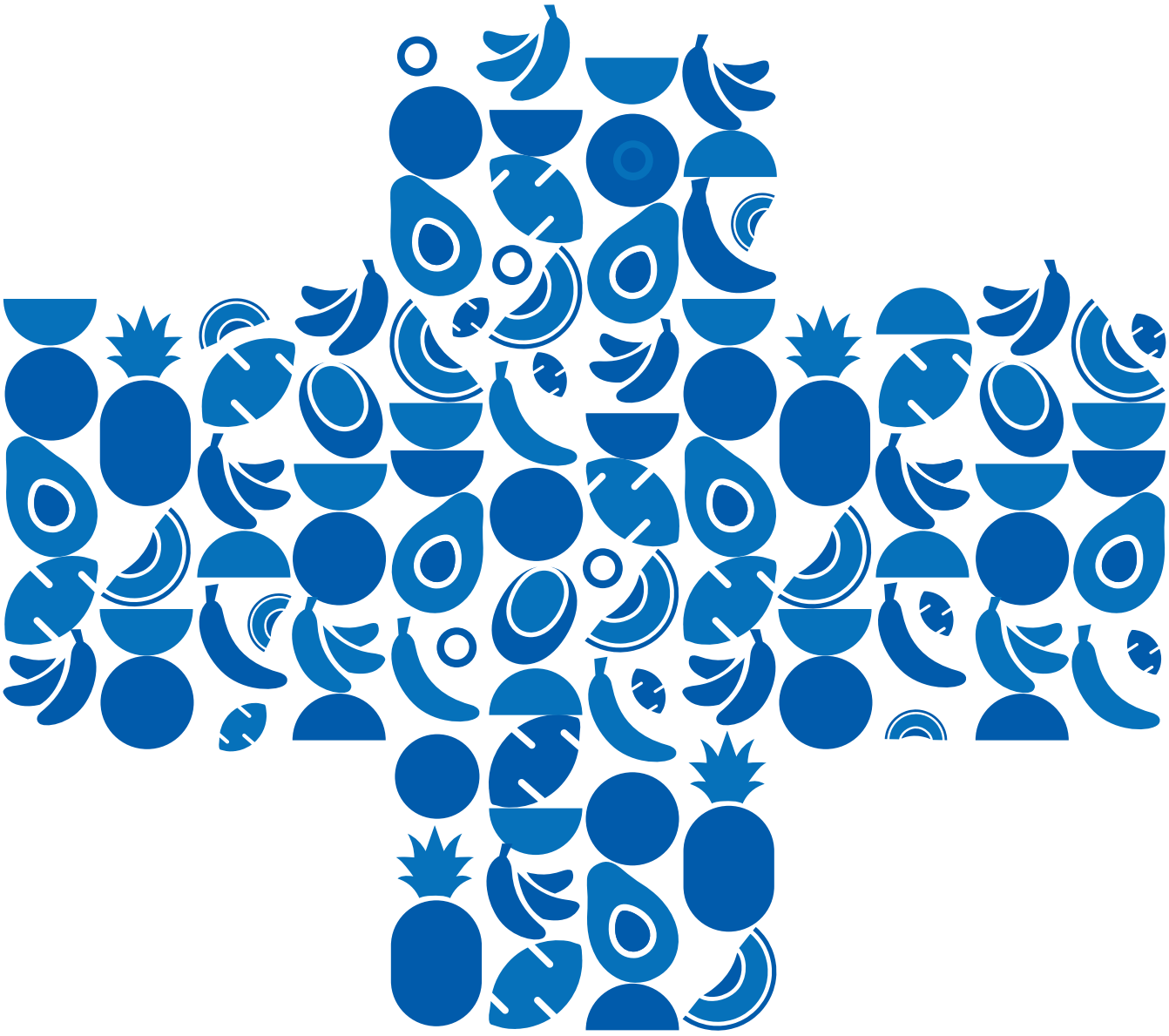
Política de Privacidad de Datos del Grupo Fyffes



Serie de Políticas: Enero 2023

TABLA DE CONTENIDOS

I. ALCANCE **3**

II. MANEJO DE DATOS PERSONALES **3**

III. REGLAS **3**

A. Principios básicos 3

B. Otras normas para situaciones especiales 6

C. Responsabilidad del cumplimiento 7

D. Excepciones 7

IV. GOBERNANZA **7**

A. Solicitudes de los titulares de los datos 7

B. Violación de datos 8

C. Registros de las actividades de procesamientos 8

D. Nuevas actividades de procesamiento 8

E. Concientización, capacitación e información adicional 9

F. Acuerdo de transferencia de datos intragrupo 9

G. Funciones de protección de datos 9

V. OTHER **10**

A. Sanciones 10

B. Revisiones 10

Anexo A: Gobernanza **11**

I. ALCANCE

Toda persona tiene derecho a estar informada y a tomar decisiones sobre la recolección y el procesamiento de sus datos personales[1]. Este derecho está estipulado en un número cada vez mayor de leyes de protección de datos y privacidad en Europa y en todo el mundo, incluida la Ley de Protección de Datos de Suiza y la Ley Revisada de Protección de Datos de Suiza (en conjunto, la **DPA de Suiza**), el Reglamento General de Protección de Datos de la UE (**General Data Protection Regulation, GDPR**), las leyes específicas de cada país en los Estados miembros del Espacio Económico Europeo (todas las leyes en conjunto, las **Leyes de protección de datos**).

Esta Política de Privacidad de Datos del Grupo (la Política) establece cómo Fyffes International S.A. y sus afiliadas identificadas en https://www.fyffes.com/ (el Grupo) protegerán dichos derechos y cumplirán con dichas Leyes de Protección de Datos. Todos los empleados deberán cumplir la Política (cuyo plazo también incluirá a todos los contratistas y otras personas que trabajen en el Grupo, tales como los consultores, de conformidad con el artículo 29 del GDPR) cuando procesen datos personales para el Grupo o en el Grupo. Por supuesto, si se aplican leyes locales más estrictas o acuerdos vinculantes de comités de empresa, tendrán prioridad sobre esta Política.

Es responsabilidad de la gerencia de cada entidad del Grupo tomar las medidas necesarias para aplicar esta Política y las leyes locales más estrictas que se apliquen en dicha entidad del Grupo.

En las instrucciones y manuales disponibles en la intranet de las entidades del Grupo y previa solicitud al Coordinador de Protección de Datos (Data Protection Coordinator, DPC) se ofrecen más detalles sobre los procedimientos y procesos de las entidades del Grupo para cumplir esta Política y las leyes de protección de datos relacionadas.

II. MANEJO DE DATOS PERSONALES[2]

La protección de datos se refiere a los **Datos Personales**, que son cualquier información relacionada con una persona física identificada o identificable, también denominada **titular de los datos**. Basta con que el titular de los datos al que se refiere un conjunto de información solo pueda ser identificado indirectamente utilizando fuentes secundarias (tales como una búsqueda en Internet u otra base de datos). Los Titulares de los datos pueden ser empleados, clientes y otras personas. Todo lo que hagamos con estos datos personales (como, por ejemplo, recolectarlos, utilizarlos, almacenarlos, divulgarlos o eliminarlos) se denomina **procesamiento**. Para determinadas **categorías especiales de datos personales**, las leyes de protección de datos establecen normas más estrictas. Estas categorías especiales de datos personales incluyen los datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, los datos genéticos, los datos biométricos con fines de identificación segura, los datos relativos a la salud o a la vida sexual u orientación sexual de una persona; según la DPA de Suiza, también incluye los datos sobre procedimientos y sanciones administrativas o penales, los datos sobre medidas de seguridad social y los datos sobre la esfera íntima en general.

III. REGLAS

A. Principios básicos

1. Procesamos los datos personales de conformidad con los principios de protección de datos y, cuando se aplica el GDPR, solo si tenemos un fundamento legal suficiente, pero evitamos basarnos en el consentimiento.

En la medida en que el procesamiento de datos personales solo esté sujeto a la DPA de Suiza: No necesitaremos un fundamento legal para procesar los datos personales, siempre y cuando cumplamos los principios de procesamiento establecidos en esta Sección III. Sin embargo, es necesario un fundamento legal para el procesamiento de datos personales en tres situaciones específicas, a saber: (i) si incumplimos uno de los principios de procesamiento establecidos en esta Sección III; (ii) si el titular de los datos se ha opuesto expresamente al procesamiento en cuestión, o (iii) si se divulgan datos personales sensibles a un tercero.

Si el procesamiento de datos personales está sujeto al GDPR: Todas las entidades del Grupo están obligadas a procesar los datos personales únicamente si existe un fundamento legal suficiente para hacerlo. Por lo tanto, todos los **Propietarios de la Actividad de Datos** (como se definen en el Anexo A) deben tomar las medidas adecuadas para confirmar que existe un fundamento legal suficiente consultando con el **Coordinador de Protección de Datos**/Funcionario de Protección de Datos (denominados en conjunto **DPC**) de la entidad relevante del Grupo. El DPC de la entidad relevante del

[1] A los fines de la presente Política de Privacidad de Datos del Grupo, se ha optado por utilizar "ellos" y "sus" al referirse a una persona para utilizar términos no binarios e incluir todos los géneros.
[2] A los fines de esta Política de Privacidad de Datos del Grupo Fyffes, los Datos Personales son cualquier información que se refiera a una persona viva identificada o identificable. Diferentes piezas de información, que recolectadas pueden conducir a la identificación de una persona en particular, también constituyen Datos Personales. Ejemplos de Datos Personales: (i) nombre y apellido; (ii) una dirección particular; (iii) una dirección de correo electrónico, como por ejemplo name.surname@company.com; (iv) un número de documento de identidad; (v) datos de ubicación (por ejemplo, la función de datos de localización de un teléfono móvil); (vi) una dirección de Protocolo de Internet (IP); (vii) un identificador de cookie; y (viii) el identificador publicitario de su teléfono.

Grupo ayudará a determinar las leyes de protección de datos aplicables. Los fundamentos legales en los que más comúnmente se basan para el procesamiento de datos personales en virtud de la DPA de Suiza y el GDPR incluyen los siguientes: (i) la ejecución de un contrato con el titular de los datos o las medidas adoptadas para celebrar un contrato con el titular de los datos a solicitud de este; (ii) el cumplimiento de una obligación legal; (iii) el consentimiento del titular de los datos, y (iv) un "interés legítimo" preponderante.

Existen otros posibles fundamentos legales, y siempre que una entidad del Grupo procese categorías especiales de datos personales o datos penales, deberán establecerse fundamentos legales independientes en consulta con el DPC de la entidad relevante del Grupo en estos casos. Asimismo, el fundamento legal debe ser documentado por el Propietario de la Actividad de Datos. En los casos en que el Propietario de la Actividad de Datos, en consulta con el DPC, haya determinado que el fundamento legal es un "interés legítimo" preponderante, el razonamiento y la ponderación de los distintos intereses deberán documentarse por escrito.

Como norma general, debe evitarse basarse en el consentimiento, ya que es muy difícil obtener un consentimiento legalmente válido y el consentimiento pue-de retirarse en cualquier momento, sin necesidad de justificarlo (lo que significa que la entidad del Grupo podría tener que dejar de procesar los datos personales si la entidad del Grupo se basó en el consentimiento en primer lugar). Cualquier empleado, en particular el Propietario de la Actividad de Datos, se pondrá en contacto con el DPC si el consentimiento debe servir de fundamento legal.

Si los datos personales de una recolección de datos existente van a utilizarse para un fin distinto de aquel para el que se recolectaron, el Propietario de la Actividad de Datos se pondrá en contacto con el DPC para comprobar si está permitido.

2. Somos transparentes y justos en el procesamiento de datos personales.

Wnformaremos al titular de los datos que estamos procesando sus datos personales, comunicándoselo, publicando avisos, utilizando carteles informativos u otros medios. No recolectaremos datos personales de forma encubierta ni los procesaremos de forma inesperada para el titular de los datos.

El Propietario de la Actividad de Datos está obligado a garantizar que se pongan a disposición de los titulares de datos avisos de privacidad adecuados en nuestros sitios web y por otros medios apropiados para informarles sobre lo que la entidad del Grupo hace con sus datos. Las Leyes de Protección de Datos aplicables definen la información que debe incluirse en estos avisos.

El Propietario de la Actividad de Datos consultará con el DPC para determinar y desarrollar los avisos de privacidad apropiados. El Propietario de la Actividad de Datos, en consulta con el DPC, verificará si cualquier nuevo procesamiento de datos personales ya está cubierto por un aviso de privacidad existente que ya se haya puesto a disposición de los titulares de los datos. Al evaluar si el aviso de privacidad cubre nuestra nueva actividad de procesamiento prevista, el Propietario de la Actividad de Datos tendrá en cuenta que los compañeros de trabajo también pueden ser titulares de los datos (y no solo terceros). Los Propietarios de la Actividad de Datos están obligados a garantizar que los datos personales no se procesen de manera que pueda percibirse como desleal o contraria a la buena fe.

3. Solo utilizaremos los datos personales para los fines para los que los recolectamos.

Si un Propietario de la Actividad de Datos planea una nueva actividad de procesamiento, debe comprender desde el principio los fines para los que se recolectarán y procesarán los datos personales. El Propietario de la Actividad de Datos está obligado a garantizar que dichos fines se comuniquen al titular de los datos en el momento de la recolección de datos (a menos que se aplique una excepción). Esto incluye informar al titular de los datos de la divulgación de sus datos personales a un tercero para sus propios fines (como controlador), si este es el plan, y de cualquier otro aspecto que deba divulgarse por ley al titular de los datos, según lo dispuesto en la sección 2 anterior. El Propietario de la Actividad de Datos consultará con el DPC para cumplir con este principio.

Si el Propietario de la Actividad de Datos desea utilizar los datos personales para un fin distinto del inicial, se pondrá en contacto con el DPC de la entidad relevante del Grupo para averiguar si esto está permitido y si se requiere algún otro paso (como facilitar nueva información al titular de los datos o su consentimiento).

[3] Se publicará próximamente

4. Solo recolectaremos los datos que realmente necesitemos.

No intentaremos recolectar tantos datos personales como sea posible, sino que trataremos de limitarnos a los que realmente necesitemos para el fin específico. Los Propietarios de la Actividad de Datos están obligados a cumplir este principio.

Si un Propietario de la Actividad de Datos desea recolectar datos personales útiles, pero no estrictamente necesarios, se pondrá en contacto con el DPC. El Propietario de la Actividad de Datos tratará de evitar actividades de procesamiento que, debido a la magnitud de los datos recolectados o al alcance de su utilización, puedan provocar malestar o preocupación en el titular de los datos o causar daños a su reputación.

5. Solo conservaremos los datos durante el tiempo que los necesitemos y limitaremos el acceso a los mismos.

Limitaremos el acceso a los datos personales a quienes realmente necesiten tener acceso a ellos (según el principio de "necesidad de conocer") y lo limitaremos continuamente. Todos los empleados, y en particular los Propietarios de la Actividad de Datos, están obligados a tomar medidas para cumplir este principio. Todos los empleados deberán consultar la Política de Conservación de Datos del Grupo[3] para obtener instrucciones detalladas sobre los períodos de conservación de las distintas categorías de documentos conservados por la entidad del Grupo. Si los datos personales ya no son necesarios para los fines para los que se obtuvieron, y si las obligaciones legales y los intereses comerciales legítimos lo permiten, los Propietarios de la Actividad de Datos se asegurarán de que los datos se eliminen o se conviertan en anónimos. Los Propietarios de la Actividad de Datos se pondrán en contacto con el DPC para recibir instrucciones sobre cómo hacerlo. Al diseñar un proyecto que implique el procesamiento de datos personales, el Propietario de la Actividad de Datos verificará la capacidad de eliminar (o anonimizar adecuadamente) los datos personales una vez que ya no sean necesarios. El Propietario de la Actividad de Datos deberá tener en cuenta desde el principio (por ejemplo, en un proyecto) cómo garantizar que los datos se eliminen en el momento adecuado y que no se pase por alto ese momento.

6. Cuando sea razonablemente posible, ofrecemos a los titulares de los datos la posibilidad de elegir.

Esto se aplica incluso cuando no nos basamos en el consentimiento. Por ejemplo, si un titular de los datos se opone a que procesemos sus datos, determinaremos si estamos obligados a dejar de hacerlo y, si no existen motivos legítimos convincentes ni requisitos legales aplicables que lo permitan, lo haremos. Si un empleado recibe una objeción de este tipo, consultará con el DPC para determinar el manejo adecuado de dicha objeción. Si no se necesitan determinados datos para alcanzar los fines previstos, el Propietario de la Actividad de Datos se asegurará de que los titulares de los datos sean conscientes de que pueden elegir si desean compartirlos con la entidad del Grupo. Si un titular de los datos ya no desea que la entidad del Grupo utilice sus datos con fines de marketing, la entidad del Grupo está obligada a poner fin a dicho procesamiento. Al diseñar una actividad de procesamiento que implique el procesamiento de datos personales, el Propietario de la Actividad de Datos se asegurará de que el procesamiento de los datos personales facilitados voluntariamente pueda detenerse en cualquier momento, sin grandes esfuerzos.

7. Garantizamos la exactitud de los datos personales que procesamos.

Tomamos medidas razonables para garantizar que los datos personales sean exactos y, si es necesario, se mantengan actualizados en función de su relevancia y sus fines. En consecuencia, el Propietario de la Actividad de Datos tomará medidas razonables para rectificar los datos o, si esto no es factible, para cederlos, y para mantener los datos sincronizados de forma generalizada. El Propietario de la Actividad de Datos tomará medidas razonables para garantizar que las rectificaciones que fueron informadas a la entidad del Grupo (por ejemplo, por un titular de los datos) "sobrevivirán" al evento de restauración de los datos mediante una copia de seguridad.

8. Anonimizaremos y no volveremos a identificar a los titulares de los datos.

Cuando sea posible, el Propietario de la Actividad de Datos se asegurará de que los datos personales estén "codificados" de tal manera que los titulares de los datos no puedan ser identificados por aquellos que no tengan la "clave de reidentificación" del código. El Propietario de la Actividad de Datos tomará medidas para limitar el acceso al código a aquellas personas que necesiten tener acceso a este. Asimismo, los empleados no intentarán volver a identificar a las personas a las que se refieren los datos, a menos que tengan una buena razón para hacerlo. Ambas medidas ayudarán a proteger su privacidad.

9. Dispondremos de una seguridad de datos adecuada, tanto desde el punto de vista técnico como de otro tipo.

Es importante mantener en todo momento la confidencialidad, integridad y disponibilidad de todos los datos personales en los sistemas y la organización de las entidades del Grupo. Por lo tanto, no solo quienes se ocupan de la infraestructura de las entidades del Grupo (TI, edificio), sino todos los empleados son personalmente responsables de garantizar la seguridad de los datos y deberán mantener la confidencialidad de cualquier dato personal al que los empleados hayan tenido acceso en el trabajo o en el contexto de su relación laboral con la entidad del Grupo. Como norma general, no está permitido llevarse copias impresas de documentos o soportes de datos relacionados con el trabajo fuera de las instalaciones. Todos los empleados deberán comunicar electrónicamente asuntos relacionados con el trabajo únicamente a través de redes seguras utilizando sistemas seguros, cuando sea posible. Todos los empleados deben consultar la Política de Uso Aceptable de TI del Grupo para obtener información más detallada sobre cómo utilizar los recursos de TI del Grupo.

10. Nos aseguraremos de que se cumplan estas normas desde el principio.

Todos los empleados deben garantizar que siempre que diseñen un sistema, planifiquen un proyecto o pongan en marcha o modifiquen una actividad que implique el procesamiento de datos personales, estas normas se cumplan desde el principio y que la entidad del Grupo pueda atender las solicitudes de los titulares de los datos que ejerzan sus derechos conforme a la Sección IV. A ("privacidad por diseño"). Asimismo, cuando los titulares de los datos puedan elegir la forma en que la entidad del Grupo procesa sus datos personales, el Propietario de la Actividad de Datos optará, por defecto, por la opción de procesamiento más respetuosa con la privacidad ("privacidad por defecto"). Esto es especialmente importante cuando se prestan servicios en línea y se utilizan aplicaciones para usuarios registrados.

11. Capacitaremos y crearemos conciencia entre los empleados en materia de protección de datos.

Las entidades del Grupo se asegurarán de que todos los empleados sean cons-cientes de sus tareas en relación con la garantía del cumplimiento de la protección de datos y de que reciban capacitación periódica sobre protección de datos en relación con su función y área de responsabilidad, como parte de nuestra capacitación para nuevas contrataciones y para empleados existentes. Dicha capacitación ayudará a los empleados, en particular a los Propietarios de la Actividad de Datos, a comprender sus obligaciones en virtud de esta Política y de la legislación aplicable en materia de protección de datos. Los registros de finalización de capacitación serán mantenidos por el departamento de Recursos Humanos a nivel local. Todos los empleados deberán comprometerse a mantener la confidencialidad.

12. Cooperaremos con las autoridades de supervisión.

Todos los empleados deben asegurarse de que las solicitudes de las autoridades de protección de datos ("**Autoridades de Supervisión**") se envíen al DPC inmediatamente para garantizar un manejo adecuado de dichas solicitudes. El DPC es responsable del manejo adecuado de dicha solicitud, incluida la consulta apropiada con las partes interesadas internas, tales como el departamento legal y de cumplimiento normativo, el enlace con asesores legales externos y la respuesta oportuna a las Autoridades de Supervisión.

B. Otras normas para situaciones especiales

1. Utilización de terceros

Si una entidad del Grupo recurre a terceros, tales como proveedores de servicios, contratistas individuales u otras entidades del Grupo, se aplicarán determinadas restricciones en virtud de la legislación sobre protección de datos si se da a estos terceros acceso a datos personales o se les pide que los procesen. Dependiendo de la función del tercero, el Propietario de la Actividad de Datos se asegurará, junto con el DPC, de que existe un fundamento legal suficiente para su acceso a los datos personales.

Si el Propietario de la Actividad de Datos desea contratar a dicho tercero en una entidad del Grupo, el Propietario de la Actividad de Datos deberá, en consulta con el DPC:

(i) aclarar la función del tercero desde el punto de vista de la ley de protección de datos, en particular si se trata de un "procesador" (es decir, alguien que procesa totalmente bajo nuestras instrucciones y mantenemos el control), un "controlador" (es decir, alguien que es en sí mismo responsable del procesamiento), un "controlador conjunto" (es decir, alguien con quien decidimos conjuntamente sobre el procesamiento) o una persona que actúa bajo nuestras instrucciones (como, por ejemplo, un consultor de conformidad con el artículo 29 del GDPR);

(ii) evaluar si el tercero es calificado y digno de confianza y si ofrece la seguridad de datos adecuada para que se le confíen los datos personales en cuestión;

(iii) establecer las cláusulas contractuales necesarias, incluido un acuerdo de procesamiento de datos en el caso de un "procesador", un "acuerdo de controlador conjunto" en el caso de un "controlador conjunto" o, como mínimo, un acuerdo de no divulgación en el caso de un "controlador" o una persona que actúe bajo nuestras instrucciones (como, por ejemplo, un consultor de conformidad con el artículo 29 del GDPR);

(iv) dar las instrucciones oportunas al tercero, cuando corresponda; y

(v) consultar al DPC de la entidad del Grupo o al asesor legal sobre todos los pasos y evaluar si está permitido que la entidad del Grupo permita incluso que el tercero tenga acceso a los datos personales, aunque solo sea como proveedor de servicios.

El proceso será documentado por el Propietario de la Actividad de Datos, con el apoyo del DPC.

2. Exportación de datos personales

Siempre que una entidad del Grupo ponga datos personales a disposición de un destinatario en un país distinto de Suiza, el Reino Unido o el AEE (entre otros), se aplicarán determinadas restricciones en virtud de las Leyes de protección de datos. Esto incluye el otorgamiento de acceso remoto a alguien en el extranjero (pero no incluye las publicaciones en línea).

Si una entidad del Grupo desea poner datos personales a disposición de un des-tinatario en otro país (excepto a otras entidades del Grupo que hayan firmado el IGDTA, consulte la Sección IV.F), el Propietario de la Actividad de Datos deberá (i) determinar, con el apoyo del DPC, si el destinatario se encuentra en un país con un nivel adecuado de protección de datos, (ii) en caso contrario facilitar toda la información necesaria al DPC para que este pueda realizar una evaluación del riesgo de acceso potencialmente ilícito por parte de autoridades extranjeras al poner los datos a disposición del destinatario en el extranjero, como exige la Ley de Protección de Datos aplicable, y en función del resultado, (iii) tomar medidas para celebrar un acuerdo de transferencia de datos adecuado entre la entidad del Grupo y el destinatario e imponer al destinatario todas las demás medidas complementarias necesarias para proteger los datos personales mientras estén en manos del destinatario; o, si esto no es posible o si los riesgos determinados por el DPC en su evaluación en (ii) siguen siendo demasiado altos (iv) determinar otra solución para el proyecto previsto junto con el DPC para cumplir con los requisitos internacionales de transferencia de datos. El DPC de la entidad del Grupo se pondrá en contacto con el asesor legal cuando lo considere necesario para cumplir los requisitos de transferencia internacional de datos.

El proceso será documentado por el Propietario de la Actividad de Datos, con el apoyo del DPC.

3. Decisiones individuales automatizadas, elaboración de perfiles

Siempre que una entidad del Grupo permita que un ordenador tome una decisión discrecional sobre una persona o evalúe las características personales de una persona ("elaboración de perfiles"), que pueda tener un efecto legal o de importancia similar sobre la persona (por ejemplo, la denegación o ejecución de un contrato), se aplicarán determinadas restricciones en virtud de las Leyes de Protección de Datos.

Si se necesitan decisiones automatizadas, el Propietario de la Actividad de Datos se asegurará de que (i) se cumplan las condiciones previas en virtud de las Leyes de Protección de Datos aplicables (por ejemplo, la decisión individual automatizada es necesaria para celebrar o ejecutar un contrato); (ii) el titular de los datos tiene derecho a ser oído por una persona y a exigir que la decisión sea reevaluada por ella; (iii) el aviso de privacidad de la entidad del Grupo hace referencia a estas decisiones, y (iv) el Propietario de la Actividad de Datos consulta con el DPC de la entidad del Grupo, el Funcionario de Protección de Datos (Data Protection Officer, DPO) del Grupo o el asesor legal antes de implementar un sistema automatizado de toma de decisiones para verificar el cumplimiento de las Leyes de Protección de Datos.

El proceso será documentado por el Propietario de la Actividad de Datos, con el apoyo del DPC.

C. Responsabilidad del cumplimiento

Garantizar el cumplimiento de las normas anteriores y las de la Sección IV en cada entidad del Grupo es responsabilidad de cada empleado. Los propietarios de aquellas actividades empresariales en las que se produzca un procesamiento de datos personales o para las que se lleve a cabo dicho procesamiento; y de cualquier persona con gestión u otro control parcial o total sobre dicho procesamiento, supervisarán el

cumplimiento dentro de su responsabilidad. En el Anexo A (Gobernanza) figuran más detalles, incluida una descripción de las funciones y responsabilidades.

D. Excepciones

En determinadas condiciones, la legislación aplicable permite a la entidad del Grupo apartarse de estos principios básicos y de otras normas para el procesamiento de datos personales. Sin embargo, cualquier desviación de este tipo deberá ser revisada por el DPC para garantizar que cumple con la ley y aprobada por el gerente comercial con la titularidad del riesgo de cumplimiento pertinente en general o en un caso concreto, previa consulta con el DPC de la entidad del Grupo en cuestión, el DPO del Grupo o el asesor legal. El proceso será documentado por el Propietario de la Actividad de Datos, con el apoyo del DPC.

IV. GOBERNANZA

A. Solicitudes de los titulares de los datos

Los titulares de los datos tienen una serie de derechos que pueden hacer valer cuando las entidades del Grupo controlan el procesamiento de sus datos personales. A menos que la Ley de Protección de Datos aplicable establezca lo contrario (por ejemplo, proteger a terceros o secretos comerciales en caso de solicitudes de acceso), la entidad del Grupo tomará medidas para cumplir las correspondientes solicitudes de los titulares de los datos. Las entidades del Grupo están sujetas a plazos para hacerlo. Antes de responder a una solicitud, el DPC debe asegurarse de que el solicitante está debidamente identificado.

Entre los derechos de los titulares de los datos figuran:

(i) el derecho a acceder y obtener una copia de los datos personales que la entidad del Grupo procese sobre ellos, además de determinada información complementaria;

(ii) el derecho a rectificar los datos personales inexactos o incompletos;

(iii) el derecho a solicitar a la entidad del Grupo que restrinja el procesamiento de sus datos personales o se oponga a él de cualquier otro modo;

(iv) el derecho a solicitar a la entidad del Grupo que elimine sus datos (“derecho al olvido”);

(v) el derecho a solicitar a la entidad del Grupo que informe a los terceros con los que la entidad del Grupo haya compartido datos personales sobre una solicitud particular del titular de los datos;

(vi) el derecho a obtener una copia de los datos personales que la entidad del Grupo haya obtenido de un titular de los datos para que este pueda utilizarlos con otro controlador (“derecho a la portabilidad de los datos”);

(vii) el derecho a retirar el consentimiento en cualquier momento; y

(viii) el derecho a oponerse, por motivos relacionados con la situación particular del titular de los datos, en cualquier momento, al procesamiento de sus datos personales, en particular, si el procesamiento se basa en un “interés legítimo” preponderante.

Por lo general, estos derechos pueden ejercerse de forma gratuita y sin indicar los motivos.

Si usted, como empleado, recibe una solicitud de este tipo, deberá enviarla inmediatamente al DPC. Si no está seguro de cómo manejar una solicitud específica, consulte al DPC de su entidad del Grupo, al DPO del Grupo o al asesor legal en dichos casos para verificar el cumplimiento de las Leyes de Protección de Datos aplicables. El proceso será documentado por el DPC.

En cada entidad del Grupo, la gerencia puede designar a una persona o crear una función para manejar las solicitudes de los titulares de los datos. Si se ha designado a dicha persona, el DPC le enviará la solicitud para que la maneje. Si no existe dicha persona o función, el DPC de la entidad del Grupo manejará estas solicitudes por sí mismo. Sin embargo, la responsabilidad de las decisiones de oponerse a una solicitud corresponderá a la gerencia de la entidad del Grupo, previa consulta al DPC y, en los casos que puedan dar lugar a litigios, al DPO del Grupo o al asesor legal.

B. Violación de datos

Si se produce una violación de la seguridad de los datos, es decir, cuando la confidencialidad, integridad, disponibilidad o resiliencia de los datos personales que procesamos se vulnera de forma intencional o accidental, dando lugar, por ejemplo, a una divulgación no autorizada o ilícita, pérdida o alteración de datos personales (por ejemplo, información enviada a un destinatario equivocado, pérdida o robo de un soporte de datos no protegido, ciberataques, etc.), la entidad del Grupo está obligada por las leyes de protección de datos a (i) tomar inmediatamente medidas para detener la violación y mitigar el posible impacto negativo sobre los titulares de los datos; (ii) investigar la violación de datos (incluido el análisis de la causa raíz), (iii) evaluar

la gravedad y la probabilidad del posible impacto negativo para los titulares de los datos afectados, (iv) notificar a las Autoridades de Supervisión competentes las violaciones que tengan riesgos relevantes para los titulares de los datos y hacerlo lo antes posible, pero en cualquier caso en el plazo de 72 horas desde que se tenga conocimiento de ellas, (v) en casos especiales, informar también a los titulares de los datos, (vi) tomar medidas que eviten dichas violaciones de datos en el futuro, y (vii) mantener un registro de cada violación de datos, su evaluación y las medidas tomadas.

Si la entidad del Grupo procesa datos personales como procesador para otra persona (actuando como controlador), la entidad del Grupo deberá en cualquier caso notificarlo inmediatamente a esta otra persona.

Si usted, como empleado, toma conocimiento de cualquier violación de datos real o presunta, ya sea por su culpa o no, está obligado a informar inmediatamente al **Punto de Contacto de Violación de Datos** de su organización y, si no existe esa persona, al DPC. Estas personas pondrán en marcha el Grupo de Respuesta ante la Violación de Datos y les indicarán las medidas que, en su caso, deban tomar.

El **Grupo de Respuesta a la Violación de Datos** se reunirá inmediatamente y garantizará el cumplimiento de las obligaciones indicadas anteriormente y establecidas en las Leyes de Protección de Datos aplicables; el DPO del Grupo, si corresponde, será informado en todo momento y consultado antes de cualquier notificación. La gerencia de cada entidad del Grupo es responsable de (i) implementar un Punto de Contacto de Violación de Datos adecuado, (ii) establecer un Grupo de Respuesta ante la Violación de Datos formado por representantes del departamento de TI, de seguridad de la información, legal, el DPC y la alta dirección (el DPC mantendrá los registros) y con un director y un adjunto, (iii) establecer los procedimientos e instrucciones necesarios y (iv) mantener informado al DPO del Grupo.

Cualquier notificación a una autoridad o a terceros será realizada exclusivamente por el DPO del Grupo, a menos que las Leyes de Protección de Datos exijan que un representante legal de la entidad del Grupo realice la notificación o que el DPO del Grupo delegue dicha tarea en el DPC, en el director del Grupo de Res-puesta a la Violación de Datos o en cualquier otra persona de la entidad del Grupo relevante. El DPC de la entidad del Grupo mantendrá los registros requeridos y facilitará una copia al DPO del Grupo.

C. Registros de las actividades de procesamiento

La entidad del Grupo debe mantener un inventario de sus actividades para las que la entidad del Grupo procesa datos personales como parte de su negocio (por ejemplo, nóminas, archivo de personal, contratación, marketing directo), ya sea en calidad de controlador o de procesador. Esto debe hacerse para cada entidad del Grupo. Las Leyes de Protección de Datos establecen qué información debe incluirse en este registro de actividades de procesamiento, y el DPC y el DPO del Grupo podrían exigir que se incluya información adicional relevante en los registros de actividades de procesamiento.

Los registros serán mantenidos por el DPC de la entidad del Grupo (que será responsable, con la ayuda de un asesor legal, según sea necesario, de asegurarse de que contienen la información necesaria), pero es responsabilidad del propietario de cada actividad de procesamiento notificar al DPC todas las actividades de procesamiento y proporcionar toda la información necesaria al DPC para que este pueda preparar y mantener los registros de actividades de procesamiento para todas las actividades de procesamiento. Los empleados deben proporcionar toda la información necesaria al DPC, ya sea previa solicitud o siempre que cambie una actividad de procesamiento, para que el DPC pueda mantener actualizados los registros de actividades de procesamiento. Cada registro de actividades de procesamiento identificará al Propietario de la Actividad de Datos responsable de la actividad de procesamiento. Se debe proporcionar una copia de los registros al DPO del Grupo cada vez que se creen o actualicen.

D. Nuevas actividades de procesamiento

Siempre que se inicie una nueva actividad que implique el procesamiento de datos personales, o se prevea modificar sustancialmente un procesamiento de datos personales existente, la entidad del Grupo deberá garantizar que cumple o sigue cumpliendo esta Política y las Leyes de Protección de Datos aplicables.

Para ello, el Propietario de la Actividad de Datos debe, en particular, verificar y documentar que (i) se cumplen los principios básicos (en la Sección III) (sujeto a cualquier excepción de conformidad con la Sección III.D); (ii) se cumplen las normas adicionales (en la Sección III.B) (sujeto a cualquier excepción de con-formidad con la Sección III.D); (iii) los registros de las actividades de procesamiento se actualizan

de conformidad con la Sección IV.C, y (iv) cuando sea necesario, se ha llevado a cabo una evaluación del impacto sobre la protección de datos (Data Protection Impact Assessment, DPIA) y/o una evaluación del interés legítimo en consulta con el DPC.

Una DPIA documentará la actividad de procesamiento, los posibles efectos negativos sobre los titulares de los datos, las medidas para prevenir o mitigar dichos efectos y el nivel general de riesgo para los titulares de los datos a pesar de las medidas implementadas. Si el riesgo residual sigue siendo elevado, podría ser necesario consultar a las Autoridades de Supervisión competentes, de conformidad con las Leyes de Protección de Datos aplicables. Es necesaria una DPIA para las actividades de procesamiento que puedan presentar un riesgo elevado para los titulares de los datos, que se define con más detalle en las Leyes de Protección de Datos aplicables.

Es responsabilidad del Propietario de la Actividad de Datos (i) garantizar el cumplimiento de esta Política y de las Leyes de Protección de Datos aplicables, e (ii) iniciar el proceso de verificación y documentación con la ayuda del DPC de la entidad del Grupo relevante o del asesor legal. Esto incluye la realización de una DPIA de conformidad con las Leyes de Protección de Datos. El DPC llevará un registro de la documentación y proporcionará una copia al DPO del Grupo, si corresponde.

La gerencia de la entidad del Grupo establecerá los procedimientos necesarios para garantizar el cumplimiento de lo anterior.

E. Concientización, capacitación e información adicional

Cada empleado debe (i) estudiar esta Política, determinar cómo se aplica a su función y cumplirla, (ii) realizar la capacitación inicial y de actualización sobre protección de datos ofrecida por el Grupo o la entidad del Grupo y, según corresponda, en vista de su función, (iii) estudiar la información proporcionada por el Grupo y la entidad del Grupo a los titulares de los datos con respecto al procesamiento de sus datos personales (avisos de privacidad, etc.) y actuar de acuerdo con dicha información (es decir, si les decimos a los titulares de los datos que solo procesamos sus datos de una determinada manera, por lo general tenemos que cumplir esta declaración, y si no podemos, tenemos que cambiar lo que les decimos a los titulares de los datos), (iv) consultar otras directrices ofrecidas por el Grupo y la entidad del Grupo sobre cómo cumplir esta Política y las Leyes de Protección de Datos aplicables, y (v) consultar al DPC de la entidad del Grupo o al asesor legal, si las cuestiones siguen sin estar claras o si el empleado no está seguro de cómo manejar el procesamiento de datos personales o de cómo cumplirlo.

F. Acuerdo de transferencia de datos intragrupo

Las transferencias de datos personales y las delegaciones del "controlador-procesador" del procesamiento de datos personales dentro del Grupo se regirán por un Acuerdo de transferencia de datos intragrupo (**Intra-Group Data Transfer Agreement, IGDTA**) del que formarán parte todas las entidades del Grupo. La entidad del DPO del Grupo será la administradora del IGDTA y lo actualizará cuando sea necesario. Cada entidad del Grupo proporcionará al DPO del Grupo toda la información y el apoyo que se le solicite para implementar el IGDTA y mantenerlo actualizado y de conformidad con las Leyes de Protección de Datos aplicables.

G. Funciones de protección de datos

La responsabilidad del cumplimiento de las Leyes de Protección de Datos aplicables es de cada entidad del Grupo y de su gerencia en lo que respecta a las actividades de procesamiento controladas por ella. Cada empleado debe tomar todas las medidas razonables establecidas en esta Política para apoyar a la entidad del Grupo en su cumplimiento de la Ley de Protección de Datos aplicable y omitir cualquier actividad que viole la Ley de Protección de Datos aplicable y esta Política.

La gerencia de cada entidad del Grupo proporcionará al DPO del Grupo un informe sobre el cumplimiento de la protección de datos por parte de la entidad al menos una vez al año. El cumplimiento de la entidad podría ser auditado a petición del DPO del Grupo, de la gerencia del Grupo o por iniciativa de la auditoría interna del Grupo, y la entidad del Grupo apoyará plenamente dichas auditorías.

El **DPO del Grupo** será responsable de gestionar el cumplimiento de las normas de protección de datos del Grupo, incluido el establecimiento de las normas mínimas de protección de datos aplicables en el Grupo y las actividades de los DPC. Se dará al DPO del Grupo la independencia y los recursos necesarios para cumplir su tarea de manera razonable. Los DPC estarán subordinados al DPO del Grupo. El DPO del

Grupo tendrá derecho a verificar el cumplimiento de la protección de datos por parte de cada entidad del Grupo, a recibir cualquier información y acceso solicitados y a dar las instrucciones correspondientes. El DPO del Grupo será consultado sobre cualquier cuestión importante relacionada con la protección de datos y tendrá una vía jerárquica sólida con la alta gerencia del Grupo. El DPO del Grupo proporcionará a la alta gerencia del Grupo un informe sobre el cumplimiento de la protección de datos por parte del Grupo al menos una vez al año, y podría plantear directamente a dicha alta gerencia cualquier cuestión relativa al cumplimiento de la presente Política y de las Leyes de Protección de Datos. Si las responsabilidades en virtud de esta Política no están claras o son objeto de controversia en un asunto concreto, el DPO del Grupo tomará una determinación al respecto, y remitirá a la gerencia de la entidad del Grupo (si las responsabilidades se limitan a dicha entidad) o a la alta gerencia del Grupo.

La gerencia de cada entidad del Grupo nombrará a un **Coordinador de Protección de Datos** o, si así lo exige la Ley de Protección de Datos aplicable, a un **Funcionario de Protección de Datos** (denominados en conjunto **DPC**) para gestionar el cumplimiento de la protección de datos en dicha entidad y asistir a la entidad en sus obligaciones de cumplimiento de la protección de datos, a costa y bajo la responsabilidad de las entidades. La gerencia de cada entidad del Grupo debe cumplir todos los requisitos a la hora de nombrar a un Funcionario de Protección de Datos, incluida la notificación del nombramiento a la Autoridad de Supervisión competente. Varias entidades podrían nombrar al mismo DPC, pero este deberá estar contratado por una de las entidades del Grupo. Se dará al DPC la independencia y los recursos necesarios para cumplir su tarea de manera razonable. El Anexo A (Gobernanza) contiene más detalles.

V. OTROS

A. Sanciones

La violación de la Ley de Protección de Datos aplicable puede dar lugar a sanciones graves por parte de las Autoridades de Supervisión y, en virtud de determinadas leyes nacionales, a responsabilidad penal personal. En virtud del GDPR, las sanciones administrativas por violaciones intencionales o no intencionales del GDPR pueden alcanzar hasta el 4% de la facturación anual total mundial o 20 millones de euros, la cantidad que sea mayor. En virtud de la DPA de Suiza, es posible imponer multas personales de hasta 250 000 francos suizos por violaciones intencionales o por ceguera voluntaria. Además, se podría ordenar a las entidades del Grupo que detengan o cambien determinadas actividades de procesamiento, y pueden ser objeto de demandas civiles por parte de los titulares de los datos.

En consecuencia, es importante que todos los empleados cumplan esta Política, ya sea como empleados regulares o en una función especial prevista en la Política. El incumplimiento de esta Política puede dar lugar a sanciones en virtud del contrato laboral, incluido el despido.

B. Revisiones

El propietario de esta Política es el DPO del Grupo. Se revisará cuando sea necesario y se examinará al menos anualmente. El DPO del Grupo tiene derecho a emitir otras políticas que detallen las obligaciones y otras disposiciones contenidas en esta Política, sujeto a la aprobación formal de la alta gerencia del Grupo.

Aprobado y emitido por Marina Souza, Directora Global de Legales de Fyffes, en enero 2024.

Anexo A

Gobernanza

Este Anexo detalla las funciones relevantes para el cumplimiento de la ley de protección de datos y se basa en la Política de Privacidad de Datos del Grupo (la **Política**), en particular en la Sección III.C y en la Sección IV.G. Lo siguiente se aplica a **cada entidad del Grupo**:

- La **Junta Directiva** es el organismo con máxima responsabilidad por el cumplimiento de la ley de protección de datos aplicable por parte de la entidad del Grupo y, en el contexto del Grupo, de la Política. Deberá:
    - Tener un conocimiento básico de la Ley de Protección de Datos aplicable y de los requisitos de la Política.
    - Exigir a la Gerencia que implemente la Política para garantizar el cumplimiento por parte de la entidad de la Ley de Protección de Datos aplicable y de la Política a nivel operativo.
    - Estudiar los informes de cumplimiento proporcionados, investigar los indicios de incumplimiento y tomar las medidas correctivas necesarias en consulta con el DPO del Grupo y la Gerencia del Grupo.
    - Proporcionar informes sobre el cumplimiento por parte de la entidad de la Ley de Protección de Datos y la Política aplicables a la Gerencia del Grupo y al DPO del Grupo (i) de forma regular (al menos una vez al año), (ii) en caso de que se produzcan desarrollos importantes, y (iii) si se solicita.
- La **Gerencia**, en particular el **director ejecutivo (CEO)**, tiene la responsabilidad operativa del cumplimiento de la ley de protección de datos aplicable y de la Política por parte de la entidad del Grupo. Deberá:
    - Tener un conocimiento básico de la Ley de Protección de Datos aplicable y de los requisitos de la Política.
    - Emitir las instrucciones necesarias para que se implemente la Política y se cumpla en la entidad, lo que incluye (i) la designación de las funciones necesarias (incluidas las previstas en este Anexo), y (ii) el establecimiento de los procesos necesarios para el cumplimiento de la Política.
    - Garantizar el cumplimiento de la Ley de Protección de Datos aplicable en la entidad, además de las disposiciones de la Política.
    - Garantizar que, cuando se deleguen tareas, los delegados sean debidamente seleccionados, instruidos y supervisados por la Gerencia.
    - Estudiar los informes de cumplimiento proporcionados, investigar los indicios de incumplimiento y tomar las medidas correctivas necesarias en consulta con el DPC y el DPO del Grupo.
    - Proporcionar informes sobre el cumplimiento por parte de la entidad de la Ley de Protección de Datos y la Política aplicables a la Junta Directiva y al DPO del Grupo (i) de forma regular (al menos una vez al año), (ii) en caso de que se produzcan desarrollos importantes, y (iii) si se solicita.
- Cada actividad de procesamiento de datos personales (la **Actividad**) tendrá al menos un **Propietario de la Actividad de Datos (DAO)**, que será responsable (solo o con otros DAO de la misma Actividad) del cumplimiento de dicha Actividad con la Ley de Protección de Datos aplicable y la Política. A menos que la Gerencia decida lo contrario en un caso específico, el DAO de una Actividad es su "beneficiario" en primera línea de defensa, es decir, el titular de aquellas actividades comerciales en las que se produce el procesamiento de datos personales y para las que se lleva a cabo la Actividad. Además, se considerará DAO a cualquier otra persona que ejerza la gestión u otro tipo de control parcial o total sobre dicho procesamiento; por "control" se entenderá el poder legal o de facto pa-ra tomar, o la toma real, de decisiones relativas a aspectos de la Actividad que son esenciales para su cumplimiento de la Política o la Ley de Protección de Datos aplicable (por ejemplo, qué categorías de datos personales se recopilan, las categorías de destinatarios de los datos personales, los períodos de conservación).
  Si hay varios DAO para la misma actividad, cada DAO es responsable de sus propias decisiones y de las de cualquier DAO que esté subordinado a dicho DAO. Deberá:
    - Tener un conocimiento de la Ley de Protección de Datos aplicable y de los requisitos de la Política con respecto a la Actividad.
    - Seleccionar al personal adecuado y dar las instrucciones necesarias para que la Política

y los requisitos adicionales de la Ley de protección de datos aplicable se implementen y se cumplan en la entidad con respecto a la Actividad, y supervisar la correcta ejecución de la instrucción, incluso solicitando los informes apropiados.
    - Tomar decisiones con respecto a la Actividad únicamente de conformidad con la Política y los requisitos adicionales de la Ley de Protección de Datos aplicable y previa consulta al DPC y, cuando corresponda, al DPO del Grupo; cuando el DAO llegue a la conclusión de que no puede o no quiere tomar una decisión, la comunicará a su superior, que también se convertirá en un DAO.
    - Estudiar los informes de cumplimiento proporcionados con respecto a la Actividad, investigar los indicios de incumplimiento y tomar las medidas correctivas necesarias en consulta con el DPC y, cuando corresponda, el DPO del Grupo.
    - Proporcionar informes sobre el cumplimiento por parte de la Actividad de la Ley de Protección de Datos y la Política aplicables a la Gerencia (i) de forma regular (al menos una vez al año), (ii) en caso de que se produzcan desarrollos importantes, y (iii) si se solicita.
    - Notificarse al DPC, quien se encargará de su seguimiento.
- El **DPC** será responsable de gestionar las actividades de cumplimiento de la protección de datos en la entidad y de asistir a las demás funciones en sus obligaciones de cumplimiento de la protección de datos. Deberá:
    - Tener un conocimiento detallado de la Ley de Protección de Datos aplicable y de los requisitos de la Política.
    - Ser independiente, es decir, no tener ningún interés en las actividades de procesamiento de datos personales de la entidad.
    - A menos que se establezca lo contrario, gestionar los procesos de protección de datos y otras actividades de cumplimiento de la protección de datos de la entidad y llevar a cabo las tareas de DPC previstas en la Política de conformidad con esta.
    - Asesorar y apoyar a los DAO y a la Gerencia en lo que respecta a su responsabilidad de cumplir la Ley de Protección de Datos aplicable y la Política.
    - Supervisar el cumplimiento por parte de los DAO de la Ley de Protección de Datos aplicable y de la Política.
    - Consultar al DPO del Grupo sobre cualquier cuestión importante relativa al cumplimiento por parte de la entidad de la Ley de Protección de Datos aplicable o de la Política, o en caso de duda.
    - Proporcionar informes sobre el cumplimiento por parte de la entidad de la Ley de Protección de Datos y la Política a la Gerencia, a la Junta Directiva y al DPO del Grupo (i) de forma regular (al menos una vez al año), (ii) en caso de que se produzcan desarrollos importantes, y (iii) si se solicita.
    - No tener ni asumir ningún poder de decisión (incluido el derecho de veto o a interferir) con respecto a cualquier procesamiento específico u otra actividad de cumplimiento de la protección de datos de la entidad; en caso de incumplimiento presunto o real, se informará de ello a la Gerencia (y al DPO del Grupo), que tomará la decisión o medida correctiva necesaria (el DPO del Grupo solicitará dicha decisión o medida a la Gerencia del Grupo); y
    - En caso de que el DPC también haya sido designado formalmente como Funcionario de Protección de Datos de conformidad con el art. 38 del GDPR, desempeñará todas las funciones de un DPO en virtud del art. 39 del GDPR en la medida en que estas tareas no estén ya cubiertas por las anteriores.

Lo siguiente se aplica a **nivel del Grupo**:

- La **Junta Directiva del Grupo** y sus miembros (que no actúan en calidad de funcionarios de una entidad específica del Grupo) establece el marco general para garantizar el cumplimiento de la protección de datos aplicable (incluso mediante la publicación de esta Política). Ellos:
    - Tendrán un conocimiento básico de la Ley de Protección de Datos aplicable.
    - Tendrán derecho a emitir políticas vinculantes para todo el Grupo en relación con el procesamiento de datos personales y el cumplimiento de la Ley de Protección de Datos aplicable.
    - Por la presente, exigen a la Gerencia del Grupo que implemente la Política a nivel de Grupo para garantizar el cumplimiento por

parte del Grupo de la Ley de Protección de Datos aplicable y de la Política.

- Estudiarán los informes de cumplimiento proporcionados, investigarán los indicios de incumplimiento y tomarán las medidas correctivas necesarias en consulta con el DPO del Grupo y la Gerencia del Grupo.
- No asumirán, salvo lo dispuesto anteriormente, ningún poder de decisión con respecto a ningún procesamiento específico de datos personales u otra actividad específica de cumplimiento de la protección de datos de una entidad específica del Grupo (a menos que actúe en calidad de Junta Directiva de dicha entidad).

- La **Gerencia del Grupo**, en particular el **director ejecutivo (CEO) del Grupo**, tiene la responsabilidad operativa del cumplimiento por parte del Grupo de la Ley de Protección de Datos aplicable y de la Política. Deberá:
  - Tener un conocimiento básico de la Ley de Protección de Datos aplicable y de los requisitos de la Política.
  - Emitir las instrucciones necesarias para que se implemente la Política y se cumpla en el Grupo, lo que incluye (i) la designación de las funciones necesarias del Grupo (incluidas las previstas en este Anexo), y (ii) el establecimiento de los procesos necesarios del Grupo para el cumplimiento de la Política.
  - Garantizar el cumplimiento de la Ley de Protección de Datos aplicable en el Grupo, además de las disposiciones de la Política.
  - Garantizar que, cuando se deleguen tareas a nivel del Grupo, los delegados sean debidamente seleccionados, instruidos y supervisados por la Gerencia del Grupo.
  - Estudiar los informes de cumplimiento proporcionados, investigar los indicios de incumplimiento y tomar las medidas correctivas necesarias en consulta con el DPO del Grupo.
  - Proporcionar informes sobre el cumplimiento por parte del Grupo de la Ley de Protección de Datos y la Política aplicables a la Junta Directiva del Grupo (i) de forma regular (al menos una vez al año), (ii) en caso de que se produzcan desarrollos importantes, y (iii) si se solicita.
- El **Funcionario de Protección de Datos del Grupo** (**DPO del Grupo**) será responsable de gestionar las actividades de cumplimiento de la protección de datos en el Grupo y de asistir a las demás funciones en sus obligaciones de cumplimiento de la protección de datos. Deberá:
  - Tener un conocimiento detallado de la Ley de Protección de Datos aplicable y de los requisitos de la Política.
  - Ser independiente, es decir, no tener ningún interés en las actividades de procesamiento de datos personales del Grupo.
  - Gestionar los procesos de protección de datos y otras actividades de cumplimiento de la protección de datos del Grupo y llevar a cabo las tareas de DPO previstas en la Política de conformidad con esta.
  - Asesorar y apoyar a los DPC, los DAO, la Gerencia de las entidades del Grupo y a la Gerencia del Grupo en lo que respecta a su responsabilidad de cumplir la Ley de Protección de Datos aplicable y la Política.
  - Supervisar el cumplimiento por parte de los DAO de la Ley de Protección de Datos aplicable y de la Política en casos que son importantes para el Grupo.
  - Proporcionar informes sobre el cumplimiento por parte del Grupo de la Ley de Protección de Datos y la Política aplicables a la Gerencia del Grupo y a la Junta Directiva del Grupo (i) de forma regular (al menos una vez al año), (ii) en caso de que se produzcan desarrollos importantes, y (iii) si se solicita;
  - No tendrá ni asumirá ningún poder de decisión (incluido el derecho de veto o a interferir) con respecto a cualquier procesamiento específico u otra actividad de cumplimiento de la protección de datos de una entidad del Grupo; en caso de incumplimiento presunto o real, se informará de ello a la Gerencia del Grupo o a la Gerencia de la entidad, que tomará la decisión o medida correctiva necesaria.

Además de lo anterior, las funciones de **auditoría interna** verificarán de forma independiente el cumplimiento por parte del Grupo de las Leyes de Protección de Datos aplicables y de la Política, y presentarán los informes correspondientes a las funciones relevantes de la gerencia y la junta del Grupo. Todas las funciones cooperarán con la auditoría interna.