos finalidades concretas, por una parte, defender el derecho fundamental a la protección de datos y por otro lado

[9] Firmado en Roma el 4 de noviembre de 1950 y publicado en España en el BOE el 10 de octubre de 1979.
[10] Consejo de Europa, Convenio para la protección de las personas con respeto al tratamiento automatizado de datos de carácter personal, Estrasburgo el 18 de enero de 1981 y ratificado por España el 27 de enero de 1984 en el BOE el 15 noviembre de 1985.
[11] Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respeta al tratamiento de datos personales y a la libre circulación de estos datos.

garantizar la libre circulación de dichos datos entre los Estados miembros de la UE.

e) Directiva 97/66/CE del Parlamento Europeo y del Consejo, de 15 de diciembre de 1997[12]. Esta directiva completa la anterior con relación a los datos de carácter personal en el sector de las telecomunicaciones. (Derogada por la Directiva 2002/58/CE)

f) Directiva 2002/58/CE[13], el ámbito de aplicación y objeto: "1. La presente Directiva armoniza las disposiciones de los Estados miembros necesarias para garantizar un nivel equivalente de protección de las libertades y los derechos fundamentales y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales en el sector de las comunicaciones electrónicas, así como la libre circulación de tales datos y de los equipos y servicios de comunicaciones electrónicas en la Comunidad."

g) Reglamento de la Unión Europea 2016/679, de 27 de abril de 2016. Este reglamento deroga la Directiva 95/46/CE. Se publicó en el Diario Oficial de la Unión Europea el 4 de mayo de 2016. El nuevo Reglamento de Protección de Datos (RGDP) se denomina, *Reglamento 2016/679 del Parlamento Europeo y del Consejo de 27 de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos*. En su artículo 1[14], establece que se otorga la protección de las personas físicas con respeto a los datos de carácter personal y sus respectivas normas que

[12] Relativa al tratamiento de datos personales y a la protección de la intimidad en el sector de las telecomunicaciones.

[13] Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones eléctricas (directiva sobre la privacidad y las comunicaciones electrónicas) http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/union_europea/directivas/common/pdfs/B.6-cp--Directiva-2002-58-CE-protecci-oo-n-e-intimidad-en-comunicaciones-electronicas.pdf

[14] Artículo 1 del RGDP Objeto "1. El presente Reglamento establece las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y las normas relativas a la libre circulación de tales datos. 2. El presente Reglamento protege los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales. 3. La libre circulación de los datos personales en la Unión no podrá ser restringida ni prohibida por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales."

protegen la libre circulación de los datos. También salvaguarda los derechos y libertades fundamentales de las personas físicas.

2. Regulación española

La Constitución Española no recoge ningún artículo que haga expresa y directa referencia al derecho de protección de los datos de carácter personal, es decir, no abarca la protección de datos como un derecho fundamental. No lo contempla porque el texto constitucional data desde 1978 y en esos tiempos no estaba previsto el gran avance de la tecnología y la información. La necesidad de proteger los datos surge una vez con los grandes avances tecnológicos ya que se podrían vulnerar los derechos de las personas.
La primera vez que se menciona en España la protección de datos, ha sido en la STC 254/1993, mediante el término "libertad informática" que se entiende como un derecho fundamental autónomo que tiene especial relación con el derecho a la intimidad[15] y la dignidad de la personas[16]. Por otro lado, nuestra Constitución reconoce en su artículo 18.4 la limitación del uso de la información dándole mayor cargo a la protección, evitando así, un enfrentamiento directo entre el derecho a la intimidad con la necesidad informática.

La Ley Orgánica de Protección de Datos de Carácter Personal, de 15 de diciembre de 1999[17], garantiza y protege los datos personales, las libertades públicas y los derechos fundamentales.

El Real Decreto 1720/2007, 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: este Reglamento se aprobó para introducir y ampliar nuevos aspectos de la LO 15/1999. Añadió en sus respectivos títulos, dando explicaciones de los distintos términos, como por ejemplo, qué se entiende por archivos y ficheros, comunicaciones electrónicas, como también clasificaciones sobre aspectos para el tráfico ordinario.

[15] Artículo 18.1, CE "Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen."
[16] Artículo 10.1, CE "La dignidad de la persona, los derechos inviolables que le son inherentes, el libre desarrollo de la personalidad, el respeto a la ley y a los derechos de los demás son fundamento del orden político y de la paz social."
[17] Publicado en BOE núm. 298, de 14 de diciembre de 1999.

Por último, el Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal[18], tiene como objeto adaptar la normativa española en materia de protección de datos de carácter personal, al Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016.

3. Novedades del Reglamento General de Protección de Datos y el Proyecto de Ley Orgánica de Protección de Datos

El Reglamento General de Protección de Datos viene a modernizar la normativa sobre la protección de datos de carácter personal. El ámbito de este Reglamento es de aplicación desde el 25 de mayo de 2018. A continuación se va a realizar una breve explicación de las novedades introducidas:

a) Nuevos principios relativos al tratamiento de datos. En su artículo 5[19], el Reglamento introduce novedades con relación al tratamiento de los datos. Cabe destacar que los datos se tienen que tratar de manera <<licita, leal y transparente>> y siempre recogidos con un fin, <<minimización de datos>>,

[18] Boletín Oficial de las Cortes Generales, Congreso de los Diputados XII legislatura serie A: Proyectos de ley 24 de noviembre de 2017 núm. 13-1; www.congreso.es/portal/page/portal/Congreso/PopUpCGI?CMD=VERLST&BASE=pu12&DOCS=1-1&DOCORDER=LIFO&QUERY=%28BOCG-12-A-13-1.CODI.%29#(Página1); [Fecha de consulta: 03/04/2018]

[19] 1. Los datos personales serán: a) tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»); b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales («limitación de la finalidad»); c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»); d) exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan («exactitud»); e) mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado («limitación del plazo de conservación»); f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»). 2. El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»)

<<exactitud>>, <<limitación del plazo de conservación>>, <<integridad y confidencialidad>>, << responsabilidad proactiva>>. Una de las novedades que implica el nuevo RGPD es la responsabilidad proactiva (*accountability*). Hace especial referencia a la necesidad de prevenir los riesgos, aplicar medidas correctoras y análisis de las evaluaciones de impacto.

b) El consentimiento. El artículo 7[20], sostiene que el interesado ha de dar su consentimiento y se tiene que poder demostrar por el responsable de protección de datos. El consentimiento se puede retirar siempre. Los cambios que hay que destacar tienen especial relación con la información que los interesados reciben y la forma en la que la reciben. Esta información debe llegar a los usuarios de una forma clara, concisa, inteligible y trasparente. Se cambia de un consentimiento táctico a un consentimiento inequívoco, libre y específico. Se amplía la posibilidad de retirar el consentimiento en cualquier momento. Otra cuestión a tener en cuenta, es el plazo en el caso de que los datos se hayan obtenido de otra fuente. Anteriormente el plazo era de tres meses máximo, nuevamente el Reglamento regula un plazo de máximo un mes.

c) Se han ampliado los derechos ARCO. El derecho al olvido y a la portabilidad de los datos.

   Si el consentimiento se ha obtenido de forma ilícita o se ha revocado el consentimiento, el derecho al olvido implica que estos datos tienen que ser suprimidos. El derecho a la portabilidad implica que los datos se podrán trasladar de un responsable a otro, siempre y cuando el interesado lo solicite.

d) Registro y notificaciones a los interesados de las violaciones de seguridad. Los registros de incidencias se cambian a las notificaciones a la Agencia Española de Protección de Datos en un plazo máximo de 72 horas y en caso de que estén implicados datos de carácter sensible a los terceros implicados. Lo que se quiere conseguir con la ampliación de estos derechos es que la ciudadanía tenga mayor control y puedan tomar decisiones sobre los datos personales que

[20] Artículo 7, Reglamento 2016/679 del Parlamento Europeo y del Consejo de 27 de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

impartan con terceros. El RGPD introduce iniciativas en cuanto a las medidas de seguridad, como copias de seguridad, procesos de verificación, reducción de información confidencial en la red.

e) Introducción de la figura del Delegado de Protección de Datos, viene recogida en los artículos 37 y 39 del RGPD. Es una nueva figura de responsabilidad con más funciones que los responsables de seguridad.
El Delegado de Protección de Datos, puede ser miembro tanto de un núcleo empresarial como también un tercero contratado desde el exterior, con un contrato de servicios. Este se insertará en los ámbitos donde se tratan datos de carácter personal a gran escala que requieren tratamientos y un seguimiento habitual y sistemático.

4. Principios y derechos

A) Los principios del tratamiento de datos

Entre los principios que se regulan en el RGPD y el Proyecto de Ley Orgánica de Protección de Datos se halla los siguientes:

a) Principios de licitud, lealtad y transparencia

Estos principios se encuentran recogidos en los artículos 5 y 7 del Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal y art 5 y 6 RGPD. Desde el punto de vista general, la licitud implica el cumplimiento de una serie de medidas tasadas en los artículos mencionados: cumplimiento de deberes de conservación, fines de tratamiento legales, adopción de medidas de seguridad oportunas, etc.

El artículo 5[21] del Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal, recoge que el tratamiento de los datos *"no debe ser sólo legal, sino también leal"*, esto implica que el interesado o el titular de los datos tiene que ser informado de forma clara precisa e inequívoca. Pero la lealtad implica más supuestos, ya que aquí también podríamos hablar de la responsabilidad de la administración en el momento de que esta efectúe un uso desleal de los datos de carácter personal.

[21] Artículo 5 del Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal

En cuanto a la transparencia en el tratamiento de los datos, nos referimos a los informes y resoluciones, tienen que estar transcritos de forma clara y sencilla, para que se pueda entender fácilmente. La información que se cede tiene que disponer de fácil acceso para los perjudicados, tienen que contener los derechos que se le otorgan, el tratamiento, las medias, etc.

b) Principio de finalidad del tratamiento

Las finalidades se distinguen en dos clases, por una parte, finalidades genéricas y por otra parte las finalidades individuales. Según el artículo 6.I.a) del RGPD, las finalidades individuales, son las siguientes:

- cumplimiento de obligaciones legales del responsable,
- la protección de intereses vitales de las personas físicas,
- cumplimiento de responsabilidades conferidas al responsable del tratamiento;

Mientras que las finalidades genéricas son:

- la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o un tercero,
- aplicación de medidas precontractuales;

A todo esto, tenemos que añadir otros desenlaces, como por ejemplo, desenlaces estadísticos, científicos e históricos.

Estas finalidades han de ser expuestas de manera determinada, explicita y legitima.

c) Principios de adecuación, conservación y exactitud de los datos

Los datos personales, tienen que basarse en el principio de minimización de los datos, este integra que dichos datos tienen que ser manipulados de forma adecuada, pertinente, legitima y explicita. Han de ser compatibles con la originaria.

Además los datos tienen que estar actualizados y exactos (RGPD art.5.I.d).

En el momento que se cumplen los fines del tratamiento, estos tienen que ser cancelados, al no ser que se conservan para fines de investigación científica, histórica, estadísticos o tienen fines de interés público. De ahí la necesidad de implantar el principio de limitación del plazo de conservación de los datos[22]

[22] RLOPD, Artículo 22. Conservación de los datos por el encargado del tratamiento.

1. Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento o al encargado que éste hubiese designado,

d) Deber de información

A los responsables de protección de datos se les otorga el deber de información. Según el RGPD, los responsables tienen la obligación de informar a los siguientes individuos:

- A los interesados y a otros responsables
- A otros responsables de tratamiento
- A la Autoridad de Control
- Encargados del tratamiento
- Organismos de supervisión
- Comité

Estas informaciones han de ser expuestas de forma clara, concisa, trasparente, inteligible (RGPD artículo 12). Cabe hacer hincapié que el deber de recibir la información está íntimamente ligado con el principio de consentimiento.

e) Principio del consentimiento, en los tratamientos habituales o generales

El consentimiento de los interesados es muy importante. En primer lugar, el consentimiento ha de ser acreditado e inequívoco. Y de aquí la especial relación con el deber de información del delegado de protección de datos, ya que este tiene que poder manifestar que el titular presto su consentimiento. Por otro lado, la AEPD, resaltó que por inequívoco se entiende la expresa existencia del consentimiento ya que este no se puede deducir. Además el consentimiento ha de ser táctico, específico e informado.

El principio del consentimiento en los tratamientos habituales o generales está recogido en los artículos 4, 7 y 8 del RGPD.

---

al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.

No procederá la destrucción de los datos cuando exista una previsión legal que exija su conservación, en cuyo caso deberá procederse a la devolución de los mismos garantizando el responsable del fichero dicha conservación.

2. El encargado del tratamiento conservará, debidamente bloqueados, los datos en tanto pudieran derivarse responsabilidades de su relación con el responsable del tratamiento.

f) Principio de responsabilidad proactiva

En el artículo 5.2 el RGPD recoge *"el responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado I*[23] *y capaz de demostrarlo"*. El delegado de protección de datos tiene que evaluar los riesgos previamente a realizar el tratamiento y aplicar las medidas necesarias.

B) Derechos

El RGPD amplía los derechos. A los derechos denominados derechos ARCO – acceso, rectificación, cancelación y oposición – se les ha añadido tres derechos más, el derecho al olvido, el de limitación y el de portabilidad de los datos.

La AEPD, considera que el derecho al olvido está incluido en el derecho de cancelación.

a) Derecho de acceso

El derecho de acceso se encuentra recogido en el artículo 15, RGPD. Se entiende por derecho de acceso, que el interesado tenga libre acceso a la información que se va tratar, a las finalidades de los tratamientos, los plazos de conservación, la existencia de otros responsables involucrados, también tiene que conocer que tiene acceso a estar en contra del tratamiento que se va realizar, de imponer una reclamación, el derecho a obtener copia.

[23] El apartado 1 del artículo 5 del RGPD recoge: "1. Los datos personales serán: a) tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»); b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales («limitación de la finalidad»); c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»); d) exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan («exactitud»); e) mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado («limitación del plazo de conservación»); f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»).

b) Derecho de rectificación

El derecho de rectificación implica la corrección de los datos incorrectos y además se pueden completar los que sean incompletos, basándonos en los fines del tratamiento. El derecho de rectificación se encuentra recogido en el artículo 16 del RDPD.

c) Derecho de suspensión ("el derecho al olvido")

El derecho de cancelación lo encontramos en el precepto 17 del RGPD, donde se establece que los datos de carácter personal se pueden cancelar o suprimir, en diferentes circunstancias, ya sea, cuando las finalidades del tratamiento son distintas a las que se establecieron o estas llegaron a su fin. También cuando el interesado este en contra de dicho tratamiento y no exista motivos legítimos del mismo. Otra circunstancia importante viene a establecer que se tienen que cancelar los datos una vez que el interesado retire el consentimiento. Además cuando los datos se hayan obtenido o hayan sido tratados ilícitamente.

Cabe destacar que estas circunstancias no son de aplicación cuando el tratamiento de los datos de carácter personal son para el ejercicio del derecho a la libertad de expresión e información, cuando se trata de una obligación legal o exista un interés público o fines de investigación científica, histórica o fines estadísticos. Por último, también se integra el supuesto para la defensa de las reclamaciones.

d) Derecho de oposición

El derecho a la oposición integra los derechos mencionados anteriormente, ya que este puede oponerse en cualquier momento al tratamiento. Por lo tanto, se cancelaran sus datos. Las causas del tratamiento al que los interesados se podrán oponer están recogidos en el artículo 6.1, apartado e) o f) del RGPD[24]. En estas circunstancias el delegado de protección de datos tendrá que dejar de tratar dichos derechos salvo en los casos que he mencionado en el apartado del derecho de suspensión.

[24] Artículo 6.1 del RGPD: "e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento; f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño."

e) Derecho a la limitación

Según el artículo 18, del RGPD, se podrá limitar el tratamiento en los siguientes casos. En el caso de que el tratamiento sea ilícito, los datos sean inexactos, cuando el interesado necesite los dados para la formulación de las reclamaciones o cuando este se haya opuesto al tratamiento.

f) Derecho a la portabilidad

El artículo 20, del RGPD defiende el derecho a la portabilidad de datos, este derecho implica que el interesado podrá recibir los datos personales en un formato de uso común y lectura mecánica para que este pueda transmitirlos a otro responsable. Además los interesados tienen derecho a que los datos se trasmitan de un responsable a otro directamente.

III Data Protection Officer vs Compliance Officer

Generalmente, las funciones del DPO corresponden con las funciones del CO. Las dos figuras tienen encomendadas tareas preventivas, de formación y de detección de infracciones, en la materia que le es propia a cada uno. Ambas juegan un papel importante en su relación con la AEPD[25]. También uno de los requisitos fundamentales es el de la independencia, tanto el CO como el DPO, tienen que tener un alto grado de independencia dentro de las distintas organizaciones para poder realizar sus funciones con éxito.

Según Cecilia Álvarez, presidenta de la Asociación Profesional de Privacidad (APEP), las funciones del DPO con las del CO, no son compatibles: *"Yo nunca he visto al DPO como a un Compliance officer", explica Álvarez, para quien las funciones de ambos profesionales "no tienen nada que ver". Si bien ambos pueden compartir el nexo común de garantizar el cumplimiento normativo en sus respectivas materias y, en consecuencia, evitar sanciones, el Compliance officer no desarolla "un trabajo de estrategia", algo que sí*

[25] RALLO LOMBARTE, Artemio, y GARCÍA MAHAMUT, Rosario: *Hacia un nuevo derecho europeo de protección de datos,* Tirant lo Blanch, Valencia, 2015, pp. 258 y ss.

desempeña un DPO, que es una figura que puede aportar valor por lo que, además, debe buscarse, entre sus habilidades y competencias, que tenga "visión de negocio".[26]

El dictamen WP 243 recomienda pedir asesoramientos a los DPO en materia de protección de datos para reducir los riesgos de los tratamientos en los programas de corporate Compliance.[27].

1. Data Protection Officer

El Data Protection Officer – Delegado de Protección de Datos- , es una de las grandes novedades del RGPD. Según la AGPD, *"es uno de los elementos claves del RGPD, y un garante de cumplimiento de la normativa de protección de datos en las organizaciones."*[28] Entendemos por datos de carácter personal, cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables.[29]

El RGPD define los datos personales como: *"«datos personales»: toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;".*[30]

---

[26] "EL DPO es estratégico para las empresas" Protección de datos, IURIS&LEX, 12/Mayo/2017 http://www.apep.es/wp-content/uploads/2016/02/El-Economista-Iuris-12-5-17.pdf [Fecha consulta: 09/04/2018]

[27] ARTICLE 29 DATA PROTECTION WORKING PARTY 16/E WP243, Guidelines on Data Protection Officers ("DPOs") Adopted on 13 December 2016. http://ec.europa.eu/justice/data-protection/index_en.htm [Fecha de consulta: 09/04/2018]

[28] AGPD, "Qué es un Delegado de Protección de Datos" 24/04/2017, https://www.agpd.es. [Fecha de consulta: 06/03/2018]

[29] AGPD, Canal del responsable de ficheros , Glosario de términos, https://www.agpd.es/portalwebAGPD/canalresponsable/inscripcion_ficheros/preguntas_frecuentes/glosario/index-ides-idphp.php [Fecha de consulta: 15/04/2018]

[30] Artículo 4 RGPD

La nueva figura del delegado de protección de datos está recogida en los artículos 37 y 39 del RGPD, se basa en los principios legalidad e integridad, profesionalidad, responsabilidad, imparcialidad, transparencia y confidencialidad[31].

Hasta el momento, no se ha encontrado ninguna definición concreta del concepto de DPO, ya que ni el Reglamento ni las directrices recogen ninguna definición explicita. En cambio, la **Comisión Europea**, define la figura del Delegado de Protección como *"una persona responsable en el seno de un responsable o un encargado del tratamiento de supervisar y monitorear de una forma independiente la aplicación interna y el respeto de las normas sobre protección de datos. El DPO puede ser tanto un empleado como un consultor externo*"[32] que velara por la seguridad de los datos personales en la empresa.
El DPO tiene que poseer diferentes habilidades y conocimientos, conocimientos en derecho nacional y europeo, además de la práctica en materia de protección de datos personales y experiencia en los tratamientos de datos, tiene que facilitar la innovación y la competitividad.

Cabe diferenciar entre las funciones de las Autoridades de Protección y las de DPO's. Las Autoridades de Protección de Datos tienen la función de suscitar formación adecuada y regular para los DPO, además estas tendrán que velar por los derechos y libertades fundamentales de las personas físicas, mientras que a los DPO's se les incumben las siguientes funciones[33]:

- *Informar y asesorar del tratamiento al responsable y a los empleados,* Formación a los recursos humanos de la organización, el DPO tiene como función estar en continuo contacto con los responsables de los tratamientos y los empleados para informarles y asesorarles de los tratamientos y de las obligaciones que les incumben.

- *Supervisar el cumplimiento de las políticas del Reglamento.* Son los encargados de velar por el cumplimiento de la normativa y en efecto de hacerse cumplir el

[31] Artículo 2 del Código Ético de las personas certificadas como delegados de protección de datos conforme al esquema de la Agencia Española de Protección de datos
[32] Diario LA LEY LEGAL MANAGEMENT, nº2, enero 2017, Nº2, 20 de ene. de 2017, Editorial Wolters Kluwer, [Fecha de consulta 20/03/2018]
[33] El artículo 39 del RGPD, "Funciones del delegado de protección de datos".

principio de *accountability* (responsabilidad proactiva), además tienen la obligación de supervisar las autorías de correspondientes, la asignación de responsabilidades, etc.

- *Ofrecer el asesoramiento sobre la evaluación de impacto.* Tienen encomendada la realización de informes, elaboración de Evaluaciones de impacto de privacidad y la función de implementación de la privacidad por diseño y por defecto.

- *Cooperar y actuar como punto de contacto de la autoridad de control,* realizar consultas a la autoridad de control, actuar como punto de contacto con las autoridades de control y otras cuestiones, etc.

Las anteriores funciones del DPO, se pueden complementar en tareas de asesoramiento y supervisión en distintas áreas: cumplimiento de principios relativos al tratamiento, identificación de las bases jurídicas de los tratamientos, valoración de compatibilidad de finalidades distintas de las que originaron la recogida inicial de los datos, valoración de solicitudes, análisis de riesgo de los tratamientos realizados, realización de evaluaciones de impacto sobre protección de datos, implantación de programas de formación y sensibilización del personal en materia de protección de datos, identificación de los instrumentos de trasferencia internacional de datos adecuados a las necesidades y características de la organización y de las razones que justifiquen la transferencia, etc..[34]

2. Compliance Officer

Compliance Officer, o también llamado "controller jurídico o controller legal", es la persona o el comité de personas responsables del cumplimiento normativo.[35]

Los modelos preventivos se elabora conforme a los estándares internacionales establecidos por la Norma UNE-ISO 19601:2017, sobre sistemas de gestión de *Compliance*. Es una norma internacional que proporciona la guía para los sistemas de gestión de *Compliance* y las prácticas recomendadas. Se basa en los principios de buen

[34] EL DELEGADO DE PROTECCIÓN DE DATOS EN LAS ADMINISTRACIONES PUBLICAS, Agencia Española de Protección de Datos, Madrid 19 de mayo de 2017 https://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/Funciones_DPD_en_AAPP.pdf [Fecha de consulta:30/04/2018]

[35] ALAYA DE LA TORRE, José Mª, *Compliance, Claves Prácticas* Francis Lefebvre, 2ª Ed. 2018 pp. 26 y ss.

gobierno, proporcionalidad, transparencia y sostenibilidad. Establece las directrices para implantar, evaluar, mantener y mejorar un sistema de gestión eficaz, al tiempo que propone los elementos que la organización debería integrar para asegurar su cumplimiento.[36]

El *Compliance Officer* o Controlador del cumplimiento del Modelo de Prevención del Delito por la persona jurídica: será el responsable de proveer o coordinar los entrenamientos continuos en materia de cumplimiento normativo, así como la figura que dará soporte en el caso de dudas sobre cómo proceder o si cierta conducta constituye o no una infracción al *Compliance*.

Si bien es cierto que la responsabilidad de diseñar e implantar el modelo preventivo en la organización es una competencia indelegable del órgano de administración, nada obsta a que este órgano pueda encargar al *Compliance officer*, bajo su supervisión, la confección y realización del modelo. En ningún caso, será función del *Compliance officer* la reacción disciplinaria ante el incumplimiento del programa, sin perjuicio del apoyo que deba prestar a los órganos de garantías.

Son funciones específicas del *Compliance Officer* (CO)[37] las siguientes:

a) Gestión del modelo preventivo:

1) *La supervisión del funcionamiento y cumplimiento del modelo*: la verificación de que el mapa de riesgos en base al que se ha diseñado todo el modelo es fruto de una adecuada valoración de los mismos. Una correcta gestión del modelo obligará, además, al CO a asesorar e informar en toda aquella toma de decisiones que tenga que ver con la organización interna, y pudiera tener relevancia a efectos de cumplimiento normativo, enfocando dicho asesoramiento desde el punto de vista de los riesgos penales. Para ello, deberá inculcar al personal de la empresa, la necesidad y repercusión que para la compañía pudiera tener el incumplimiento del modelo, y asegurarse de que les llegue fluidamente la necesaria información desde los ámbitos con riesgo de repercusión penal.

2) *La vigilancia y control del personal sometido al Compliance Officer personal:* Por personal de la compañía debe entenderse no sólo la plantilla con relación laboral o dependencia, sino a cualquier otro, que se encuentre bajo el ámbito de dirección del órgano de

[36] ALAYA DE LA TORRE, José Mª, *Compliance*,…cit., pp. 23 y ss

[37] Según el artículo 10, Norma Española UNE 19601, mayo de 2017, Sistema de gestión de Compliance penal, Requisitos con orientación para su uso.

administración (colaboradores externos). Y para evitar la posible responsabilidad penal de la persona jurídica por los delitos cometidos por sus representante legales o por los autorizados para tomar decisiones en su nombre o los que ostentan facultades de organización y control dentro de la misma, y teniendo en cuenta que la persona jurídica podría eximirse de su responsabilidad si lograra acreditar que tiene establecido un programa eficaz de cumplimiento, estos representantes también deben de estar sometidos al control del *Compliance Officer* y al cumplimento de las normas del programa de prevención, interpretando esta vigilancia y control en el sentido de asesoramiento y recomendación, no de función ejecutiva.

b) Información y formación sobre el Modelo de Prevención:

Una de las obligaciones más importantes de CO penal es divulgar entre el personal de la empresa el contenido del programa de prevención penal.

Para ello, el CO deberá redactar un manual, que se deberá divulgar entre todo el personal de la empresa. Ahora bien, entendemos que tampoco es necesario que todo el personal de la empresa, conozca, la totalidad del manual o del programa, sino únicamente aquella parte que pueda afectar a cada departamento (financiero, administrativo, tecnológico, de producción, etc…). Aunque habrá alguna parte genérica que deberá ser de general conocimiento.

Otra cuestión trascendental es la formación del personal en el cumplimiento normativo, a cuyo efecto, bien directamente, o bien subcontratando o externalizando el servicio, el CO deberá responsabilizarse de que periódicamente se forme a todo el personal de la empresa en todos los aspectos relativos que puedan afectar en su actividad, al cumplimiento normativo penal.

c) Revisión y modificación del modelo de prevención:

Fruto del seguimiento pormenorizado y del chequeo constante del grado de cumplimento en la compañía del modelo de prevención, será la rápida detección de situaciones de riesgo, o fallos del programa, incumplimientos del mismo o comportamientos irregulares que se pueden haber producido por deficiencias del programa. Detectados esos fallos, incumplimientos o comportamientos irregulares, es una de las principales obligaciones del

CO modificar el programa, o proponer su modificación al Órgano de Administración para que dichas anomalías no vuelvan a producirse, por lo tanto, este programa, se irá autoalimentando y enriqueciéndose precisamente con sus propias deficiencias, que cada vez, si se lleva a cabo esta fundamental labor, harán que el sistema de prevención de riesgos penales, sea más eficaz y permita evitar con mayor grado de fiabilidad que en el seno de la compañía se den conductas penales que puedan repercutir en su posible responsabilidad penal.

Por supuesto, cualquier variación en el mapa de riesgos, por una modificación legislativa, de cualquier índole, o por cualquier otro motivo, que pueda tener repercusión en la posible responsabilidad penal de la empresa, obligará a la adecuación del plan de prevención, y esta adecuación debe ser responsabilidad del CO penal. Así como cualquier cambio en la estructura de la empresa, o en su organización, o incluso en la actividad que desarrolla.

d) Gestión del canal de denuncias e investigaciones internas:

El Canal de denuncias es el sistema a través del cual se reciben las noticias de posibles comportamientos con relevancia penal, que pueden llegar, bien de los propios trabajadores o empleados de la compañía o del exterior, (clientes, colaboradores, proveedores, etc…). Y ello independientemente de dilucidar si la denuncia debe ser anónima o nominal.

Esta labor deber ser realizada sin ningún género de dudas por el CO penal, porque no deja de ser otra forma de detectar anomalías en el cumplimiento del programa que nos permitan modificar éste y hacerlo cada vez más eficiente y con mayor capacidad de coadyuvar a la exención de la responsabilidad penal de la compañía.

Además, todas estas denuncias y el resultado de las subsiguientes investigaciones, sin lugar a dudas, deben plasmarse en los correspondientes informes, y toda la información y conclusiones obtenidas, deben ser material muy valioso para modificar y adaptar el programa al mejor cumplimiento de su verdadera finalidad. Todo ello sin perjuicio de la necesaria y estricta confidencialidad con el que se deben llevar a cabo estas tareas.

3. Responsabilidades criminales: de las personas jurídicas en materia de protección de datos y del CO y DPO

Con la responsabilidad penal de las personas jurídicas se completa un círculo de la respuesta punitiva del Estado frente al potencial criminógeno, la capacidad de amplificación del daño y el aseguramiento de la impunidad que pueden derivarse del mal uso de las formas colectivas dotadas de personalidad jurídica.

Nos remitimos a la legislación civil para poder entender el concepto de persona jurídica. El artículo 35 del Código Civil establece:

"*Son personas jurídicas:*

1. Las corporaciones, asociaciones y fundaciones de interés público reconocidas por la Ley. Su personalidad empieza desde el instante mismo en que, con arreglo a derecho, hubiesen quedado válidamente constituidas.

2. Las asociaciones de interés particular, sean civiles, mercantiles o industriales, a las que la Ley conceda personalidad propia, independiente de la de cada uno de los asociados (…)".

La responsabilidad penal de las personas jurídicas se introduce por primera vez en el ordenamiento jurídico español en el año 2010, con la reforma del CP, LO 5/2010, de 22 de junio.[38] Se encuentra recogida en su artículo 31 bis.

Posteriormente, la reforma del CP, realizada por la LO 7/2012, de 27 de diciembre, modifica nuevamente la redacción del artículo 31 bis, apartado 5º párrafo 1.

La última reforma de nuestro CP, se llevó a cabo por la LO 1/2015, de 30 de marzo. En su materia relacionada con la responsabilidad de las personas jurídicas, introduce nuevos artículos 31 ter, 31 quater y, 31 quinquies, así como, modifica el artículo 31 bis.

Esta reforma quiere mejorar el sistema de responsabilidad de las personas jurídicas, se mantienen los dos supuestos de responsabilidad, por una parte los delitos cometidos por los representantes legales de la persona jurídica[39] y los delitos cometidos por los

[38] BOE Ley Orgánica 5/2010, de 22 de junio, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

[39] Artículo 31 bis 1 a) del CP "*a) De los delitos cometidos en nombre o por cuenta de las mismas, y en su beneficio directo o indirecto, por sus representantes legales o por aquellos que actuando individualmente o como integrantes de un órgano de la persona jurídica, están autorizados para*

empleados en los supuestos de incumplimientos graves en materias de supervisión, vigilancia y control[40].

En los últimos años, la ley penal ha cambiado a una gran velocidad, pasando de la tradicional defensa penal corporativa a la defensa penal preventiva. Es decir, esta defensa penal preventiva utiliza métodos de defensa integral a través de los Programas de Cumplimiento Penal y de Prevención de Delitos.[41]

El apartado 2 del artículo 31 bis, el legislador introduce unas condiciones que han de cumplirse para la exención de responsabilidad:

- Que el órgano administrativo haya adoptado y ejecutado un modelo de organización y gestión que incluya la prevención del delito.[42]
- Una supervisión que demuestre el correcto funcionamiento del modelo, el cumplimiento del dicho por parte de un órgano específico con poderes autónomos de control o un órgano con funciones de control interno.[43]
- Que la persona física haya eludido fraudulentamente los modelos de prevención.[44]
- Que el órgano de vigilancia y control haya ejercido la diligencia debida[45]

En cuanto a los **requisitos legales** de los modelos de organización y gestión, el CP reúne distintos requisitos legales[46].

---

tomar decisiones en nombre de la persona jurídica u ostentan facultades de organización y control dentro de la misma."

[40] Artículo 31 bis 1 b) del CP "*b) De los delitos cometidos, en el ejercicio de actividades sociales y por cuenta y en beneficio directo o indirecto de las mismas, por quienes, estando sometidos a la autoridad de las personas físicas mencionadas en el párrafo anterior, han podido realizar los hechos por haberse incumplido gravemente por aquéllos los deberes de supervisión, vigilancia y control de su actividad atendidas las concretas circunstancias del caso."*

[41] GONZÁLEZ CUSSAC José L., *Comentarios a la reforma del Código Penal de 2015*. Actualizada con la corrección de errores (BOE 11 de junio de 2015). 2ª Ed. 2015. [Fecha de consulta: 17/04/18]

[42] "Artículo 31 bis 2 1ª del CP "*1.ª el órgano de administración ha adoptado y ejecutado con eficacia, antes de la comisión del delito, modelos de organización y gestión que incluyen las medidas de vigilancia y control idóneas para prevenir delitos de la misma naturaleza o para reducir de forma significativa el riesgo de su comisión;"*

[43] Artículo 31 bis 2, 2ª del CP "2.ª *la supervisión del funcionamiento y del cumplimiento del modelo de prevención implantado ha sido confiada a un órgano de la persona jurídica con poderes autónomos de iniciativa y de control o que tenga encomendada legalmente la función de supervisar la eficacia de los controles internos de la persona jurídica;"*

[44] Artículo 31 bis 2, 3ª del CP "3.ª *los autores individuales han cometido el delito eludiendo fraudulentamente los modelos de organización y de prevención y"*

[45] Artículo 31 bis 2, 4ª del CP "4ª *no se ha producido una omisión o un ejercicio insuficiente de sus funciones de supervisión, vigilancia y control por parte del órgano al que se refiere la condición 2ª"*

Cada uno de los citados requisitos va a ser estudiado a continuación comparando su regulación por la Fiscalía General del Estado[47] y la novedosa Norma UNE-ISO 19601:2017:

1) Identificar las actividades que pueden incurrir en actos ilícitos[48]

La Circular de la Fiscalía General del Estado núm. 1/2016 dice al respecto:[49]

«La persona jurídica deberá establecer, aplicar y mantener procedimientos eficaces de gestión del riesgo que permitan identificar, gestionar, controlar y comunicar los riesgos reales y potenciales derivados de sus actividades de potenciales derivados de sus actividades de acuerdo con el nivel de riesgo global aprobado por la alta dirección de las entidades, y con los niveles de riesgo específico establecidos. Para ello el análisis identificará y evaluará el riesgo por tipos de clientes, países o áreas geográficas, productos, servicios, operaciones, etc., tomando en consideración variables como el propósito de la relación de negocio, su duración o el volumen de las operaciones. En las empresas de cierto tamaño, es importante la existencia de aplicaciones informáticas que controlen con la máxima exhaustividad los procesos internos de negocio de la empresa. En general, pues depende del tamaño de la empresa, ningún programa de Compliance puede considerarse efectivo si la aplicación central de la compañía no es mínimamente robusta y ha sido debidamente auditada.»

La Norma UNE 19601 relaciona directamente el apartado del artículo 31 bis 5 numeral 1 con:

- Determinación del alcance del sistema de gestión de Compliance penal (con especial referencia a los resultados de la evaluación de riesgos penales),

---

[46] Artículo 31 bis 5 del CP "*5. Los modelos de organización y gestión a que se refieren la condición 1.ª del apartado 2 y el apartado anterior deberán cumplir los siguientes requisitos:"*

[47] Circular FGE 1/2016, sobre la Responsabilidad Penal de las Personas Jurídicas conforme a la Reforma del Código Penal efectuada por la Ley Orgánica 1/2015.

[48] Artículo 31 bis 5, 1º del CP, "*1º Identificarán las actividades en cuyo ámbito puedan ser cometidos los delitos que deben ser prevenidos."*

[49] Especial eficacia y certificación de los programas de Compliance penal, redacción Wolters Kluwer http://www.smarteca.es/myreader/SMT2017011_00000000_0?fileName=content%2FEX0000120949_20170518.HTML&location=pi-31 [Fecha de consulta: 22/03/2018]

- Política de Compliance penal (apartado c), haciendo hincapié en la identificación de las áreas con riesgos de actividad delictiva para poder prevenirlo,
- Identificación, análisis y evaluación de riesgos penales (identificar los riesgos penales que pueden afectar a la organización),
- Diligencias debida, desarrollar el análisis para detectar las actividades donde se plasman ilícitos penales.

2) **Establecer los protocolos o procedimientos adaptándolos a la formación de la persona jurídica en materia toma de decisiones y ejecución de las mismas[50]**

.

Sobre este requisito la Circular 1/2016, de la FGE interpreta:

«Tales procedimientos deben garantizar altos estándares éticos, de manera singular en la contratación y promoción de directivos y en el nombramiento de los miembros de los órganos de administración. Además de la obligación de atender a los criterios de idoneidad fijados por la normativa sectorial y, en defecto de tales criterios, la persona jurídica debe tener muy en consideración la trayectoria profesional del aspirante y rechazar a quienes, por sus antecedentes carezcan de la idoneidad exigible».

La Norma UNE 19601 relaciona directamente el apartado del artículo 31 bis 5 numeral 2 con:

- El órgano de gobierno (Apartado g), es decir, la organización, voluntariamente, tiene que concretar el proceso, tomar decisiones y concretar las mismas.

3) Tener modelos de gestión adecuados que impidan la comisión de hechos delictivos[51]

[50] Artículo 31 bis 5, 2º del CP "*2º Establecerán los protocolos o procedimientos que concreten el proceso de formación de la voluntad de la persona jurídica, de adopción de decisiones y de ejecución de las mismas con relación a aquéllos"*

[51] Artículo 31 bis 5, 3º del CP "*3º Dispondrán de modelos de gestión de los recursos financieros adecuados para impedir la comisión de los delitos que deben ser prevenidos."*

4) Información continua de los riesgos e incumplimientos al organismo encargado de vigilar[52]

La Circular 1/2016, de la FGEº entiende:

«La existencia de unos canales de denuncia de incumplimientos internos o de actividades ilícitas de la empresa es uno de los elementos clave de los modelos de prevención. Ahora bien, para que la obligación impuesta pueda ser exigida a los empleados resulta imprescindible que la entidad cuente con una regulación protectora específica del denunciante (whistleblower), que permita informar sobre incumplimientos varios, facilitando la confidencialidad mediante sistemas que la garanticen en las comunicaciones (llamadas telefónicas, correos electrónicos…) sin riesgo a sufrir represalias».

La Norma UNE 19601 relaciona directamente el apartado del artículo 31 bis 5 numeral 3 con:

- Órgano de gobierno Apartado c), relativo a la dotación al sistema de gestión de Compliance penal, de los recursos financieros, materiales y humanos adecuados y suficientes.
- Alta dirección Apartado c) disponibilidad de los recursos necesarios para ejecutar eficazmente el sistema de gestión del Compliance.
- Objetivos de prevención de delitos y planificación para lograrlos, para poder prevenir hay que invertir y evitar la materialización de los riesgos penales.
- Controles financieros, relativos a los sistemas implantados.

En cuanto al apartado del artículo 31 bis 5 numeral 4 la Norma UNE lo relaciona con:

- Alta dirección, apartado h) con el objetivo de fomentar el uso de los procedimientos para el conocimiento de futuras conductas delictivas.
- Política de Compliance penal Apartado h), relativo a la obligación de informar sobre hechos o conductas sospechosas relativas a riesgos penales.
- Comunicación de incumplimiento e irregularidades, canales de comunicación y procedimientos asociados con ellos.

[52] Artículo 31 bis 5, 4º del CP "*4º Impondrán la obligación de informar de posibles riesgos e incumplimientos al organismo encargado de vigilar el funcionamiento y observancia del modelo de prevención.*"

5) Sistema disciplinario[53]

La Circular 1/2016, de la FGEº concreta:

«Presupone la existencia de un código de conducta en el que se establezcan claramente las obligaciones de directivos y empleados. Las infracciones más graves, lógicamente, serán las constitutivas de delito, debiendo contemplarse constitutivas de delito, debiendo contemplarse también aquellas conductas que contribuyan a impedir o dificultar su descubrimiento así como la infracción del deber específico de poner en conocimiento del órgano de control los incumplimientos detectados a que se refiere el requisito cuarto».

La Norma UNE 19601 relaciona directamente el apartado del artículo 31 bis 5 numeral 5 con:

- Alta dirección Apartado d), cumplimiento de la política del Compliance interna y externa,
- Política de Compliance penal Apartado K), expone las consecuencias de no cumplir con los requisitos de la política de Compliance penal y del sistema de gestión,
- Diligencia debida común a todos los miembros de la organización Apartado d), adopción de acciones disciplinarias proporcionales.

6) Realizaciones periódicas con sus respectivos cambios, en situaciones de cambios en la organización, concurrencia de infracciones, etc. [54]

La Circular 1/2016, de la FGEº especifica:

«Aunque el texto no establece plazo ni procedimiento alguno de revisión, un adecuado modelo de organización debe contemplarlos expresamente. Además, el modelo deberá ser revisado inmediatamente si concurren determinadas circunstancias que puedan influir en el análisis de riesgo, que habrán de detallarse y

[53] Artículo 31 bis *5, 5º del CP "5º Establecerán un sistema disciplinario que sancione adecuadamente el incumplimiento de las medidas que establezca el modelo."*

[54] Artículo 31 bis 5, 6º del CP "*6º Realizarán una verificación periódica del modelo y de su eventual modificación cuando se pongan de manifiesto infracciones relevantes de sus disposiciones, o cuando se produzcan cambios en la organización, en la estructura de control o en la actividad desarrollada que los hagan necesarios."*

que incluirán, además de las indicadas en este requisito, otras situaciones que alteren significativamente el perfil de riesgo de la persona jurídica (por ej., modificaciones en el Código Penal que afecten a la actividad de la corporación)».

La Norma UNE 19601 relaciona directamente el apartado del artículo 31 bis 5 numeral 6 con:

- Órgano de gobierno Apartado e) evaluar la eficacia,
- Evaluación de los riesgos penales, adoptar medidas para remediar deficiencia de los controles,
- Auditoría interna,
- Revisión por el órgano de Compliance penal, actividades de supervisión y evaluación periódica de sistema de gestión penal,
- Revisión por la alta dirección, revisa la información emitida por el CO y los resultados de las auditorias llevadas a cabo,
- Revisión por el órgano de gobierno, examen periódico al sistema de gestión,
- Mejora, acciones de mejora ante no conformidades.

La nueva regulación ha implantado la necesidad de tener sistemas de gestión y control aplicados al ámbito de prevención y detección penal. La Norma UNE-ISO 19601:2017 establece sistemas de gestiones de Compliance penal adecuados a la legislación española (CP), además de que completa los estándares internacionales en esta materia con la finalidad de incrementar la eficacia. [55]

Este sistema de gestión del Compliance penal, tiene como objetivo eliminar o prevenir los riesgos penales, a través de la implementación de una política de Compliance dentro de la organización. Esta norma tiene dos finalidades básicas, una finalidad preventiva (evitar la responsabilidad de la persona jurídica) y una finalidad reputacional (desde su introducción deja claro que aspira cumplir con los estándares internacionales en materia de Compliance)[56]

[55] Norma Española UNE 19601, mayo de 2017, Sistema de gestión de Compliance penal, Requisitos con orientación para su uso. [Fecha de consulta 16/04/2018]
[56] ALAYA DE LA TORRE, José Mª, *Compliance*,...cit., pp. 61 y ss.

Responsabilidad penal del Compliance Officer [57]

Teniendo en cuenta de que el CO, tiene que ser considerado como un directivo más de la organización, concurre en una doble responsabilidad:

1. Interna, en su relación con la organización;
2. Externa, respeto a los terceros a quienes puede perjudicar con su actuación.

Cabe destacar que no todo incumplimiento de la prevención de los hechos delictivos da lugar a la responsabilidad del CO, ya que, hay casos donde el incumplimiento debe responsabilizar a la empresa por no cumplir el sistema implantado, pero, cuanto se yerra en la implantación del programa de Compliance y se derivan en daños a terceros o a la propia empresa, la responsabilidad es del mismo CO, ya que las funciones que este ha de cumplir, no solo son de prevenir los riesgos de la organización sino también los riesgos que puede afectar a terceros. Además éste tiene que denunciar los hechos ilícitos y evitarlos. Si no cumple con esta función, incurre en la figura del artículo 11 del CP, comisión por omisión.

Concluyendo, el Complince Officer es un asesor de cumplimiento normativo penal y no alcanza la condición ni la posición de garante, es decir, este no incurre en delito en su función de asesoramiento a la persona jurídica, exceptuando los casos de una convivencia activa en la acción delictiva, ya lo fuese como inductor, cooperador necesario o cómplice.[58] La condición de posición de garante la tiene el empresario[59]. Como señala GUTIERREZ PÉREZ, E., para sustentar la posición de garante de Compliance Officer se ha de acudir a la denominada <<delegación de funciones>> en el ámbito empresarial.[60]

Responsabilidad penal del Delegado de Protección de Datos.

El DPO no puede ser sancionado por llevar a cabo las funciones que se le son encomendadas. Según el Dictamen WP 243 del GT29, explica que aunque tenga

[57] ALAYA DE LA TORRE, José Mª, *Compliance*,…cit..,pp. 29 y ss.
[58] TORRAS COLL, José Mª, *Jurisprudencia aplicada a la práctica*, LA LEY Penal nº 130, enero-febrero 2018, Nº 130, 1 de ene. de 2018, Ed. Wolters Kluwer [Fecha de consulta 19/04/2018]
[59] VELASCO PERDIGONES, Juan C, *Nociones sobre cuestiones civiles y penales controvertidas en la responsabilidad penal de las personas jurídicas: el Compliance Officer, transparencia y prevención de la corrupción en las empresas y secreto profesional del abogado y blanqueo de capitales."* Revista Aranzadi Doctrinal num. 3/2018 parte Estudios, Ed. Aranzadi, S.A.U., Cizur Menor. 2018 [Fecha de consulta: 19/04/18]
[60] GUTIÉRREZ PÉREZ, E., *La figura del Compliance Officer. Algunas notas sobre su responsabilidad penal,* Diario La Ley 8653, Secc. Tribuna.2015. [Fecha de consulta:19/04/18]

inmunidad no queda excluido que sea despedido por su mala práctica en el desempeño de sus funciones. Con especial referencia al artículo 38.3 del RGPD, El DPO tiene que informar directamente al más alto nivel jerárquico.

El informe de la CEDPO (The Confederation of European Data Protection Organisations)[61] señala:

- *"El art. 38.3 estipula que el/la DPO informará directamente al más alto nivel jerárquico del responsable o del encargado. Esto requiere reforzar la autonomía y relevancia de los/las DPOs y requiere que la organización del responsable o del encargado vincule a los/las DPOs al más alto nivel jerárquico (como el Consejo de Administración o un miembro de este). Por ejemplo, la estructura organizativa debe garantizar que:*
- *El/la DPO tenga acceso directo a la alta dirección y sin filtros, esto es, sin nivel intermedio entre el/la DPO y la alta dirección. Esto ayudará a garantizar que los/las DPOs no tengan conflictos de intereses respecto a su función como DPO y por lo tanto gocen de suficiente protección en el desempeño de sus tareas.*
- *El respectivo Consejo o miembro del Consejo actúe como supervisor funcional y administrativo del/de la DPO, con responsabilidades respecto de las cuestiones relativas al personal y presupuesto del/de la DPO.*
- *La línea de reporte del/de la DPO a la alta dirección pueda ser claramente identificada (por ejemplo, en un organigrama)."*

4. Prevención en materia de protección de datos de carácter personal

La información y las nuevas tecnologías están dando un giro radical en las distintas organizaciones, a la hora realizar su actividad empresarial. Por eso se ha ido implantando los distintos sistemas para evaluar los riesgos. La AEPD determina el concepto de riesgo como *"un riesgo es la probabilidad de que una amenaza se materialice aprovechando una vulnerabilidad de los sistemas de información o, dicho de otra manera, la probabilidad de*

[61] Posición de CEDPO sobre el Delegado de Protección de Datos (DPO) en el Reglamento General de Protección de Datos (RGPD) 15 de febrero de 2017 http://www.apep.es/wp-content/uploads/2017/02/Posici%C3%B3n-de-CEDPO-sobre-el-DPO.pdf[Fecha consulta: 10/04/18]

que ocurra un incidente que cause un impacto con un determinado daño en los sistemas de información".[62]

Pero lo complicado aquí no es saber que significa un riesgo sino saber cuándo dicho riesgo se convierte en una vulneración de nuestros datos personales. Para ello nos remitimos a la norma ISO/EIC 27035:11 que establece el Estándar para la Gestión de Incidentes de Seguridad de la Información. Además el Reglamento, define este concepto en su artículo 4 como: *"toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales trasmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos".*[63]

Para evitar estos incidentes tanto el Delegado de Protección de Datos como el Compliance Officer estudian e implementan sus respectivos sistemas de prevención de riesgos.

Por un lado tenemos la **Evaluación del Impacto**, consecuencia del tratamiento de datos de carácter personal, que es función del DPO, mientras que, por otro lado encontramos los sistemas de gestión del Compliance penal, con sus respectivos mapas de riesgo.

La evaluación del Impacto, se caracteriza por sus distintos elementos, análisis de tecnologías, documentación, valoración de las finalidades de los tratamientos, consideraciones de los usos previos, los riesgos de privacidad de los usos de datos de carácter personal y el ciclo de vida de estos datos personales. Los riesgos que se pueden producir, tienen especial relación con la manera de implantar una correcta política de protección de datos y las violaciones de los derechos de las personas. El derecho a la intimidad personal y familiar es uno de ellos.[64] Estos derechos están protegidos en el Código Penal en el artículo 197, del delito de descubrimiento y revelación de secretos, incluido en el título X, de los Delitos contra la Intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio:

---

[62] Puyol Javier, El modelo de evaluación de riesgos en la protección de datos EIPD/PIA's, enero de 2018, www.tirantonline.com [Fecha de consulta: 22/04/18]

[63] Ciberseguridad, Ciberseguridad páctica. La notificación de violaciones de seguridad, Diario LA LEY LEGAL MANAGEMENT, nº7, junio 2017, Nº7, 23 de jun de 2017, Ed Wolters Kluwer [Fecha de consulta: 28/04/2018]

[64] Puyol Javier, El modelo de evaluación de riesgos en la protección de datos EIPD/PIA's, enero de 2018, www.tirantonline.com [Fecha de consulta: 22/04/18]

"1. El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales, intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.

2. Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.

3. Se impondrá la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores.

Será castigado con las penas de prisión de uno a tres años y multa de doce a veinticuatro meses, el que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realizare la conducta descrita en el párrafo anterior.

4. Los hechos descritos en los apartados 1 y 2 de este artículo serán castigados con una pena de prisión de tres a cinco años cuando:

a) Se cometan por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros; o

b) se lleven a cabo mediante la utilización no autorizada de datos personales de la víctima.

Si los datos reservados se hubieran difundido, cedido o revelado a terceros, se impondrán las penas en su mitad superior.

5. Igualmente, cuando los hechos descritos en los apartados anteriores afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen

racial o vida sexual, o la víctima fuere un menor de edad o una persona con discapacidad necesitada de especial protección, se impondrán las penas previstas en su mitad superior.

6. Si los hechos se realizan con fines lucrativos, se impondrán las penas respectivamente previstas en los apartados 1 al 4 de este artículo en su mitad superior. Si además afectan a datos de los mencionados en el apartado anterior, la pena a imponer será la de prisión de cuatro a siete años.

7. Será castigado con una pena de prisión de tres meses a un año o multa de seis a doce meses el que, sin autorización de la persona afectada, difunda, revele o ceda a terceros imágenes o grabaciones audiovisuales de aquélla que hubiera obtenido con su anuencia en un domicilio o en cualquier otro lugar fuera del alcance de la mirada de terceros, cuando la divulgación menoscabe gravemente la intimidad personal de esa persona.

La pena se impondrá en su mitad superior cuando los hechos hubieran sido cometidos por el cónyuge o por persona que esté o haya estado unida a él por análoga relación de afectividad, aun sin convivencia, la víctima fuera menor de edad o una persona con discapacidad necesitada de especial protección, o los hechos se hubieran cometido con una finalidad lucrativa."

Para establecer un mapa de riesgo de la comisión de estos actos delictivos en un sistema de gestión de Compliance, nos tenemos que remitir a la Norma UNE-ISO 19601:2017 para identificar las características principales: identificación de riesgos, evaluaciones de impacto y de la frecuencia, priorización de riesgos e implementación de planes de mitigación con especial relación al seguimiento y la reevaluación.

En la Tabla I, abajo expuesta, la primera columna identifica el riesgo (el artículo) y la segunda columna la descripción del supuesto de hecho (el delito). En la tercera columna, analizaremos la frecuencia del riesgo en un horizonte de tiempo, **casi imposible,** corresponde al riesgo que se produce menos de una vez cada 5 años; **rara,** concierne a la posibilidad de que se produzca menos de una vez al año pero más de una vez cada 5 años; **posible,** probabilidad de que el riesgo se produzca cada año consecutivo; **incidente aislado,** atañe un riesgo de producción una vez al mes; mientras que los **incidentes repetitivos,** incumben los riesgos que se producen todas las semanas.

En la última columna, analizaremos el impacto en la organización, **bajo** – no afecta al funcionamiento de la organización (multa, sanción económica, indemnización a terceros) **medio** – afecta al funcionamiento de la organización (prohibición temporal de actividad en cuyo ámbito se realizó la actividad delictiva, suspensión temporal de la actividad) y por último, **grave** – afecta gravemente al funcionamiento de la organización, además de tener otras consecuencias negativas que no son del ámbito penal (prohibición definitiva de la actividad en cuyo ámbito se realizó el delito, clausura de locales, disolución de la organización).

Tabla I: Mapa de riesgo: Frecuencia e Impacto:

Artículo CP	**Delito**	**Frecuencia**	**Impacto**		
197 y ss.	Revelación de secretos y vulneración del derecho a la intimidad	Casi imposible	Bajo	Medio	Alto
		Rara			
		Posible			
		Incidentes aislados			
		Incidentes repetitivos			

Además del mapa de frecuencia e impacto, se podría proceder al análisis de la matriz de riesgos penales, en la cual analizaremos el riesgo penal, las acciones que pueden causar el riesgo, los procesos de la organización, los recursos a asignar y los planes mitigantes.
Tomamos por ejemplo, el artículo 197 y ss. Con carácter general, con relación al delito de descubrimiento y revelación de secretos, nos topamos con distintas acciones: Robo de información, divulgación de información confidencial, revelar o ceder a terceros secretos descubiertos, utilizar elementos de grabación, de escuchas, etc. y hacer uso indebido, etc..
En cuanto a los procesos, hay que destacar que son distintos en cada organización.
Los planes de mitigación pueden ser comunes tratando del delito arriba mencionado. Las organizaciones en los planes pueden incluir, formación por parte del CO y/o DPO, a los empleados y demás personal sujeto a la organización sobre la delimitación del uso

informático en relación con los datos de carácter personal. Facilitar manuales de protección de datos. Contratos de confidencialidad y cumplimiento del código ético.

Concluyendo, después de analizar la posibilidad de riesgos e impacto y los mecanismos de mitigación vamos a proceder al análisis del mapa de supervisión (Tabla II) que se llevará a cabo después de la implantación del sistema de gestión de cumplimiento.

En la primera columna de la Tabla II, vamos a identificar el riesgo delictivo, en la segunda columna, los controles actuales, es decir, aquellos controles que se han de llevar a cabo para revisar y supervisar el buen funcionamiento del sistema de Compliance penal. En la tercera columna, exponemos las medidas preventivas con su principal función de prevenir los riesgos penales detectados. En la cuarta columna identificamos la persona responsable y por último, la fecha de revisión.

Tabla II: Mapa de supervisión

Riesgo penal	Controles actuales	Medidas preventivas	Persona encargada	Fecha
197 y ss. Revelación de secretos y vulneración del derecho a la intimidad	Auditorías Internas	Canales de denuncias; Auditorias preventivas; Cláusulas de protección de datos conforme a la normativa “ficheros” (RGPD)	Compliance Officer Órgano directivo Encargado del Canal de denuncias Data Protección Officer	Xx/xx/xxxx

Finalizando, hacemos hincapié que cada organización tiene que disponer de un Informe de situación de inscripción en el registro general de la Agencia Española de Protección de Datos.

El RGPD y el Proyecto de LOPD, incluye que se ha de disponer de claves de seguridad, políticas de uso correcto de las páginas web, códigos de conducta, contratos de teletrabajos y modelos de contratos con el cliente.

Consecuentemente, hay que tener en cuenta que tanto los mapas de riesgos como las Evaluaciones de Impacto, no se pueden hacer a nivel general sino que se han de aplicar a cada organización en particular para conseguir resultados satisfactorios.

5. Salidas profesionales de un criminólogo

El perfil del CO[65]: básicamente, el Compliance Officer, tiene que tener un conocimiento multidisciplinar. En la mayoría de los casos se reclama un perfil jurídico, con amplios conocimientos del derecho penal y otras ramas del ordenamiento jurídico. Además dependiendo de la organización donde se integra el CO tiene que ser conocedor de las distintas regulaciones, local, nacional, internacional, en función de donde opere la empresa.

Características que delimitan el perfil:

- Formación, debido a los altos estándares, es complicado fijar un perfil único con formación y experiencia en todas las materias de cumplimiento.
- Integridad, una persona honesta que actúe bajo los principios del Código ético, ya que algunas veces tiene que eliminar del cargo a aquellas personas que hayan incurrido en delito o han realizado malas prácticas.
- Neutralidad e independencia. Tiene que ser neutral en su actividad e independiente.
- Retribución económica
- Dotes de comunicación y coordinación.

El perfil del puesto de Delegado de Protección de Datos[66]. El profesional encargado de proteger los datos de carácter personal, tendrá que tener un abanico de competencias en

[65] Alaya de la Torre, José Mª, Compliance…, pp. 28 y ss.
[66] ESQUEMA DE CERTIFICACIÓN DE DELEGADOS DE PROTECCIÓN DE DATOS (ESQUEMA AEPD-DPD),http://www.agpd.es/portalwebAGPD/temas/certificacion/common/pdf/ESQUEMA_AEPD_DPD.pdf, [Fecha de consulta: 09/04/2018]

materia de derecho y en su práctica, así como la práctica en relación con la protección de datos. Tiene que poseer las destrezas necesarias para poder llevar a cabo cada una de las funciones que se le encomiendan, artículo 39 RGPD (UE).

Además, la AEPD requiere unos prerrequisitos para poder acceder a la fase de evaluación[67] para conseguir la certificación necesaria:

- Experiencia profesional de un mínimo de cinco años en tareas relacionadas con la protección de datos
- Experiencia profesional de un mínimo de tres años y un curso de formación en materia de protección de datos de al menos 60 horas.
- Experiencia profesional de un mínimo de dos años y una formación mínima de 100 horas.
- Cursos de formación de al menos 180 horas en materia de protección de datos

Los cursos de formación tienen que seguir el programa definido por el Esquema de la AEPD. No vale solo con la presencia al curso, los aspirantes a un certificado de Delegado de Protección de Datos tendrán que superar un examen donde demostrarán los conocimientos adquiridos y las capacidades técnicas. Dicho certificado tendrá una validez de tres años. También se valoran los méritos adicionales, en caso de no poseer experiencia, como por ejemplo, formación universitaria especifica o complementaria en protección de datos o privacidad según EEES (Espacio Europeo de Educación Superior), trabajo de fin de curso en temas de protección de datos o privacidad, prácticas en empresas en temas de protección de datos o privacidad, etc.[68] Sobre la certificación hay que tener en cuenta que la AEPD ha optado que dichas certificación sean emitidas por entidades acreditadas, ENAC (Entidad Nacional de Acreditación).

Pero según la AEPD, la certificación no es la única vía y tampoco es obligatoria, pero se llegó a proceder para abrir una vía a cualquier persona que desee y tenga interés en dicho puesto.

[67] Tabla nº 1 ESQUEMA DE CERTIFICACIÓN DE DELEGADOS DE PROTECCIÓN DE DATOS (ESQUEMA AEPD-DPD).
[68] Tabla nº 2, ESQUEMA DE CERTIFICACIÓN DE DELEGADOS DE PROTECCIÓN DE DATOS (ESQUEMA AEPD-DPD)

***IV. Conclusiones*.**

PRIMERA: En la UE el nuevo Reglamento General de Protección de Datos (RGPD) refuerza la protección de datos de carácter personal y exige mayor implicación de los encargados de los tratamientos de datos. El RGPD homogeneiza la regulación de la protección de datos de carácter personal en toda la Unión Europea. El RGPD se basa en principios como los de transparencia, limitación en el plazo de conservación de datos, y en el de "accountability" o responsabilidad proactiva, esto es, prevención de riesgos, adopción de medidas correctoras y realización de evaluaciones de impacto. A pesar de los avances que esta norma supone en prevención de los ataques a la privacidad, se plantean ciertas incógnitas respecto a si las personas jurídicas públicas y privadas van a ser capaces de adaptarse a los grandes cambios operados en la regulación de la materia ante su reciente entrada en vigor, en mayo de 2018.

SEGUNDA: La figura del Data Protection Officer (DPO) es asimismo otra de las novedades introducidas por el RGPD, siendo el garante del cumplimiento de la normativa de la protección de datos de carácter personal. Esta figura es voluntaria, siendo obligatoria únicamente en determinados casos: como el de las personas jurídicas tanto privadas como públicas que lleven a cabo el tratamiento de grandes cantidades de datos de carácter personal. En este aspecto, la Administración General del Estado no ha dado señales de creación de los DPO en los respectivos Departamentos Ministeriales.

TERCERA: Otra de las novedades introducidas por el RGPD, es la ampliación de los derechos ARCO - acceso, rectificación, cancelación y oposición – se les ha añadido tres derechos más, el derecho al olvido, el de limitación en el tratamiento de los datos y el de portabilidad voluntaria de los mismos por parte del interesado.

CUARTA: Tanto el denominado Oficial de Cumplimiento (CO) normativo en las personas jurídicas privadas, como el Delegado de Protección de Datos para personas jurídicas privadas y públicas, tienen varios dominadores en común, como algunas de su funciones, pero lo que les distingue es la materia en que las desempeñan. Estas dos figuras cobran en el panorama normativo actual una especial importancia para la AEPD por su relevante papel, respectivamente, en materia de prevención de riesgos delictivos de la persona

jurídica concreta y correcto desarrollo de la normativa penal que le atañe (CO), y, prevención en cuanto a la protección de datos de carácter personal (DPO).

QUINTA: La norma UNE-ISO 19601:2007, se presenta como una norma idónea, por su carácter preventivo respecto al Compliance. La norma considera y complementa los requisitos de la Ley Orgánica 1/2015 de Reforma del Código Penal en lo referente a la responsabilidad penal de las personas jurídicas. La norma UNE establece medidas de vigilancia y control para la reducción de los riesgos penales, implementa una cultura de cumplimiento penal en la organización y gestión de modelos de prevención para la exoneración y atenuación de la responsabilidad de las personas jurídicas. Dichas normas son garantía de calidad, y son certificables. Si bien, el hecho de que una persona jurídica se encuentre certificada por una empresa como AENOR en el cumplimiento de esta norma UNE, ello no vincula el resultado de una causa penal en la que se halle como investigada, pero sí que resulta un buen argumento para la defensa.

SEXTA: Tanto en los cometidos y funciones del Oficial de Cumplimiento penal en la empresa como en los del Delegado de Protección de Datos, que no son sino de prevención delictiva, el criminólogo, como experto en el análisis de las distintas variables del crimen, lleva ya aprendidas unas destrezas fundamentales. Con una ulterior especialización en esta materia, el egresado en Criminología y Seguridad se considera que podría ser apto para ejercer cualquiera de los dos cargos.

V. Bibliografía

AGPD, “Qué es un Delegado de Protección de Datos” 24/04/2017, https://www.agpd.es. [Fecha de consulta: 06/03/2018]

AGPD, Canal del responsable de ficheros, Glosario de términos, https://www.agpd.es/portalwebAGPD/canalresponsable/inscripcion_ficheros/preguntas_frecuentes/glosario/index-ides-idphp.php [Fecha de consulta: 15/04/2018]

ALAYA DE LA TORRE, José Mª, *Compliance*, Claves Prácticas Francis Lefebvre, 2ª Ed. 2018

ARTICLE 29 DATA PROTECTION WORKING PARTY 16/E WP243, Guidelines on Data Protection Officers (“DPOs”) Adopted on 13 December 2016 http://ec.europa.eu/justice/data-protection/index_en.htm [Fecha de consulta: 09/04/2018]

BOE Ley Orgánica 5/2010, de 22 de junio, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal

Boletín Oficial de las Cortes Generales, Congreso de los Diputados XII legislatura serie A: Proyectos de ley 24 de noviembre de 2017 núm. 13-1; www.congreso.es/portal/page/portal/Congreso/PopUpCGI?CMD=VERLST&BASE=pu12&DOCS=1-1&DOCORDER=LIFO&QUERY=%28BOCG-12-A-13-1.CODI.%29#(Página1) [Fecha de consulta: 03/04/2018]

CARAU CRIADO, R. *Compliance pana pymes*, Tirant lo Blanch, Valencia, 2016

CASTELLS, Manuel. *La galaxia Internet*, Barcelona: Areté, 2001

Ciberseguridad, Ciberseguridad páctica. La notificación de violaciones de seguridad, Diario LA LEY LEGAL MANAGEMENT, nº7, junio 2017, Nº7, 23 de jun de 2017, Ed Wolters Kluwer [Fecha de consulta 28/04/2018]

Circular FGE 1/2016, sobre la Responsabilidad Penal de las Personas Jurídicas conforme a la Reforma del Código Penal efectuada por la Ley Orgánica 1/2015.

Diario LA LEY LEGAL MANAGEMENT, nº2, enero 2017, Nº2, 20 de ene. de 2017, Editorial Wolters Kluwer [Fecha de consulta 20/03/2018]

DÍAZ DÍAZ, Efrén, *El nuevo Reglamento General de Protección de Datos de la Unión Europea y sus consecuencias jurídicas para las instituciones*. Aranzadi, 2016.

EL DELEGADO DE PROTECCIÓN DE DATOS EN LAS ADMINISTRACIONES PUBLICAS, Agencia Española de Protección de Datos, Madrid 19 de mayo de 2017https://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/Funciones_DPD_en_AAPP.pdf [Fecha de consulta: 30/04/2018]

EL DPO es estratégico para las empresas" Protección de datos, IURIS&LEX, 12/Mayo/2017 http://www.apep.es/wp-content/uploads/2016/02/El-Economista-Iuris-12-5-17.pdf [Fecha consulta: 09/04/2018]

ESPAÑA MARTÍ, Mar, Memoria_AEPD, http://www.agpd.es/portalwebAGPD/LaAgencia/informacion_institucional/common/memorias/2016/Memoria_AEPD_2016.pdf [Fecha de consulta: 30/04/2018]

Especial eficacia y certificación de los programas de Compliance penal, redacción Wolters Kluwer
http://www.smarteca.es/myreader/SMT2017011_00000000_0?fileName=content%2FEX0000120949_20170518.HTML&location=pi-31 [Fecha de consulta 16/04/2018]

ESQUEMA DE CERTIFICACIÓN DE DELEGADOS DE PROTECCIÓN DE DATOS (ESQUEMA AEPD-DPD), http://www.agpd.es

Estudios sobre la Cibercriminalidad en España, 2016; Ministerio del Interior http://www.interior.gob.es/documents/10180/5791067/Estudio+Cibercriminalidad+2016.pdf/456576b2-9ce8-4f3c-bbcc-ca0dbf3bb3cf [Fecha de consulta: 30/04/2018]

GONZÁLEZ CUSSAC José L. *Comentarios a la reforma del Código Penal de 2015*. Actualizada con la corrección de errores (BOE 11 de junio de 2015). 2ª Ed. 2015.

GUTIÉRREZ PÉREZ, E., *La figura del Compliance Officer. Algunas notas sobre su responsabilidad penal,* Diario La Ley 8653, Secc. Tribuna.2015. [Fecha de consulta: 19/04/18]

LÓPEZ ÁLVARES, Luis Felipe, *Claves prácticas, Protección de datos personales: adaptaciones necesarias al nuevo Reglamento europeo*, Francis Lefebvre, 2016

LÓPEZ CALVO, José, *Comentarios al Reglamento Europeo de Protección de datos*. Las Rozas (Madrid), Sepin, 2017

LORENTE LÓPEZ, Mª Cristina, *Los derechos al honor, a la intimidad personal y familiar y a la propia imagen del menor*. Aranzadi, Navarra, 2015.

Memoria de la Fiscalía General del Estado de 2017 < https://www.fiscal.es/memorias/memoria2017/FISCALIA_SITE/index.html > [consulta: 25 de febrero de 2018].

NOAIN SÁNCHEZ, Amaya*, La protección de la intimidad y vida privada en internet: la integridad contextual y los flujos de información en las redes sociales (2004-2014)*, XIX Edición del Premio Protección de Datos Personales de Investigación de la Agencia Española de Protección de Datos. Agencia Estatal Boletín Oficial del Estado Madrid, 2016

Norma Española UNE 19601, mayo de 2017, *Sistema de gestión de Compliance penal*, Requisitos con orientación para su uso. [Fecha de consulta 16/04/2018]

ORTEGA GIMÉNEZ, A. *El nuevo régimen jurídico de la Unión Europea para las empresas en materia de Protección de datos de carácter personal*, Aranzadi, 2017.

Posición de CEDPO sobre el Delegado de Protección de Datos (DPO) en el Reglamento General de Protección de Datos (RGPD) 15 de febrero de 2017 http://www.apep.es/wp-content/uploads/2017/02/Posici%C3%B3n-de-CEDPO-sobre-el-DPO.pdf[Fecha consulta: 10/04/18]

Puyol Javier, El modelo de evaluación de riesgos en la protección de datos EIPD/PIA's, enero de 2018, www.tirantonline.com [Fecha de consulta: 22/04/18]

RALLO LOMBARTE, A Y GARCÍA MAHAMUT, ROSARIO: *Hacia un nuevo derecho europeo de protección de datos,* Tirant lo Blanch, Valencia, 2015.

REBOLLO DELGADO, L Y SERRANO PÉREZ, Mª: *Manual de protección de Datos,*2ª Ed., Dikynson. Madrid 2017.

RECIO GAYO, Miguel, *Directrices del GT29 sobre el delegado de protección de datos: figura clave para la responsabilidad (<<accountability>>).* Wolters Kluwer, 2017.

RODRÍGUEZ BALLANO, Susana y VIDAL, María, *Habemus nuevo Reglamento General de Protección de Datos*. Aranzadi, 2016.

SERRANO CHAMORRO, Mª Eugenia, *Persona y derechos A Fondo, Protección de datos personales: información, consentimiento y trasparencia. Nuevas exigencias jurídicas comunitarias*; Actualidad Civil nº5, 1 de may. de 2017, Ed Wolters Kluwer

TORRAS COLL, José Mª, *Jurisprudencia aplicada a la práctica*, LA LEY Penal nº 130, enero-febrero 2018, Nº 130, 1 de ene. de 2018, Ed. Wolters Kluwer [Fecha de consulta:19/04/2018]

VELASCO PERDIGONES, Juan C, *Nociones sobre cuestiones civiles y penales controvertidas en la responsabilidad penal de las personas jurídicas: el Compliance Officer, transparencia y prevención de la corrupción en las empresas y secreto profesional del abogado y blanqueo de capitales."* Revista Aranzadi Doctrinal num. 3/2018 parte Estudios, Ed. Aranzadi, S.A.U., Cizur Menor. 2018 [Fecha de consulta: 19/04/18]

ZALDÍVAR ROBLES, Javier La protección penal del derecho a la intimidad (19/2016) Fecha de publicación, 06/2016 www.tirantonline.com [Fecha de consulta: 23/04/2018]