Directiva

relativa a la transferencia de datos personales

a países terceros fuera del EEE

(Directiva del Grupo de Reaseguro Münchener Rück para la transferencia de datos a países terceros)

Fecha: 1 de Enero 2021

Contenido

1. Introducción

La tecnología moderna de la información y comunicación da lugar a cambios tecnológicos y económicos cuyas dimensiones y consecuencias empiezan a perfilarse paulatinamente y son comparables a la transformación de la sociedad agraria a la sociedad industrial. El acceso a Internet e informaciones vía WorldWideWeb (WWW), la utilización de sistemas electrónicos de correo y noticias así como el diálogo e intercambio de informaciones a nivel mundial: todas estas facilidades se consideran hoy en día instrumentos decisivos e imprescindibles para ejercer cualquier actividad económica y actuar con éxito en el mercado, así como para poder reaccionar con rapidez y flexibilidad ante nuevas influencias y ampliar los servicios tanto a nivel interior como exterior.

Sin embargo, la comunicación electrónica conlleva ventajas que, al mismo tiempo, la hacen vulnerable. Dada la infinidad de posibilidades en el tratamiento de datos, existe el riesgo de que los datos puedan ser manipulados sin autorización; la transferencia de datos personales a través de redes públicas hace posible que los datos sean revelados sin que las personas interesadas lo sepan; un sistema de computadoras que es accesible desde redes internacionales también está expuesto a manipulaciones intencionadas desde estas redes. El intercambio mundial de datos nos ofrece oportunidades que no deben verse amenazadas por ninguna violación de los derechos de personalidad y propiedad intelectual o por cualquier revelación de secretos comerciales.

Por esta razón, la planificación e implantación de nuevos sistemas de tecnología de la información (TI) deben ir acompañadas por la revisión y posiblemente adaptación de las medidas de seguridad existentes. Este requisito se debe, por un lado, al interés de la compañía de evitar en lo posible que se produzca un daño de gran envergadura. Por otro lado, es necesario cumplir las regulaciones legales, especialmente aquellas que protegen al consumidor, tales como la Directiva de la UE en materia de Protección de Datos y sus requisitos a nivel europeo y la Ley Federal alemana en materia de Protección de Datos (“Bundesdatenschutzgesetz” – BDSG) o leyes equiparables a nivel nacional. Bajo el amparo de esta legislación se han de tomar medidas técnicas y organizativas en protección de los datos de los clientes, clientes prospectivos y de los empleados, a fin de evitar repercusiones negativas en los derechos de la personalidad. Sin embargo, la protección de los derechos de la personalidad también implica, entre otras cosas, asumir los intereses de los clientes en cuanto a la protección de datos. Para una compañía que opera a nivel internacional como el Grupo de Reaseguro Münchener Rück, ello constituye una elemento esencial de su política empresarial. Para asegurar, independientemente de las regulaciones legales existentes, un nivel de protección de datos uniforme a escala mundial dentro del Grupo de Reaseguro Münchener Rück, la Münchener Rückversicherungs-Gesellschaft Aktiengesellschaft in München y/o las compañías del Grupo de Reaseguro Münchener Rück, han asumido el compromiso de cumplir los siguientes criterios:

2. Objetivo de la Directiva

La presente Directiva tiene por objetivo establecer estándares uniformes en materia de protección y seguridad de datos –de conformidad con la Directiva de la UE relativa a la Protección de Datos– para el tratamiento de datos dentro del Grupo de Reaseguro Münchener Rück en lo que respecta a la transferencia de datos de compañías del Grupo de Reaseguro Münchener Rück de los Estados miembros del EEE (véase Anexo 3 de la Directiva) a países terceros y, así, garantizar a las mismas un nivel de protección adecuado así como suficientes

garantías para la protección del derecho a la intimidad personal y el ejercicio de los correspondientes derechos.

3. Ámbito de aplicación de la Directiva

La presente Directiva viene a ser un conjunto de líneas directrices aplicables tanto a la transferencia como al consiguiente tratamiento de los datos personales correspondientes a empleados, clientes (afiliados a fondos del seguro de salud de la empresa, tomadores de préstamo, titulares de cuentas bancarias, tomadores de crédito, inquilinos, tomadores de seguro), intermediarios y otras personas interesadas, especialmente en relación con la ejecución de un contrato y la liquidación de siniestros (demandantes, accionistas, titulares de préstamo y ahorro para viviendas, cotizantes, beneficiarios, damnificados, suministradores y sus clientes, clientes potenciales, peritos, personas aseguradas, testigos), por compañías del Grupo de Reaseguro Münchener Rück, independientemente de la base jurídica para la transferencia de datos[1].

Las regulaciones de esta Directiva son vinculantes para todas las compañías del Grupo de Reaseguro Münchener Rück. Compañías no pertenecientes al Grupo de Reaseguro Münchener Rück también pueden comprometerse a cumplir las regulaciones de forma voluntaria y sobre una base legalmente vinculante; en caso contrario, no están sujetos a la presente Directiva. En tal caso, se estudiará en cada uno de los supuestos la admisibilidad de la transferencia de datos, adoptando las correspondientes medidas para garantizar la misma si fuera necesario. En el caso de que fuera revocada la declaración de compromiso, las obligaciones asumidas en virtud de la presente Directiva continuarán siendo vigentes para cualquier tratamiento de datos personales llevado a cabo hasta la fecha de la revocación.

La presente Directiva se aplica a la transferencia así como al subsiguiente tratamiento y utilización de los datos personales por compañías del Grupo de Reaseguro Münchener Rück del EEE a aquellas en países terceros.

Las obligaciones legales existentes no se ven afectadas por esta Directiva. Si, en países terceros, tales obligaciones fueran contradictorias a las obligaciones resultantes de esta Directiva, se le informará de la forma correspondiente a la compañía transmitente del Grupo de Reaseguro Münchener Rück en el EEE, incluso si tales obligaciones surgieran posteriormente.

4. Definiciones

A efectos de la presente Directiva se entiende por:

- **Datos personales**: toda información sobre una persona física identificada o identificable (el “interesado”). Se considera identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, por ejemplo, mediante un número de identificación.

- **Transferencia de datos personales**: comunicación de los datos personales, su difusión o cualquier otra forma que facilite el acceso a los mismos a terceros.

[1] Además del cumplimiento de las regulaciones de la presente Directiva, también se requiere una base legal para la transmisión de datos.

- **Tratamiento de datos personales**: cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales, como la recogida, registro, conservación, elaboración, modificación, extracción, consulta, utilización, comunicación por transmisión así como bloqueo, supresión o destrucción.

- **Responsable del tratamiento de datos** (autoridad de control): en relación con terceros es la compañía legalmente independiente del Grupo de Reaseguro Münchener Rück cuya actividad comercial ha motivado la transmisión de datos. Las sucursales dependientes forman una parte de la autoridad de control.

- **Encargado del tratamiento de datos**: la persona física o jurídica que trata datos personales por cuenta del responsable del tratamiento.

- **Tercero**: la persona física o jurídica distinta del responsable del tratamiento.

- **Consentimiento**: toda manifestación de voluntad libre, específica e informada, mediante la cual el interesado consiente el tratamiento de los datos personales que le conciernen[2].

- **Clientes**: personas físicas con las cuales se mantiene o se tiene previsto mantener una relación comercial.

- **Intermediario**: personas físicas que se dedican profesionalmente a la intermediación de productos de seguros y/o productos de servicios financieros.

- **País tercero**: cualquier país fuera de la Unión Europea/del EEE.

- **Delegación de funciones**: ello se refiere, en particular, cuando se transfiere a largo plazo por completo o una parte esencial de la distribución, gestión de cartera, evaluación de crédito, tramitación de prestaciones, contabilidad, inversiones o gestión de activos de una compañía del Grupo de Reaseguro a otra compañía del Grupo de Reaseguro.

5. Admisibilidad del tratamiento de datos

Solamente se permite el tratamiento de datos mencionado en la cifra 3 si se reúnen los siguientes criterios generales de admisibilidad:

- consentimiento,
- permisibilidad u
- otras disposiciones legales

Ello constituye un prerrequisito para cualquier exportación de datos. Básicamente, las regulaciones generales también son aplicables al tratamiento de datos por cuenta de una autoridad de control y a la delegación de funciones. Tales regulaciones se derivan de la legislación nacional del Estado del EEE, en el cual la autoridad de control tiene fijada su sede.

[2] La respectiva legislación nacional puede tener previsto el cumplimiento de requisitos particulares para el consentimiento.

6. Principios aplicables a la transferencia y al subsiguiente tratamiento y uso de los datos personales

6.1 Finalidad

La recogida y el tratamiento de datos personales deben tener una finalidad determinada, explícita y legítima. Las compañías del Grupo de Reaseguro o compañías en países terceros que asumieron voluntariamente el compromiso de cumplir las regulaciones de esta Directiva están obligadas a observar esta finalidad de los datos transmitidos, tanto en lo que se refiere a su registro como utilización posterior. Solamente se permite alterar la finalidad tras previo consentimiento por parte de la persona interesada o si lo permite la respectiva ley nacional del país exportador de datos.

6.2. Calidad de los datos

Los datos personales tienen que ser exactos y, cuando sea necesario, deben ser actualizados. Se han de tomar medidas razonables para que los datos inexactos o incompletos sean suprimidos o rectificados. Los datos han de ser requeridos para la finalidad en cuestión.

6.3 Transparencia

Las personas físicas cuyos datos personales son transmitidos de una compañía del Grupo de Reaseguro en un país del EEE a una compañía del Grupo de Reaseguro en un país tercero, deben obtener las siguientes informaciones:

- identidad de la autoridad de control en el país tercero
- finalidad de la transferencia
- otras informaciones si fuese necesario por razones equitativas, p.ej.,
  - derechos de acceso, rectificación y supresión
  - derecho de oposición en el caso de publicidad

El deber de información se puede omitir si

- es necesario por motivos de protección
  - de las persona interesada o
  - de los derechos y obligaciones de otras personas;
- la persona interesada ya está informada;
- implica esfuerzos desproporcionados;
- los datos son accesibles al público y las informaciones desproporcionadas debido al elevado número de casos afectados.

6.4 Seguridad

Las autoridades de control han de adoptar las medidas técnicas y organizativas apropiadas a fin de garantizar el nivel de seguridad requerido para la proteccion de datos. Las medidas se refieren, en particular, a computadoras (servidores y estaciones de trabajo), redes o enlaces de comunicación así como a aplicaciones. En el **Anexo 1** se encuentra un catálogo de medidas.

6.5 Confidencialidad del tratamiento

Solamente tienen derecho a recabar, procesar o utilizar datos personales las personas autorizadas y los empleados especialmente obligados a guardar el secreto de los datos. Queda prohibido utilizar tales datos para fines privados, así como transmitirlos o hacerlos accesibles de cualquier otra forma a personas no autorizadas. En este sentido, los empleados, por ejemplo, también han de considerarse personas no autorizadas, salvo que sus responsabilidades y actividades concretas requieran lo contrario. En el **Anexo 2** se encuentra la muestra de una declaración de confidencialidad.

La obligación de confidencialidad incluso sigue vigente tras haber finalizado la relación laboral.

6.6 Tratamiento de datos por cuenta de otras autoridades

Si las compañías del Grupo de Reaseguro, o las compañías que se comprometieron voluntariamente a observar las regulaciones de esta Directiva, actúan como contratante o contratado bajo un contrato de encargo respecto al tratamiento de datos personales, serán de aplicación las siguientes disposiciones:

- Se debe elegir a un contratante que tome todas las medidas técnicas y organizativas necesarias para garantizar la seguridad del tratamiento.
- La ejecución del tratamiento de datos por cuenta de otra autoridad debe ser regularizada en un contrato por escrito o documentado de cualquier otro modo, en el cual figuran establecidos los derechos y obligaciones del contratado.
- La parte contratada debe estar contractualmente obligada a que los datos recibidos del contratante solamente sean procesados dentro de los márgenes establecidos en el contrato de encargo y según las instrucciones facilitadas por el contratante. Queda excluido por contrato cualquier tratamiento para fines propios o para fines de terceros.
- El parte contratante sigue siendo la persona de contacto para los clientes, empleados, etc.

7. Derechos de la persona interesada

El cliente, empleado, intermediario o cualquier otra persona interesada (véase cifra 3), disfruta determinados derechos inalienables respecto a sus datos personales:

- Derecho de **informarse** (en caso dado incluso por escrito[3]) sobre los datos registrados acerca de su persona, así como sobre la fuente y la finalidad de tales datos.

- Derecho de **informarse** sobre los receptores o categorías de receptores en el caso de una transferencia de sus datos personales.

- El derecho de informarse queda descartado si implica la revelación de secretos comerciales.

- Derecho de **rectificación** si se constata que los datos personales son incorrectos o incompletos.

[3] La información siempre se facilita por escrito.

- Derecho al **bloqueo** si no se puede comprobar ni la exactitud ni inexactitud de los datos personales.

- Derecho a **supresión** si el tratamiento de datos fue inadmisible o cuando ya no se requieren los datos para los fines que motivaron su tratamiento. En el caso de existir obligación legal de conservación, los datos no son eliminados sino bloqueados.

- Derecho a oposición si la utilización de sus datos se debe
  - a fines publicitarios o
  - a fines de estudios de mercado y sondeo de la opinión pública.
  - Asimismo, tiene derecho general a oposición, el cual se debe tener en cuenta siempre y cuando una evaluación revele un interés de la persona interesada que sea digno de protección y que prevalezca sobre el interés de la autoridad de control debido a la situación específica individual de la persona interesada.

La persona interesada también puede ejercer los derechos que le corresponden en virtud de la presenta Directiva frente a la autoridad transmitente.

8. Revelación de datos

8.1 Transferencia de datos del EEE a otros países

Solamente se permite transmitir datos personales de un Estado miembro del EEE a un Estado no perteneciente al EEE, en consideración de lo previsto en la cifra 5,

- si el interesado ha dado su consentimiento de forma inequívoca; o
- si la transferencia es necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la aplicación de medidas precontractuales adoptadas a petición del interesado; o
- si la transferencia es necesaria para la formalización o cumplimiento de un contrato concluido o a concluir en interés del interesado entre el responsable del tratamiento y un tercero; o
- si la transferencia es necesaria o legalmente prescrita para salvaguardar un interés público importante o para hacer valer, ejercer o defender derechos legales ante los tribunales; o
- si la transferencia es necesaria para proteger el interés vital del interesado; o
- si el país receptor/autoridad receptora garantiza un adecuado nivel de protección de datos para los fines de esta Directiva[4]. Si el receptor de los datos es una compañía que está sujeta a la presente Directiva, no es necesario verificar si tal nivel de protección es adecuado; o [5]si el responsable del tratamiento ofrece suficientes garantías de protección respecto al derecho de la personalidad o ejercicio de los respectivos derechos. Si el receptor de los datos es una compañía que ha de cumplir con lo establecido en la presente Directiva, dichas garantías se derivan de la Directiva[6].

[4] Ello es competencia de la Comisión Europea.
[5] No obstante, un prerrequisito adicional para la transferencia es una base legal.
[6] Sin embargo, un prerrequisito adicional para la transferencia es una base legal.

8.2 Revelación de datos transferidos a un país tercero dentro de este país tercero o a otro país tercero

De conformidad con lo establecido en la cifra 5), solamente se permite la comunicación de datos personales transferidos a una autoridad dentro de este país tercero o a otro país tercero si este país tercero/autoridad receptora ofrece un adecuado nivel de protección de datos o cuando se cumple una de las condiciones mencionadas en el punto 8.1 [7]. Siempre y cuando se trate de una compañía del Grupo de Reaseguro que se haya comprometido a observar esta Directiva, no es necesario verificar tal nivel de protección; de lo contrario hay que asegurarse –salvo que se haya cumplido una de las condiciones mencionadas en el punto 8.1– que el nivel de protección de datos es adecuado, obligando al receptor, si fuese necesario, a cumplir con los principios de esta Directiva. En todo caso, ello tiene que ser puesto en conocimiento de la compañía del Grupo de Reaseguro Münchener Rück en el EEE, la cual ha transmitido los datos.

9. Categorías especiales de datos personales

Generalmente se prohíben la transferencia así como el subsiguiente tratamiento y uso de determinados tipos de datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como datos personales relativos a la salud o a la sexualidad. No obstante, ello no se aplicará si el interesado ha dado su consentimiento explícito a tal tratamiento, salvo en los casos en los que

- el interesado está incapacitado para dar su consentimiento;
- o el tratamento se refiere a datos que el interesado haya hecho manifiestamente públicos;
- o si la transferencia así como subsiguiente tratamiento y uso se refieren a datos que son necesarios para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial (¡ponderación de intereses!).

Ello también se aplica a los datos recogidos en el país tercero.

10. Márketing directo/estudio de mercados y de la opinión pública

Si los datos personales son procesados o utilizados para fines de márketing directo/estudios de mercados y de la opinión pública, el interesado tiene el derecho de oponerse en cualquier momento a la utilización de sus datos[8]. En este caso, los datos deben ser bloqueados para tal propósito.

11. Decisiones individuales automatizadas

Si los datos personales son transferidos y, en caso dado, procesados con el objetivo de tomar una decisión individual automatizada, los intereses legítimos del interesado deben ser protegidos mediante medidas apropiadas. Las decisiones que conllevan consecuencias legales negativas para el cliente o le afectan de forma significativa, no deben basarse únicamente en una decisión individual automatizada que sirva para evaluar determinados

[7] Sin embargo, un prerrequisito adicional para la transferencia es una base legal.
[8] En tanto que esté previsto en la legislación nacional, el interesado debe ser informado sobre su derecho de interponer recurso de oposición y sobre la autoridad de control.

aspectos personales. Solamente se permiten excepciones si los intereses del interesado son protegidos mediante informaciones sobre la lógica de la decisión y la posibilidad de dar comentarios al respecto. En el caso de que el interesado diera sus comentarios, la autoridad de control está obligada a verificar su decisión.

12. Cuestiones relativas al procedimiento

12.1 Implantación a nivel empresarial

Una vez que se hayan comprometido a observar los principios arriba mencionados, las compañías del Grupo de Reaseguro Münchener Rück, como receptores competentes, han de garantizar que estos principios sean respetados en las relaciones con terceros (p.ej. clientes, intermediarios, etc.).

Para ello es necesario que los cargos directivos de cada compañía garanticen la puesta en marcha de esta Directiva, facilitando sobre todo las correspondientes instrucciones a los empleados. En el caso de considerar conveniente cualquier cursillo de formación o adiestramiento, se ponen en contacto con el Encargado de Protección de Datos del Grupo de Reaseguro Münchener Rück[9]. En las instrucciones facilitadas cabe mencionar, entre otras cosas, que cualquier infracción de estos principios puede traer consigo consecuencias penales, jurídico-laborales y de responsabilidad civil.

12.2 Preguntas y quejas

En el caso de preguntas y quejas, los interesados pueden dirigirse en todo momento al Encargado de la Protección de Datos del Grupo de Reaseguro Münchener Rück[10] o al representante local y/o la autoridad de supervisión correspondiente. Los receptores en países terceros y el Encargado de la Protección de Datos del Grupo de Reaseguro Münchener Rück[11] en la UE están obligados a cooperar con la autoridad de supervisión del Estado en el cual la autoridad transmitente tiene su sede, y a respetar sus declaraciones respecto a las consultas de esta autoridad. Asimismo, la autoridad transmitente en la UE/EEE tiene el derecho de verificar, en la autoridad receptora, el tratamiento de datos en casos individuales. Esta autoridad impondrá los derechos determinados, apoyando a los interesados que hayan sufrido un daño debido al incumplimiento de la obligación resultante de esta Directiva, a la hora de hacer valer sus derechos frente a la autoridad de control en el país tercero.

Los interesados pueden ejercer gratuitamente sus derechos en los procesos extrajudiciales.

13. Publicidad

Esta Directiva empresarial se pondrá a disposición de los interesados de la forma conveniente, p.ej., a través de internet.

---

[9] Rogamos dirigirse al Coordinador Regional de Protección de Datos o al Encargado de Protección de Datos de la Münchener Rückversicherungs-Gesellschaft Aktiengesellschaft in München.
[10] El Encargado de Protección de Datos de la Münchener Rückversicherungs-Gesellschaft Aktiengesellschaft en München.
[11] El Encargado de Protección de Datos de la Münchener Rückversicherungs-Gesellschaft Aktiengesellschaft en München.

14. Encargado de la Protección de Datos en el Grupo de Reaseguro Münchener Rück

Se nombrará a un Encargado de la Protección de Datos del Grupo de Reaseguro Münchener Rück[12], el cual colaborará con el auditor del Grupo o los auditores de la respectiva compañía del Grupo de Reaseguro Münchener Rück con el objetivo de supervisar el cumplimiento de las normas nacionales[13] e internaciones en materia de protección de datos así como las normas establecidas en esta Directiva. En este contexto, el Encargado recibe el apoyo de los representantes locales[14] quienes, en nombre de él y actuando como autoridad de control, son responsables de garantizar la protección de datos en la correspondiente compañía y de informarle sobre las quejas; los representantes locales han de respetar las declaraciones del Encargado y son apoyados por los respectivos cargos directivos en el desempeño de sus actividades.

Todos los empleados pueden dirigirse en cualquier momento al Encargado de la Protección de Datos del Grupo de Reaseguro Münchener Rück[15] con sus preguntas, sugerencias y quejas, las cuales siempre serán tratadas de forma confidencial.

El Encargado de la Protección de Datos en el Grupo de Reaseguro[16] es actualmente el Dr. Wolfgang Mörlein, al cual se le puede contactar bajo la siguiente dirección electrónica: datenschutz@munichre.com

[12] El Encargado de Protección de Datos de la Münchener Rückversicherungs-Gesellschaft Aktiengesellschaft en München.
[13] Las regulaciones nacionales en materia de Protección de Datos son revisadas por la propias compañías nacionales.
[14] Coordinadores Regionales de Protección de Datos
[15] El Encargado de Protección de Datos de la Münchener Rückversicherungs-Gesellschaft Aktiengesellschaft en München.
[16] El Encargado de Protección de Datos de la Münchener Rückversicherungs-Gesellschaft Aktiengesellschaft en München.

Anexo 1
relativo a la Directiva del Grupo de Reaseguro Münchener Rück para la transferencia de datos a países terceros

Si los datos personales son procesados **o utilizados** de forma automatizada, **la organización interna debe diseñarse de tal forma que cumpla las exigencias especiales de la protección de datos. Para ello es particularmente** necesario adoptar medidas adecuadas en función del tipo de datos personales **o categorías de datos** a proteger, a fin de

1. denegar a personas no autorizadas el **acceso** a equipos de procesamiento de datos utilizados para el tratamiento **o utilización** de datos personales **(control de acceso)**;
2. impedir a personas no autorizadas el uso de sistemas de procesamiento de datos **(control de acceso)**;
3. garantizar que las personas autorizadas para utilizar un sistema de procesamiento de datos solamente puedan tener acceso a los datos que les corresponden y **que los datos personales no se puedan leer, copiar, modificar o retirar sin autorización durante el tratamiento y utilización de los mismos así como después de su registro** (control de acceso);
4. **garantizar** que los datos personales **no puedan ser leídos, copiados**, modificados o **eliminados sin autorización** durante su **transferencia electrónica** o su transporte o su **registro en los soportes de datos; y con el objetivo de poder verificar y establecer a qué autoridades u organismos tienen previsto transferir los datos personales las instituciones de transmisión de datos (control de transferencia)**;
5. garantizar que se pueda comprobar y establecer con posterioridad **si y por quién** se han introducido, **modificado o eliminado** datos personales en los sistemas de procesamiento (control de introducción de datos);
6. garantizar que el tratamiento de datos personales por cuenta de otra autoridad solamente se realice de acuerdo con las instrucciones de la parte contratante (control del encargo);
7. **garantizar que los datos personales estén protegidos contra destrucción fortuita o pérdida accidental (control de disponibilidad)**;
8. **garantizar el tratamiento separado de los datos recogidos para diferentes fines.**

Anexo 2
relativo a la Directiva del Grupo de Reaseguro Münchener Rück
para la transferencia de datos a países terceros

Declaración de confidencialidad

Sr. D./Sra. Dña.
.....
(nombre, número de personal)

se obliga por la presenta a guardar el secreto de datos.

Se le advierte al empleado que está prohibido procesar o utilizar ilícitamente datos personales protegidos para cualquier otra finalidad que no corresponda al cumplimiento legítimo de las respectivas tareas y que estas obligaciones persisten incluso después de haber concluido la actividad.

La obligación incluye los siguientes puntos:

- Los datos y programas solamente se pueden almacenar, procesar o imprimir de la manera que lo hayan ordenado las autoridades responsables de tomar decisiones.
- No está permitido reproducir datos, programas y otras informaciones para cualquier otro fin que no sea comercial.
- Queda prohibido falsificar datos o programas, producir datos o programas falsos, así como utilizar intencionadamente datos y programas falsos o falsificados.
- Solamente se pueden recurrir a datos necesarios para el cumplimiento de una tarea específica.
- Solamente se permite la revelación de datos personales a terceros si el receptor tiene derecho de acceso a los mismos en virtud de lo establecido legalmente.
- Los documentos que contengan datos personales deben estar guardados de tal forma que estén protegidos contra el acceso de terceros.

Son de cumplimiento obligatorio las normas vigentes en materia de gestión y protección de datos (p.ej. respecto a la protección de contraseñas). Por motivos de seguridad, los datos personales deben ser gestionados con la debida diligencia dentro del marco de la tarea asignada; cualquier deficiencia detectada debe ser notificada.

Se le informa al empleado que la violación del secreto de datos puede ser sancionada con condena de prisión o una multa conforme a lo establecido en las correspondientes disposiciones legales. En la mayoría de los casos, cualquier violación del secreto de datos supone al mismo tiempo una infracción del secreto profesional, de modo que ello conllevará medidas contempladas en la ley laboral, incluyendo el despido sin preaviso.

En señal de recibo y conformidad con lo establecido en la presente declaración de confidencialidad, rogamos se sirva remitir una copia firmada al Encargado de la Protección de Datos. (La copia remitida será archivada en el expediente personal del empleado.)

....
(Fecha) (Firma del empleado)

Anexo 3
relativo a la Directiva del Grupo de Reaseguro Münchener Rück para la transferencia de datos a países terceros

El Espacio Económico Europeo (EEE) está integrado por Estados miembros de UE y de Estados pertenecientes a la Asociación Europea de Libre Comercio (AELC), a excepción de Suiza.

Por lo tanto, los países que forman parte del EEE son:

Bélgica, Alemania, Dinamarca, Estonia, Finlandia, Francia, Grecia, Irlanda, Italia, Letonia, Lituania, Luxemburgo, Malta, Países Bajos, Austria, Polonia, Portugal, Bulgaria, Suecia, Eslovaquia, Eslovenia, España, República Checa, Croacia, Hungría, Rumanía, Chipre (zona griega) - países miembros de la UE

Estados miembros de la AELC: Islandia, Liechtenstein, Noruega