Nombre de la política: Política de protección de datos, RGPD
Autor: Radosław Bieliński
Aprobada por: Radosław Bieliński
Fecha de aprobación: 12.05.2020
Fecha de revisión del director de cumplimiento: 12.05.2020

VERSIÓN	AUTOR	DESCRIPCIÓN DEL CAMBIO	APROBADO POR
16.06.2020	Radosław Bieliński	Introducción del sistema nuevo de nombres de políticas	Radosław Bieliński

Índice

1. Introducción

La privacidad es un derecho fundamental y para nuestra organización es importante proteger dicho derecho. Por lo tanto, DYWIDAG, como grupo global, se compromete a cumplir con todas las leyes, reglas y regulaciones relacionadas con la Protección de datos por las que se rigen sus filiales, incluido, entre otros, el Reglamento general de protección de datos ("RGPD").

DYWIDAG recopila, almacena y trata datos personales relacionados con diversos Titulares de datos, como sus empleados, candidatos a puestos de trabajo, clientes, proveedores y otros terceros. El tratamiento correcto y lícito de los datos personales se mantendrá de forma segura y en consonancia con la reputación del Grupo DYWIDAG como socio comercial y empleador socialmente responsable.

Esta política establece los requisitos que deben cumplir todos aquellos que se encuentren dentro del alcance de la política y comprende los principios de privacidad de datos aceptados internacionalmente. Dichos requisitos aplican a todas las filiales de DYWIDAG, sus empleados, contratistas, empleados temporales y trabajadores de agencias, incluidas todas las personas con las que colaboramos o las actúan en nuestro nombre y pueden necesitar acceso ocasional a datos. La política abarca todas las actividades del tratamiento que involucran datos personales y lo ayudará a reconocer lo que pueden ser datos personales, así como sus derechos y obligaciones con respecto a dichos datos.

La Política de protección de datos de DYWIDAG complementa las leyes nacionales de privacidad de datos o aplica cuando no haya una legislación nacional. Las filiales de DYWIDAG a las que esta política no aplica directamente debido a las reglas de gestión existentes (p. ej., empresas conjuntas) deben implementar sus propias políticas y procedimientos en función de su legislación y requisitos nacionales.

Una infracción de las leyes de privacidad de datos pertinentes puede causar un daño enorme a DYWIDAG, ya sea en términos de pérdida de reputación, multas elevadas y deterioro de la confianza de los clientes, empleados y el público, así como de todas las demás partes interesadas. Por lo tanto, confiamos en que usted cumplirá con los requisitos establecidos en esta Política.

2. Alance

El alcance de esta Política abarca lo siguiente:

- Todas las actividades de tratamiento que involucran datos personales y confidenciales en las que DYWIDAG actúa como Responsable del tratamiento de datos, incluidos los datos personales almacenados en forma física en un sistema de llenado pertinente.
- Todos los Empleados, Contratistas, Terceros, Encargados u otros que tratan datos personales o confidenciales en nombre del Grupo DYWIDAG.
- Todos los territorios geográficos, incluidos los terceros países fuera de la Unión Europea (UE). Todas las filiales de DYWIDAG y sus empleados deben tratar los datos personales con la debida diligencia y de conformidad con los requisitos legales y esta política.

En particular, para las Entidades y las actividades de tratamiento de datos que están sujetas al RGPD, las pautas y procedimientos locales adicionales son esenciales y deben desarrollarse y configurarse por la dirección local o un delegado designado para el cumplimiento de las reglas que se han aplicado desde mayo de 2018 además de la posible legislación nacional. Las filiales que operan fuera de la Unión Europea también deben desarrollar políticas y normas locales adicionales si esto es necesario para cumplir con las leyes de protección de datos y la legislación nacional. Las filiales de DYWIDAG que no tengan leyes nacionales de protección de datos deben adoptar y aplicar esta política.

Si las leyes nacionales pertinentes contradicen esta política o tienen requisitos más estrictos que los del presente, las filiales pueden derogar esta política. Es responsabilidad de la dirección local de la Entidad controlar la legislación nacional de protección de datos y su desarrollo o enmiendas. En caso de que las enmiendas de la legislación nacional contradigan esta política, se debe informar al director de cumplimiento.

3. Definiciones

- "Datos personales": cualquier información relacionada con una persona física identificada o identificable, denominado "titular de los datos".

- "Titular de los datos": una persona física identificable es aquella que puede ser identificada, directa o indirectamente, en particular por referencia a un identificador como un nombre, una dirección, un número de identificación, cualquier tipo de datos de ubicación, un identificador en línea o uno o más factores específicos de la identidad física, fisiológica, genética, mental, económica, cultural o social de dicha persona física. La información sobre el origen racial o étnico de una persona, sus opiniones políticas, creencias religiosas o similares, afiliación sindical, salud o condición física o mental, salud y vida sexual, y acusaciones o delitos penales se considera confidencial y pertenece a categorías especiales de datos personales. En virtud de la legislación nacional, otras categorías de datos pueden considerarse altamente confidenciales o el contenido de las categorías de datos se puede cumplimentar de manera diferente.
  Los datos anonimizados y los datos no relacionados con una persona física (p. ej., datos de una empresa, como nombres y direcciones de la empresa) no están sujetos a esta política.
- "Tratamiento": de datos personales hace referencia a cualquier operación o conjunto de operaciones que se realicen con datos personales o con conjuntos de datos personales, ya sea por medios automatizados o no, tales como recolección, registro, organización, estructuración, almacenamiento, adaptación o alteración, recuperación, consulta, uso, divulgación por transmisión, difusión o puesta a disposición de otro modo, alineación o combinación, restricción, eliminación o destrucción.
- Un "responsable del tratamiento de datos": es "una persona física o jurídica, autoridad pública, agencia u otro organismo que, solo o conjuntamente con otros, determina los fines y medios del tratamiento de datos personales".
- "Encargados del tratamiento de datos": tratan datos personales en nombre de un Responsable del tratamiento de datos (p. ej., agencia de liquidación de sueldos que DYWIDAG, que es el Responsable del tratamiento de datos, contrata para liquidar sueldos).
- "Violación de la seguridad": es cualquier incidente que tenga como consecuencia el acceso no autorizado a datos, aplicaciones, servicios, redes o dispositivos mediante la evasión de sus mecanismos de seguridad subyacentes.
  Una violación de la seguridad ocurre cuando un individuo o una aplicación ingresan ilegítimamente a un perímetro de TI lógico privado, confidencial o no autorizado. Una violación de la seguridad también se conoce como falla de seguridad y potencialmente termina en una violación de datos personales.
- "Filtración de datos": es una violación de seguridad que conduce a la destrucción, pérdida, alteración, divulgación no autorizada o el acceso a datos personales transmitidos, almacenados

o tratados de otro modo, en forma electrónica o impresa, accidental o ilegal, que da lugar a un posible riesgo en relación con la confidencialidad o integridad de los datos.

- "Tercero": hace referencia a una persona física o jurídica, autoridad pública, agencia u organismo que no sea el titular, responsable o encargado del tratamiento de datos, o cualquier persona que, en virtud de la autoridad directa del responsable o encargado del tratamiento de datos, esté autorizada para tratar datos personales.

4. Marco y principios de la protección de datos

Esta sección describe el marco y los principios básicos, define la normativa y los requisitos mínimos de nuestra organización de protección de datos y es una guía para garantizar, controlar y mantener un nivel adecuado de seguridad de los datos personales. Dentro de la organización DYWIDAG, la información personal se recopila de forma transparente y solo con la plena cooperación y conocimiento de las partes interesadas. Una vez recopilados los datos personales, se aplicarán los siguientes principios:

Los datos personales y todas las actividades de tratamiento:

- Se registrarán con precisión y se mantendrán actualizados.
- Se recopilarán solamente para fines específicos, explícitos y legítimos.
- Se conservarán solo durante el tiempo que sea necesario y de acuerdo con los requisitos legales del período de conservación.
- Se tratarán de modo justo y legal.
- Se protegerán de cualquier acceso no autorizado o ilegal y del uso indebido por partes internas o externas.
- Serán adecuados, relevantes y estarán limitados a aquello que sea necesario.

Los datos personales y todas las actividades de tratamiento:

- No se comunicarán internamente sin un fin.
- No se transferirán a organizaciones (y filiales), estados o países que no tengan políticas y regulaciones de protección de datos adecuadas.

Además de las formas del manejo de los datos, cada entidad del Grupo DYWIDAG tiene obligaciones directas hacia las personas a las que pertenecen los datos. En concreto, si así lo solicitaran, debemos

informar: a) cuáles de sus datos se tratan, b) cómo tratamos dichos datos y c) quién tiene acceso a la información.

También debemos:

- Tener disposiciones en casos de datos perdidos, corrompidos o comprometidos.
- Permitir que las personas soliciten que modifiquemos, borremos, reduzcamos o corrijamos los datos que mantenemos en nuestras bases de datos.

Para garantizar un nivel adecuado de protección de los datos personales, nos comprometemos a:

- Restringir y controlar el acceso a los datos personales, especialmente a los datos personales confidenciales.
- Desarrollar procedimientos transparentes de recopilación de datos.
- Capacitar a los empleados sobre las medidas de seguridad y privacidad en línea.
- Crear redes seguras para proteger los datos en línea de los ciberataques.
- Establecer procedimientos claros para informar sobre violaciones de la privacidad o el uso indebido de datos.
- Incluir cláusulas contractuales siempre que se considere necesario o realizar declaraciones sobre cómo manejamos los datos.
- Establecer las mejores prácticas de protección de datos (controles de acceso a edificios, oficinas y sistemas de TI, destrucción de documentos, bloqueos seguros, cifrado de datos y dispositivos, copias de seguridad frecuentes, autorización de acceso, planes de recuperación ante desastres, etc.).

Esos principios se describen con más detalle en las siguientes secciones de esta política.

4.1 Principios fundamentales para el tratamiento de datos personales

Cuando se tratan datos personales, aplican los siguientes principios:

- Equidad, legalidad y transparencia: los datos personales solo pueden recopilarse y tratarse para fines específicos, explícitos y legítimos de modo justo y transparente y de conformidad con la legislación vigente. Se debe informar al titular de los datos cómo se están tratando sus datos.

En general, los datos personales deben recopilarse directamente del individuo en cuestión. Cuando se recopilan los datos, el titular de los datos debe conocer o recibir información sobre: a) la identidad del responsable del tratamiento de datos, b) la finalidad del tratamiento de datos y c) los terceros o las categorías de terceros a quienes se pueden transmitir dichos datos.

- Limitación del propósito: los datos personales solo pueden recopilarse y tratarse para el propósito que se definió antes de la recopilación, limitado a lo necesario en relación con los propósitos para los que se tratan y no pueden tratarse posteriormente de una manera que sea incompatible con dichos propósitos.
- Minimización de datos: los datos personales deben restringirse en la medida adecuada, necesaria y relevante para lograr el propósito de su tratamiento. Los datos personales no deben recopilarse con anticipación y almacenarse para posibles propósitos futuros, a menos que el titular de los datos haya dado su consentimiento, lo requiera o que la ley nacional lo permita.
- Precisión: los datos personales archivados deben ser correctos, estar completos y, de ser necesario, mantenerse actualizados. Se deben tomar las medidas adecuadas para garantizar que los datos inexactos o incompletos se eliminen, corrijan, complementen o actualicen.
- Limitación de almacenamiento y eliminación: los datos personales deben mantenerse solo mientras sea necesario para lograr los propósitos previstos de recopilación y tratamiento. Después de que caduquen los períodos relacionados con los procesos comerciales legales, los datos personales que ya no se necesitan deben eliminarse de forma segura.
- Integridad y confidencialidad, y seguridad de los datos: los datos personales deben tratarse de manera que: a) se garantice la seguridad adecuada de los datos, y b) los datos se almacenen de forma segura utilizando sistemas y software adecuados y modernos que se mantengan actualizados.

Nuestras Entidades deben establecer y describir formalmente medidas de seguridad organizativas y técnicas adecuadas (TOM, p. ej., controles de acceso, reglas de contraseñas, seguridad física de los servidores, pautas de respaldo, etc.) para evitar el uso indebido, el acceso, el tratamiento o la distribución no autorizados o ilegales, así como la pérdida accidental, la modificación o la destrucción de los datos.

El cumplimiento de dichos principios debe estar respaldado por un registro de los sistemas (TI) y las actividades de tratamiento donde se documente toda la información y los procedimientos relacionados con los datos personales (p. ej., categoría del titular de los datos, categoría de datos personales, propósito del tratamiento). Todas las Entidades deben conservar dicho Registro de actividades de

tratamiento, especialmente las Entidades con actividades de tratamiento sujetas al RGPD (Art. 30, RGPD).

4.2 Legalidad del tratamiento

DYWIDAG debe garantizar que el tratamiento sea legal y documentar los fundamentos legales del tratamiento. Para que los datos personales se traten legalmente, deben tratarse en función de uno de los siguientes fundamentos legales:

- El consentimiento del titular de los datos para el tratamiento (p. ej., de los solicitantes de empleo que envían currículums, boletín de marketing).
- El tratamiento es necesario para celebrar o cumplir un contrato con el titular de los datos (p. ej., contrato laboral).
- Para el cumplimiento de una obligación legal a la que DYWIDAG y sus filiales (los responsables del tratamiento de datos) están sujetos (p. ej., declaraciones de impuestos y seguridad social).
- Por el interés legítimo de DYWIDAG o de la parte a la que se revelan los datos personales (p. ej., los archivos de registro del usuario o las direcciones IP pueden almacenarse temporalmente, y esto se justifica para garantizar el funcionamiento y la seguridad adecuados de la red).
- Por el interés vital del público y otras partes interesadas.
- Para tareas y obligaciones públicas.

El tratamiento de categorías especiales de datos personales debe estar expresamente permitido o prescrito en virtud de la legislación nacional. Además, se puede permitir el tratamiento, de ser necesario, para que la autoridad responsable cumpla con sus derechos y deberes en materia de derecho laboral. El empleado también puede dar su consentimiento expreso para el tratamiento.

A excepción del almacenamiento, el tratamiento cesará inmediatamente cuando ya no existan fundamentos legales.

4.3 Derechos de los titulares de los datos

Cuando los titulares de los datos lo soliciten, la Entidad en cuestión debe informarles sobre sus datos personales recopilados dentro del alcance de la legislación vigente. En general, los titulares de los datos tiene derecho a:

- Solicitar acceso a cualquier dato personal que un responsable del tratamiento de datos conserve sobre ellos.
- Prevenir, objetar o restringir el tratamiento de sus datos personales, p. ej. para fines de marketing directo.
- Solicitar que se enmienden datos personales inexactos.
- Solicitar información sobre la identidad del destinatario o las categorías de destinatarios si sus datos personales se han transmitido a terceros (p. ej., encargados del tratamiento de datos subcontratados).
- Solicitar la eliminación de sus datos si el tratamiento de dichos datos no tiene un fundamento legal o si dicho fundamento legal ya no aplica. Lo mismo aplica si el propósito que respaldaba el tratamiento de datos ha caducado o ha dejado de aplicar por otros motivos. Los períodos de retención legal pueden anular este derecho y deben controlarse cuidadosamente.

Si recibió alguna solicitud de acceso por parte de un titular de los datos, comuníquese con el director de cumplimiento de inmediato. Dicha solicitud se completará lo antes posible, pero no más de 30 días calendario, y se comunicará al titular de los datos de forma segura.

4.4 Transferencias de datos personales y tratamiento de datos (contractuales) en representación

La transmisión de datos personales dentro del grupo o el "Tratamiento en representación" de un responsable del tratamiento de datos debe basarse en los principios establecidos en las secciones 4.1 a 4.3 y cumplir con la legislación vigente y los requisitos legales de la protección de datos del país correspondiente.

El "Tratamiento en representación" significa que un Encargado del tratamiento de datos está llevando a cabo el tratamiento de datos personales en representación de un responsable del tratamiento de datos

y de acuerdo con las instrucciones de este, quien determina los propósitos y medios para el tratamiento de los datos personales. En otras palabras, el responsable del tratamiento de datos contrata a un Encargado del tratamiento de datos para tratar datos personales (p. ej., subcontratación de la administración de liquidación de sueldos, subcontratación de los servidores de TI a un proveedor de alojamiento/nube).

Las actividades del "Tratamiento en representación" dentro de la UE no se subcontratarán sin un contrato escrito vinculante que establezca el objeto y la duración del tratamiento, la naturaleza y el propósito del tratamiento, el tipo de datos personales y las categorías de los titulares de los datos, y las obligaciones y derechos de la Entidad de DYWIDAG que obra como Responsable del tratamiento de datos (Artículo 28, RGPD UE). En el caso de que los datos personales se transmitan desde una Entidad de DYWIDAG (responsable del tratamiento de datos) dentro de la UE a un destinatario (encargado del tratamiento de datos) fuera de la UE (incluidas las transferencias dentro del grupo), dicho destinatario debe aceptar mantener un nivel de protección de datos equivalente al que establece esta Política de protección de datos.

El responsable del tratamiento de datos debe utilizar solo encargados del tratamiento de datos que brinden garantías suficientes para implementar las medidas técnicas y organizativas apropiadas de manera tal que el tratamiento cumpla con los requisitos de esta política y garantice la protección de los derechos del titular de los datos.

4.5 Confidencialidad del tratamiento

Cualquier tipo de datos personales está sujeto a la privacidad de datos, por tanto:

- Se prohíbe cualquier recopilación y tratamiento no autorizados de dichos datos por parte de los empleados.
- Se prohíbe cualquier tratamiento de datos por parte de un empleado que no esté autorizado a realizarlo como parte de sus deberes legítimos.

Aplica el principio de "necesidad de saber": los empleados pueden tener acceso a la información personal solo si es apropiada para el tipo y alcance de la tarea en cuestión. Esto requiere un desglose y una división cuidadosos, así como la implementación de roles y responsabilidades.

Se prohíbe el uso por parte de los empleados de nuestros datos personales recopilados para fines privados o comerciales o su divulgación a personas no autorizadas; los empleadores deben informar a sus empleados al inicio de la relación laboral sobre la obligación de proteger la privacidad de los datos y darles a conocer esta política (p. ej., solicitando una confirmación por escrito de esta política). Esta obligación permanecerá vigente incluso después de la finalización de la relación laboral.

4.6 Seguridad del tratamiento

Los datos personales deben protegerse del acceso no autorizado y del tratamiento o divulgación ilegal, así como de la pérdida, modificación o destrucción accidentales. Esto aplica independientemente de si los datos se tratan electrónicamente o en papel. Dichas medidas de seguridad técnicas y organizativas deben basarse en las tecnologías más modernas y de última generación, los riesgos de tratamiento y la confidencialidad de los datos a proteger. En general, cada DYWIDAG y todas las filiales deben asegurarse de que:

- Los edificios y las oficinas estén adecuadamente protegidos contra el acceso no autorizado (p. ej., sistemas de alarma, controles de entrada y registro).
- Los datos personales se almacenen de forma segura mediante un software moderno que se mantenga actualizado.
- El acceso a los datos personales se limite solo al personal que necesite acceso y que se hayan implementado las medidas de seguridad adecuadas para evitar el intercambio no autorizado de información.
- Los datos del personal se transfieran solo por medios seguros (p. ej., correo electrónico/computadora portátil cifrados, memorias USB cifradas).
- El acceso a los datos personales esté supervisado y controlado (p. ej., registros de auditorías para entradas de datos).
- Haya disponibilidad y recuperación de datos (procedimientos de respaldo y recuperación ante desastres, firewalls, programas antivirus).
- Cuando se eliminen datos personales, esto se haga de forma segura de manera que la eliminación sea irrecuperable.

- Existen controles adecuados cuando los datos personales se subcontratan a un encargado del tratamiento de datos externo.
- Los incidentes de seguridad, las filtraciones de datos y cualquier otro incidente se notifiquen y gestionen adecuadamente.

Deben definirse e implementarse medidas técnicas y organizativas antes de la introducción de métodos nuevos de tratamiento de datos personales, especialmente antes de introducir sistemas y aplicaciones de TI nuevos. Deben evaluarse y analizarse continuamente con respecto a los avances técnicos y los cambios organizativos.

4.7 Concientización sobre la protección de datos

La eficacia de la organización de la protección de datos de DYWIDAG requiere que todos las filiales y todos sus empleados que tratan datos personales para DYWIDAG sean conscientes de la importancia de la protección de datos y la privacidad de los datos.

Por lo tanto, la dirección de cada Entidad de DYWIDAG tiene el deber de fomentar esta concientización entre todos los empleados que tratan datos personales, por ejemplo, mediante capacitaciones periódicas, por lo menos anuales, en materia de protección de datos, programas de concientización y sensibilización corporativa a través de capacitaciones en línea u otros métodos adecuados (p. ej., capacitaciones in situ).

4.8 Estructura organizacional

La dirección ejecutiva de todas las Entidades de DYWIDAG es responsable de garantizar un nivel adecuado de protección de los datos que cumpla con toda legislación vigente en todas sus filiales y que permita la implementación de una organización de protección de datos adecuada.

Para garantizar un nivel adecuado de protección de datos y la ejecución de esta política, se requiere la implementación de los siguientes roles y funciones:

- Coordinadores de la protección de datos ("CPD"). La dirección local de cada Entidad debe designarlos. Los coordinadores de la protección de datos son los puntos de contacto in situ para la protección de datos. Pueden realizar verificaciones y deben informar a los empleados sobre el contenido de esta política de protección de datos.
- Delegados de protección de datos ("DPD"), cuando así lo requiera la ley aplicable.

Requisitos legales nacionales pueden definir roles y tareas adicionales. La dirección regional y/o local de una Entidad asegura que los CPD y DPD:

- Están suficientemente involucrados y a su debido tiempo en todos los asuntos relacionados con la protección de datos personales.
- Tienen acceso a todos los procesos relacionados con el tratamiento de datos personales.
- Pueden rendirle cuentas directamente al director de cumplimiento.
- Tienen la obligación de mantener la privacidad y no divulgar sus actividades de conformidad con la legislación vigente.

Los CPD y DPD pueden realizar otras tareas, deberes y funciones si estos no constituyen un conflicto de intereses con respecto a sus actividades como CPD o DPD. Varias Entidades de una región o un país pueden nombrar a los CPD y DPD si dicho nombramiento no constituye un conflicto de intereses.

4.9 Incidentes sobre la protección de datos

La dirección regional o local de una Entidad debe informar de inmediato a sus CPD o DPD locales a cargo, así como al director de cumplimiento y al Departamento legal los siguientes incidentes relevantes para la protección de datos:

- Cualquier violación de datos informada, anticipada o potencial (p. ej., correo electrónico enviado a los destinatarios incorrectos, información personal revelada a personas no autorizadas, una violación de seguridad generalmente conlleva una violación de datos).

- Quejas, reclamos y acusaciones en relación con la protección de datos por parte de los titulares de los datos (p. ej., empleados, clientes, proveedores).
- Solicitudes en relación con la protección de datos por parte de cualquier titular de datos (p. ej., cliente que consulta sobre las actividades de tratamiento de sus datos personales).
- Violaciones o posibles violaciones de las leyes de protección de datos, así como la violación de esta Política de protección de datos.
- Multas impuestas por las autoridades de protección de datos.
- Auditorías recomendadas por las autoridades de protección de datos.
- Cualquier violación o incidente de seguridad relacionado con los sistemas de TI (p. ej., sistemas comprometidos, fallas del sistema, intentos de piratería, intrusión de sistemas, intentos de acceso no autorizados) que puedan resultar en una violación de datos.

La pérdida o robo de dispositivos móviles (computadoras portátiles, teléfonos móviles, tabletas, memorias USB) puede dar lugar a una posible violación de datos y, por lo tanto, también debe informarse al CPD o DPD local, al director de cumplimiento y al director global de TI.

Además de ello, la dirección local debe:

- Mantener un registro de todos los incidentes y eventos mencionados anteriormente.
- Mantener todos los documentos, comunicaciones y medidas tomadas relevantes relacionadas con esos incidentes y solicitudes en un archivo separado y tenerlo disponible en caso de que sea solicitado.

Todos los CPD y DPD designados, así como cualquier cambio posterior, deben informarse con todos sus datos de contacto al director de cumplimiento y/o al departamento legal del Grupo.

5. Responsabilidades y deberes: auditoría

El personal de la dirección local y del grupo es responsable de garantizar que se implementen todas las medidas organizativas, técnicas y de recursos humanos relevantes para que cualquier tratamiento de datos personales se lleve a cabo de acuerdo con las leyes nacionales de protección de datos. La

ejecución y cumplimiento de esos requisitos es responsabilidad de todos los empleados pertinentes.

Todos los empleados de DYWIDAG (incluidos los empleados temporales y el personal contratado), ejecutivos y proveedores de servicios que tratan datos personales en las instalaciones de DYWIDAG, utilizan los sistemas y equipos de tratamiento de datos de DYWIDAG o están conectados a ellos están obligados a cumplir con esta política.

Auditoría interna del grupo revisará periódicamente el cumplimiento de esta Política de protección de datos mediante revisiones de seguridad de TI o de protección de datos in situ o remotas o evaluaciones similares. Para el desempeño de esta tarea, Auditoría interna del Grupo está autorizada a contratar auditores externos o expertos en esta área.