



# **INFORME DPO 2024**

***LLUCH & JUELICH***  
***CORREDURIA DE***  
***SEGUROS SL***



# INDICE

1. Introducción y contexto actual
  - 1.1 Marco Normativo
  - 1.2 Funciones del DPO
  - 1.3 Responsabilidades
2. Nombramiento DPO
3. Valoración
4. Análisis
5. Conclusiones



## 1. INTRODUCCION Y CONTEXTO ACTUAL

### 1.1. Marco Normativo

El Parlamento Europeo, en su sesión plenaria de 14 de abril de 2016, aprobó el Reglamento General de Protección de **Datos (UE) 2016/679 (RGPD)**. El objetivo del nuevo Reglamento que entró en vigor el 25 de mayo del 2018 consiste en dar mayor control a las personas físicas sobre sus datos personales en un entorno de comunicaciones avanzadas tecnológicamente. Una de las principales novedades que nos trae este nuevo reglamento es el nombramiento o la designación del **delegado de protección de datos**. (también llamado **DPO o DPD**).

Esta figura constituye uno de los elementos claves del RGPD y un garante del cumplimiento de la normativa de protección de datos en las organizaciones, si bien la **responsabilidad** sobre este cumplimiento **recae en el responsable o encargado del tratamiento**.

### 1.2. Funciones del DPO

Las funciones del DPO se encuentran reguladas en el artículo 39 del RGPD, siendo las siguientes:

- Informar y asesorar** al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento, de las obligaciones del RGPD y demás normativa aplicable en protección de datos.
- Supervisar** el cumplimiento del RGPD y demás normativa aplicable en protección de datos, y de las políticas del responsable o encargado del tratamiento en dicha materia, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en operaciones de tratamiento, y las auditorías correspondientes.
- Ofrecer el asesoramiento** que se solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación conforme al artículo 35 del RGPD.
- Cooperar con la autoridad de control**. Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa del artículo 36 del RGPD, y realizar consultas, en su caso, sobre cualquier otro asunto.

### 1.3. Responsabilidades

El artículo 38 del RGPD establece que el responsable y el encargado del tratamiento garantizarán que el delegado de protección de datos (DPD) "participe de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales".



Asimismo, es importante que el DPD sea considerado como un interlocutor dentro de la organización y que forme parte de los correspondientes grupos de trabajo que se ocupan de las actividades de tratamiento de datos dentro de la organización.

En el ejercicio de sus funciones el delegado de protección de datos tendrá acceso a los datos personales y procesos de tratamiento, no pudiendo oponer a este acceso el responsable o el encargado del tratamiento la existencia de cualquier deber de confidencialidad o secreto.

En cuanto a la responsabilidad del Delegado de Protección de Datos, el RGPD deja claro que es el responsable o el encargado del tratamiento quien está obligado a garantizar y ser capaz de demostrar que el tratamiento se realiza conforme a las disposiciones del Reglamento. La función del DPO de supervisar la observancia no significa que el DPO sea personalmente responsable de cualquier caso de inobservancia. El cumplimiento de las normas en materia de protección de datos es responsabilidad corporativa del responsable del tratamiento, no del DPD.

## **2. NOMBRAMIENTO DPO**

La entidad Lluich & Juelich Correduría de Seguros SL con CIF B57041659 con domicilio en Carrer General Riera nº 58 07010 Palma de Mallorca y representada por Carlos Lluich Cerdá, tiene designado como Delegado de Protección de Datos a APM Asesores Privados 2002 SL (en adelante Exponent Consultores) con CIF B97190599 don domicilio en Calle Industria nº 22 bajo izquierda 46022 de Valencia y representada por Carlos Albo Portero.

Dicho nombramiento fue efectuado ante la agencia española de protección de datos el día 05/10/2020.

## **3. VALORACION**

APM Asesores Privados 2002 SL en colaboración con Lluich & Juelich Correduría de Seguros SL han verificado el correcto uso de los procedimientos implantados en esta última con el fin de detectar posibles rectificaciones y mejoras tras su implantación en dicha correduría de seguros.

Tras esa verificación se desprenden las siguientes consideraciones:

1. Se sigue facilitando la información en materia de protección de datos a todos los clientes a través de un documento de confidencialidad para firmar antes de la emisión de un presupuesto o póliza de seguro.



2. Lluich & Juelich Correduría de Seguros SL sigue teniendo una base jurídica sobre la que se sustentan los tratamientos realizados sobre los datos personales recabados y que está basada en el Real Decreto-Ley 3/2020, de 4 de febrero, de medidas urgentes por el que se incorporan al ordenamiento jurídico español diversas directivas de la Unión Europea en el ámbito de la contratación pública en determinados sectores, de seguros privados, de planes y fondos de pensiones, del ámbito tributario y de litigios fiscales.
3. En Lluich & Juelich no se tratan datos personales inadecuados ni excesivos para la finalidad del tratamiento, así como no se utilizan para una finalidad distinta para la cual fueron recabados que no es otra que la emisión de una póliza de seguro.
4. Se almacena la documentación por periodo indefinido por decisión de la empresa, siendo éste por un período superior al necesario.
5. En cuanto a las transferencias internacionales de datos, Lluich & Juelich Correduría de Seguros SL, comunica que no realiza ninguna transferencia.
6. En el momento de la revisión de procedimientos, se nos comunica que hasta la fecha no han recibido ninguna solicitud de ejercicios de derechos ARCO, por parte de ningún cliente.
7. Lluich & Juelich Correduría de Seguros SL debe tener firmados los contratos con los encargados del tratamiento con los que se trata, dichos contratos fueron incluidos en la revisión de procedimientos de protección de datos de 2021.
8. Lluich & Juelich Correduría de Seguros SL dispone de un Registro de actividades del tratamiento según marca la ley 3/2018 de protección de datos de carácter personal y garantía de los derechos digitales basado en la información que facilita a Exponent Consultores, donde se recogen las actividades de tratamiento efectuadas bajo su responsabilidad.
9. Se dispone de una estructura organizativa, procesos y recursos para una adecuada gestión de la seguridad en Lluich & Juelich Correduría de Seguros SL puesto que en todos equipos informáticos de la correduría de seguros disponen de contraseñas para acceder tanto al sistema operativo como al programa de gestión. Asimismo se tienen instalados en cada uno de dichos equipos informáticos distintos antivirus, Windows



Defender, Firewall y un programa de escaneo diario para evitar la entrada de software malicioso que pueda suponer una pérdida de información de datos personales.

10. Hasta la fecha no se han producido fallos de seguridad en desarrollos de una nueva aplicación o de nuevas funcionalidades y/o parches de una aplicación ya existente.
- 11.No han tenido la entrada de ningún Software malicioso en ningún equipo de la correduría de seguros, para estos casos Lluich & Juelich Correduría de Seguros SL debe tener un procedimiento de información y comunicación de dichas entradas de software malicioso.
- 12.No se ha producido ninguna fuga de información.
- 13.No se han producido violaciones de confidencialidad de los datos personales por parte del personal propio ni de personal externo a la correduría de seguros.
- 14.No se ha realizado ninguna manipulación ni modificación no autorizada de información.
- 15.En Lluich & Juelich Correduría de Seguros SL se realizan copias de seguridad diarias y automáticas del programa Soft QS en la nube y de la información para evitar que se pierda información en caso de errores técnicos o fallos que ocasionen una indisponibilidad de los sistemas de información.
- 16.En Lluich & Juelich Correduría de Seguros SL dispone de la suficiente capacidad para asegurar la disponibilidad de la información puesto que como se ha comentado en el punto anterior se realizan copias de seguridad de la información.
- 17.No se ha producido ningún robo o extravío de equipos, soportes o dispositivos con datos personales de la Correduría de seguros.
- 18.No se han producido daños en las infraestructuras de la correduría de seguros producidas por catástrofes naturales.
- 19.No se detectan deficiencias en los protocolos de almacenamiento de los datos personales en formato físico puesto que no se conserva mucha documentación en formato papel puesto que en su gran mayoría se conserva informatizada.



20. Las medidas de control de acceso físico a las instalaciones de Lluich & Juelich son suficientes para garantizar la seguridad física, ambiental y de los equipos informáticos.

#### 4. ANALISIS DE LLUCH & JUELICH CORREDURIA DE SEGUROS SL

Finalidades del tratamiento	DETALLE	SI / NO
<b>¿La recogida de los datos tiene como finalidad el tratamiento a gran escala (3)? Por favor, detalle los puntos indicados a continuación para poder analizar si se trata de un tratamiento a gran escala:</b>		
El número de sujetos afectados (es decir, cuantos interesados van a ser objeto de este tratamiento)	De 0 a 10.000	SI
	De 10.000 a 100.000	
	+ de 100.000	
Las categorías de datos tratados. (Datos especialmente protegidos, Datos de carácter identificativo, Características personales, Circunstancias sociales, Datos académicos y profesionales, Detalles del empleo, Información comercial, Datos económicos, financieros y de seguro, Transacciones de bienes y servicios). Indicar cuántas de estas categorías aplicarían.	1 2 3 4 5 6 7 8 9	1,2,3,4 5,6,7,8,9
La duración del tratamiento (instantáneo (I), días (D), semanas (S), meses (M),...)	Instantáneos días	
	Semanas meses	SI
La extensión geográfica del tratamiento (Tratamiento a nivel regional (R), nacional (N) o internacional (I))	Regional nacional	SI
	internacional	SI
<b>¿La recogida de los datos tiene como finalidad la monitorización o evaluación sistemática y exhaustiva de aspectos personales?</b> (tratamiento para monitorizar, observar y/o controlar a los interesados, a través del cual, se pueden determinar hábitos, comportamientos, preferencias, gustos, intereses, etc. de personas identificadas o identificables?)		NO
<b>¿La recogida de los datos tiene como finalidad el tratamiento de datos especialmente protegidos (4)?</b>		
(4) Datos identificativos de personas identificadas o identificables asociadas a: Ideología o opiniones políticas Afilación sindical Religión o opiniones religiosas Creencias o creencias filosóficas Origen étnico o racial Datos relativos a salud Vida sexual u orientación sexual Datos de violencia de género y malos tratos Datos biométricos Datos genéticos que proporcionan una información única sobre la fisiología o la salud del identificado obtenidas del análisis de una muestra biológica Datos solicitados para fines policiales sin consentimiento de las personas afectadas Datos relativos a condenas y delitos penales"		SI
<b>¿El tratamiento involucra contacto con los interesados de manera que, dicho contacto, pueda resultar intrusivo (5) o se prevé el uso de tecnologías que se pueden percibir como especialmente intrusivas en la privacidad (6)?</b>		NO



<i>¿La finalidad del tratamiento implica el uso específico de datos de personas con discapacidad o cualquier otro colectivo en situación de especial vulnerabilidad (p.e.: menores de 14 años, ancianos, personas con riesgo de exclusión social, empleados, ...)?</i>		NO
<i>¿Se van a tratar datos personales para elaborar perfiles, categorizar/segmentar, hacer ratings/scoring o para la toma de decisiones(7)?</i>		SI
(7) A modo de ejemplo, la segmentación de clientes en base a sus datos personales con el objetivo de realizar comunicaciones comerciales		
<i>¿El tratamiento de los datos implica una toma de decisiones automatizada sin que haya ninguna persona que intervenga en la decisión o valore los resultados (8)?</i>		NO
(8) A modo de ejemplo, autorizar o denegar un tipo de producto a un cliente mediante un algoritmo automatizado sin que ningún gestor valore el resultado para confirmar las decisiones		
<i>¿Se enriquece la información de los interesados mediante la recogida de nuevas categorías de datos o se usen las existentes con nuevas finalidades que antes no se contemplaban, en particular, si estas finalidades son más intrusivas o inesperadas para los afectados (9), o incluso pueda llegar a bloquear el disfrute de algún servicio?</i>		NO
(9) A modo de ejemplo, el uso de la información contenida en ficheros externos como ASNEF o CIRBE		
<i>¿El tratamiento implica que un elevado número de personas (más allá de las necesarias para llevar a cabo el mismo) tenga acceso a los datos personales tratados? Por ejemplo, un departamento que no participe en el tratamiento.</i>		NO
<i>¿Se van a tratar datos relativos a la observación de zonas de acceso público? (por favor, tenga en cuenta que las zonas de acceso público únicamente estarán situadas en la vía pública, excluyendo los lugares de trabajo (p.e.: oficinas comerciales)</i>		NO
<i>Para llevar a cabo este tratamiento, ¿se combinan conjuntos de datos utilizados por otros responsables de tratamiento cuya finalidad diste en exceso de las expectativas del interesado (10)?</i>		NO
(10) A modo de ejemplo, utilizar el resultado de un tratamiento de análisis de datos de un cliente para realizarle ofertas comerciales en base a dichos resultados		
<i>¿Se utilizan datos de carácter personal no disociados o no anonimizados de forma irreversible con fines estadísticos, históricos o de investigación científica??</i>		NO
<b>Tecnologías empleadas para el tratamiento</b>	<b>DETALLE</b>	<b>SI / NO</b>
<i>¿Se prevé el uso de tecnologías que se pueden percibir como inmaduras, de reciente creación o salida al mercado, cuyo alcance no puede ser previsto por el interesado de forma clara o razonable e implique elevado riesgo para el acceso no autorizado (11)?</i>		NO
(11) A modo de ejemplo, la combinación de tecnologías ya existentes, como el uso de dispositivos inteligentes de nueva creación y reconocimiento facial para aumentar la seguridad del acceso físico a las instalaciones, se considera una tecnología inmadura		
<b>Cesiones de datos y transferencias internacionales de datos</b>	<b>DETALLE</b>	<b>SI / NO</b>
<i>¿Se realizan cesiones de datos a otras entidades, ya sean del mismo grupo o proveedores externos al mismo?</i>		SI
<i>¿Se realizan transferencias internacionales de datos a países fuera de la Unión Europea y que no cuenten con medidas de protección de datos de carácter personal similares a las establecidas por la Autoridad de Control (12)? (en caso afirmativo detallar cuáles)</i>		NO
(12) A modo de referencia, el siguiente listado contiene los países considerados seguros para las transferencias de datos: Andorra Argentina, Canadá (Sector privado) Suiza, Islas Feroe Guernsey Israel, Isla de Man, Jersey, Nueva Zelanda Uruguay		



Percepción de la existencia un riesgo elevado por parte del responsable de la actividad del tratamiento	JUSTIFICACION	SI / NO
<i>¿Es este tratamiento similar a otro para el que haya sido necesario realizar un EIPD (13)?</i>		NO
(13) En caso afirmativo, se pueden utilizar las conclusiones del EIPD ya realizado para dicho tratamiento		
<i>¿Este tratamiento puede conllevar una pérdida o alteración de la información?</i>		NO
<i>¿Se utilizada documentación en papel para tratar datos personales?, en tal caso, indicar las medidas aplicadas:</i>		SI
Se guarda bajo llave Se destruye de forma confidencial Se guarda con un registro de accesos Otros		
Terceros que intervengan en el tratamiento	JUSTIFICACION	SI/ NO
<i>¿Interviene algún proveedor en el proceso?</i>		SI

## 5.CONCLUSIONES

Tras la revisión de los procedimientos implantados por Lluich & Juelich Correduría de Seguros SL se concluye que la correduría de seguros tiene un resultado favorable en cuanto a la identificación del riesgo cumpliendo con las directrices que marca la normativa vigente en materia de protección de datos.

Se ruega subsanación de aquellos apartados que no están completos, comunicándolo a Exponent Consultores a la mayor brevedad posible.

De la misma manera se informa que es obligatoriedad de la empresa, realizar reuniones para verificar los procedimientos implantados para la correcta aplicación de los mismos en el día a día, así como la notificación de cualquier brecha de seguridad.