Política de privacidad General UE

Grupo Bondioli & Pavesi

Índice

1. INTRODUCCIÓN

El Grupo Bondioli & Pavesi da mucha importancia al respeto de la privacidad y de las normativas en materia de protección de datos personales con el objetivo de un desarrollo correcto de sus operaciones, sus negocios y de su imagen en el mercado. La protección de los datos personales que cada sociedad del grupo recoge y archiva, con sistemas electrónicos o modalidades tradicionales, es un valor importante y estratégico para el grupo y el desarrollo de los negocios.

En este sentido el Reglamento (UE) 2016/679 (a continuación también **«GDPR»**) representa el eje de la nueva normativa europea en materia de protección de los datos personales y es el punto de referencia principal para las actividades que implican datos personales en el ámbito UE.

Por lo tanto es fundamental valerse de una Política de Privacidad común (a continuación **«Política de Privacidad»**) para las sociedades ubicadas en la UE e indicadas en el punto 3 (a continuación, cada una se indica como **«Sociedad»** y en general **«Grupo UE»**), y poner en conocimiento los principios y las reglas que el Grupo UE respetará, tanto en el caso de empleados como de los que operen en nombre y por cuenta de cada Sociedad, de manera que se garantice un nivel de protección de la información personal uniforme y elevado.

A raíz, por un lado, de la complejidad de la normativa y, por otro, de los procedimientos empresariales que involucran los datos personales, es necesario valerse previamente de una estructura de gobernanza de la privacidad en el ámbito de las Sociedades del Grupo UE mediante la definición de la configuración de los roles, las responsabilidades y las tareas pertenecientes a la protección de los datos personales.

2. FINALIDAD

Esta Política de privacidad quiere describir:

(i). los principios y las modalidades que cada Sociedad debe respetar durante las actividades de tratamiento de los datos personales,
(ii). la organización de la privacidad para gestionar la gobernanza de la materia, y
(iii). la asignación de tareas y responsabilidades de los diferentes niveles operativos.

Por lo tanto, todas las personas que realizan tratamientos de datos personales en las Sociedades deben conocer esta Política de privacidad.

3. ÁMBITO DE COMPETENCIA

Las siguientes Sociedades deben respetar esta Política de privacidad:

- todas las sociedades italianas que forman parte del grupo Bondioli & Pavesi;
- Bondioli & Pavesi GMBH;
- Bondioli & Pavesi France SA;

- Bondioli & Pavesi Iberica SA;
- Bondioli & Pavesi Sp. Zo.o.;
- OM Protivin AS.

Cada sociedad, además de conformarse a esta política de privacidad, debe claramente respetar el GDPR y las normativas locales adicionales en materia de privacidad y protección de los datos personales.

4. DEFINICIONES

A efectos de esta política de privacidad se proporcionan las siguientes definiciones provenientes del GDPR en orden de importancia:

- **Dato personal**: toda información sobre una persona física identificada o identificable (**«Interesado»**). Es identificable la persona física que puede identificarse directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona. Además, en caso de actividades de marketing que el destinatario no solicita (por ejemplo: envío espontáneo de publicidad, venta directa, estudios de mercado o de comunicación comercial) y también toda información relativa a una persona jurídica, incluidos los entes y las asociaciones.
  Por ejemplo: datos de registro, direcciones de correo electrónico, telefónicas, telemáticas, códigos identificativos, pedidos, facturación, imagen, voz, currículo, hábitos de compra, acceso a los sistemas y, más en general, todo lo que se registre en los soportes de papel o informáticos y que pueda relacionarse con un interesado identificado o identificable.

- **Tratamiento**: Toda operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procesos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción, bloqueo.
  Por ejemplo: gestión de las nóminas y de las presencias de los empleados, gestión de los contratos, envío de comunicaciones de marketing, elaboración de perfiles, videovigilancia etc.

- **Categorías especiales de datos personales:** datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la afiliación sindical o los datos relativos a la vida o a la orientación sexual, además de los datos genéticos o biométricos dirigidos a identificar de manera unívoca una persona física. Son un subconjunto de datos personales.
  Por ejemplo: certificados de baja, afiliación al sindicado, permisos sindicales, discapacidades, accidentes, afiliación a un partido, salud etc.

- **Datos personales relativos a condenas penales y delitos:** (a continuación **«datos penales»**) datos personales relativos a las condenas penales y a los delitos o a las medidas de seguridad conexas. Es un subconjunto de datos personales.

- **Responsable del tratamiento**: la persona física o jurídica, la autoridad pública, el servicio u otro órgano que, individualmente o con otros, establece los fines y los medios del tratamiento de los datos personales.
  Por ejemplo, si Bondioli & Pavesi S.p.A. gestiona por entero el sitio web, los tratamientos de datos que le conciernen estarán a cargo de la sociedad en calidad de responsable.
  Cada Sociedad será responsable cuando elija cómo realizar el tratamiento en autonomía. Por ejemplo, los tratamientos de datos de los empleados prevén que la titularidad del tratamiento le corresponda a cada Sociedad.

- **Encargado del tratamiento:** la persona física o jurídica, la autoridad pública, el servicio u otro órgano que trata datos personales por cuenta del responsable del tratamiento, de conformidad con el art. 28 del GDPR.

- **Persona Autorizada para el tratamiento:** (también «Procesador») la persona física que trata datos personales bajo la autoridad directa del responsable o del encargado;

- **Interesado.** La persona física identificada o identificable a la que se refieren los datos personales. Además, en caso de actividades de marketing que el destinatario no solicita (por ejemplo: envío espontáneo de publicidad, venta directa, estudios de mercado o de comunicación comercial), el interesado es también la persona jurídica, incluidos los entes o las asociaciones, como indicado en la Directiva (UE) 2002/58 sobre la privacidad y las comunicaciones electrónicas y sus posteriores modificaciones e integraciones.
  Por ejemplo: clientes, incluso los potenciales, empleados, candidatos a la contratación, asesores, proveedores, visitantes, usuarios de los sitios web del Responsable etc...

5. MODELO ORGANIZATIVO DE LA PRIVACIDAD DEL GRUPO UE

El Grupo UE ha decidido valerse de este modelo organizativo con la intención de uniformar las actividades internas de protección de los datos personales:

- **Referente Corporativo:** en síntesis, coordina la materia a nivel de todo el Grupo UE y guía en sus funciones a todos los Referentes de privacidad del Grupo UE. Un detalle de las responsabilidades y de las tareas asignadas se encuentra en el documento PRCY011 disponible en la intranet de la empresa.

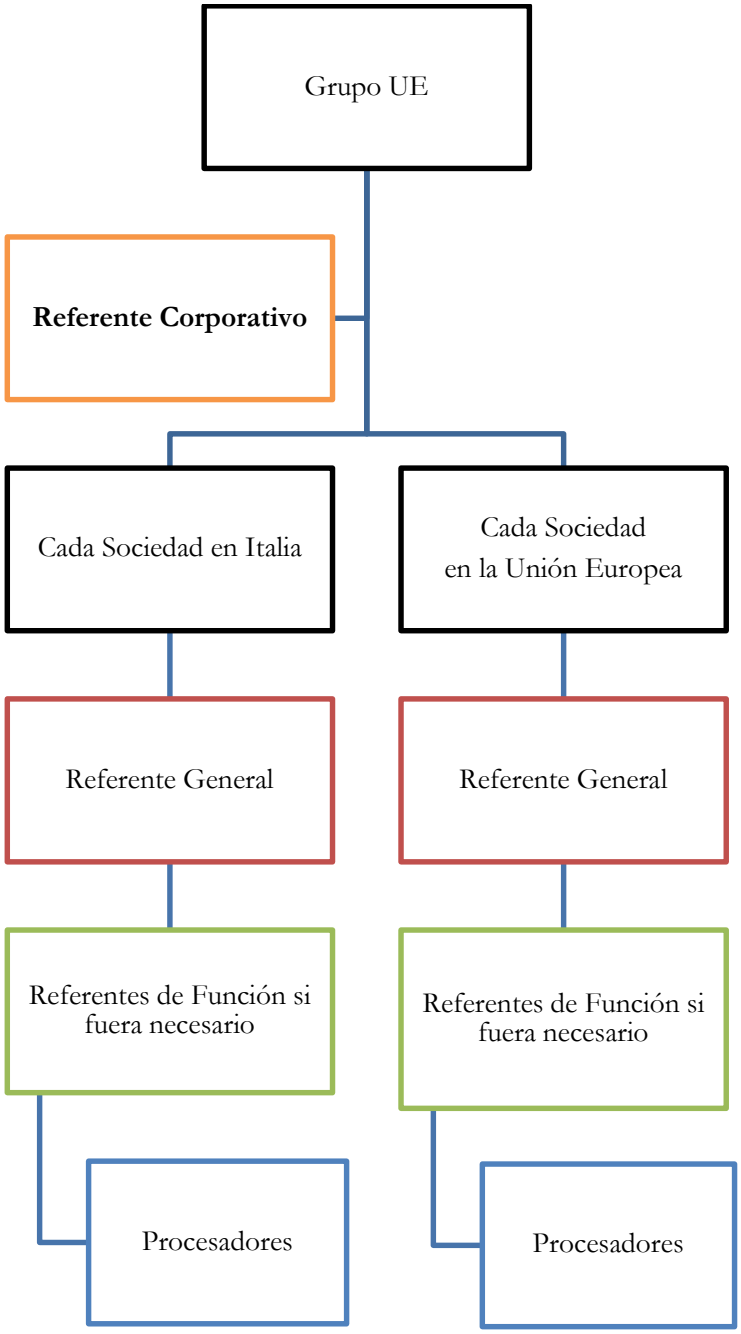
- **Referente General:** en síntesis, coordina la materia a nivel de cada Sociedad que lo ha nombrado, considerada en su totalidad, y guía en sus funciones a todos los Referentes de función eventualmente nombrados en la misma Sociedad. Un detalle de las responsabilidades y de las tareas asignadas se encuentra en el documento PRCY014 disponible en la intranet de la empresa.

- **Referente de función:** en síntesis, coordina la materia a nivel del departamento de la empresa que le ha sido asignado en la Sociedad que lo ha nombrado. Un detalle de las responsabilidades y de las tareas asignadas se encuentra en el documento PRCY015 disponible en la intranet de la empresa. Este Referente se nombra solo si el Referente general lo considera necesario.

- **Persona autorizada/procesador:** es la persona física que realiza concretamente las operaciones de tratamiento de los datos con el auxilio de instrumentos informáticos y/o mediante soportes de papel en el ámbito del departamento de la empresa al que ha sido asignado. Cada sociedad debe nombrar como procesador a los empleados que traten datos personales durante la realización de sus encargos. El documento de designación como procesador con la especificación del ámbito de los tratamientos permitidos, las instrucciones transmitidas y las tareas asignadas está a disposición en el documento PRCY016 disponible en la intranet de la empresa.

6. ESQUEMA ORGANIZATIVO PRIVACIDAD UE

En virtud de lo mencionado anteriormentre, el esquema organizativo de privacidad es el siguiente:



7. OTROS SUJETOS INVOLUCRADOS

En el ámbito de la gestión de los datos personales es posible involucrar a otros sujetos, como:

- **Encargado del tratamiento:** es el sujeto externo que realiza tratamientos de datos personales por cuenta del responsable. Estos tratamientos deben realizarse de acuerdo a un contrato escrito que reglamente la materia en cuestión, la duración del tratamiento, la naturaleza y los fines del tratamiento, el tipo de datos personales, las categorías de los interesados, las obligaciones y los

derechos del titular. En ámbito UE este contrato debe contener también los elementos esenciales establecidos por el art. 28, párrafo 3 del GDPR.
Los servicios que normalmente pueden externalizarse a los Encargados son, por ejemplo, la gestión de las nóminas, del sitio web, del soporte TI, etc.

- **DPO:** el Encargado de la Protección de Datos (Data Protection Officer) es una figura prevista por el art. 37 y siguientes del GDPR que una sociedad debe nombrar cada vez que:
  - las actividades principales del responsable del tratamiento o del encargado del tratamiento consistan en tratamientos que, por su naturaleza, ámbito y/o fines necesiten una supervisión constante y sistemática de los interesados a gran escala; o
  - las actividades principales del responsable del tratamiento o del encargado del tratamiento consistan en el tratamiento, a gran escala, de categorías específicas de datos personales contemplados en el art. 9 del GDPR o de datos relativos a condenas penales y delitos indicados en el art. 10 del GDPR.

  Sus tareas principales son el control del respeto del GDPR, el asesoramiento para la sociedad, el control de la actuación, formación y sensibilización en la materia etc.

  No ha sido necesario el nombramiento de un DPO para las Sociedades porque, vista la actividad típica de las Sociedades, que por su naturaleza no causa riesgos en el ámbito de la protección de los datos, dada la mínima actividad de tratamiento de datos personales de los interesados, sin duda no a gran escala, y dado que el tratamiento de categorías especiales de datos en el ámbito de la relación de trabajo no representa la actividad principal, sino secundaria (véase WP29, Directrices DPO, 2.1.2., p.9), no concurren las condiciones antes mencionadas.
  En caso de que las directrices o las normativas locales impongan a una de las Sociedades el nombramiento de un DPO (excepto a las italianas), deberá señalarse previamente la circunstancia al Referente corporativo.

- **Otros sujetos potenciales:** las normativas locales podrían prever la necesidad de identificar otros sujetos importantes para la protección de los datos personales. Cada sociedad deberá considerar si existe una normativa local que imponga obligaciones parecidas.
  Por ejemplo, en Italia existen los Administradores de Sistemas, que son las personas físicas que se ocupan de la gestión técnica de todo el sistema informático, o incluso de un único componente o de las actividades conexas. Estas personas deben recibir una designación específica como Administrador de Sistemas e instrucciones detalladas.

8. PRINCIPIOS GENERALES

Con referencia al tratamiento de los datos personales, el Grupo UE adopta todas las medidas tecnológicas, organizativas y logísticas más apropiadas para garantizar el respeto real de las garantías de protección de los datos personales.
Con este objetivo los procedimientos empresariales y las operaciones reales de tratamiento de datos realizados por los empleados y los procesadores deben respetar los siguientes principios.

8.1. **Licitud, lealtad y transparencia**

El tratamiento de los datos personales debe realizarse solo en caso de que se cumpla una de las condiciones previstas por la ley que lo permite, solo si el interesado lo sabe y si esto corresponde a lo que le ha sido declarado.

8.2. **Limitación de la finalidad**

Los datos personales deben tratarse solo para los fines declarados al interesado y no debe existir ninguna incompatibilidad con estos fines.

8.3. **Minimización**

El uso de los datos personales debe reducirse al mínimo y por consiguiente, si estos fines también pueden alcanzarse sin el uso de datos personales, el tratamiento debe realizarse con datos anónimos. Los datos anónimos son datos que no pueden asociarse de ninguna manera a un interesado identificado o identificable. Sobre todo, los datos deben ser adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que se tratan.

8.4. **Exactitud**

Los datos tratados deben ser exactos y estar actualizados. El interesado debe tener la posibilidad de controlarlos y rectificarlos.

8.5. **Limitación del plazo de conservación**

Los datos personales tratados no se conservan durante periodos de tiempo indefinidos. Deben eliminarse cuando se haya alcanzado el fin y por lo tanto cada Sociedad debe determinar los tiempos de conservación compatibles con dichos fines, respetando a su vez las normativas locales.

8.6. **Integridad y confidencialidad**

Cada Sociedad debe tratar los datos personales con el fin de garantizar una seguridad y una confidencialidad adecuadas y también para impedir el acceso o el uso no autorizado de los datos personales y de los instrumentos utilizados para el tratamiento.

8.7. **Rendición de cuentas**

Cada Sociedad debe garantizar el respeto de los principios antes mencionados y ser capaz de demostrarlo.

9. REGLAS OPERATIVAS

Con arreglo a los principios antes mencionados y a las otras normas indicadas en el GDPR, cada Sociedad deberá operar respetando las siguientes reglas operativas.

9.1. **Registros de las actividades de tratamiento**

Cada Sociedad, a través de sus Referentes, debe documentar los tratamientos informáticos y manuales realizados en los diferentes departamentos internos. Cada Sociedad debe cumplir con esta obligación, cumplimentando los registros de las actividades de tratamiento, de conformidad con el art. 30 del GDPR y respetando las indicaciones proporcionadas en cada país por las Autoridades de control locales.

El Referente general tiene la responsabilidad de garantizar que cada Sociedad disponga de los registros previstos y de su constante actualización. Deberá definir un procedimiento de gestión apropiado, estableciendo las responsabilidades y las tareas en la Sociedad y colaborando con los Referentes de función, si están presentes.

De todas maneras, la actualización de los registros debe realizarse cada año.

9.2. **Declaración de privacidad y recogida de los datos *(transparencia y lealtad)***

En general los interesados conceden directamente sus datos personales en el ámbito de los contactos comunes de trabajo, durante la realización de actividades operativas en las Sociedades o mediante el sitio web, pero también pueden obtenerse a través de terceros. Los empleados que recojan los datos personales de un interesado deberán comprobar, durante la recogida, que dicho interesado haya sido informado de manera apropiada sobre los fines para los cuales se recogen y se tratarán posteriormente.

Para ello deben proporcionar la «declaración de privacidad» apropiada preparada por la Sociedad.

La entrega de la declaración de privacidad deberá realizarse siempre, incluso cuando no es necesario que el interesado dé su consentimiento para el tratamiento de sus datos.

Las operaciones que no tengan una declaración de privacidad o que no estén presentes en la misma son ilícitas y por lo tanto no pueden realizarse.

La declaración de privacidad se proporciona una sola vez y con anterioridad a la primera recogida de datos de un interesado.

Se proporcionará una nueva declaración de privacidad en caso de variación de algunos elementos indicados en el documento entregado anteriormente.

9.3. **Condiciones de licitud del tratamiento**

Para cada fin presente en la declaración de privacidad debe identificarse por lo menos una base legal que permita el tratamiento lícito.

Las bases legales se indican en el art. 6 del GDPR con referencia a los datos personales «comunes», que en síntesis consisten en las siguientes alternativas:

- Consentimiento
- Cumplimiento del contrato
- Cumplimiento de una obligación legal
- Protección de los intereses vitales
- Misión de interés público
- Interés legítimo (no debe predominar sobre los derechos del interesado)

Por lo que se refiere al tratamiento de categorías especiales de datos, las bases legales se indican en el art. 9 del GDPR y en el art. 10 en el caso de Datos penales, y son más restrictivas que las de los datos comunes.

9.4. **Consentimiento del interesado *(licitud)***

Se menciona el consentimiento del interesado entre las bases legales de licitud. El consentimiento no se recoge si el tratamiento se basa en una de las otras condiciones de licitud (como indicado en el punto anterior). Sin embargo, algunos tratamientos lo necesitan como condición de licitud. Las operaciones de tratamiento deben ser conformes a este consentimiento dado por el interesado como respuesta a la declaración de privacidad. El interesado debe dar libremente su consentimiento, debe recogerse solo mediante una declaración de privacidad apropiada, ser demostrable y no ambiguo.

Cuando el tratamiento requiere el consentimiento, no se podrá realizar hasta haberlo obtenido.

9.5. **Accesibilidad a los datos y actividades permitidas al personal**

Se permiten el acceso a los datos personales y el desarrollo de las actividades de tratamiento solo a las personas que hayan sido debidamente autorizadas y hayan recibido instrucciones apropiadas. Estos procesadores podrán acceder a los datos solo en base de un principio «need to know» (principio de mínimo conocimiento). Los datos deben utilizarse solo para realizar el encargo y las tareas gradualmente atribuidas.

Como ya se ha indicado anteriormente, cabe destacar que:

- las operaciones que no tengan una declaración de privacidad o que no estén presentes en la misma no podrán realizarse;
- está prohibido realizar tratamientos sin que se haya obtenido el consentimiento, cuando es necesario.

9.6. **Accesibilidad a las categorías especiales de datos y a los datos penales. Actividades permitidas al personal**

Estos datos deben ser tratados solo por los procesadores que los necesiten estrictamente para la realización de su encargo y mediante autorización específica.

Además de los vínculos antes mencionados, que se refieren a le necesidad de una declaración de privacidad y de un eventual consentimiento, se recuerda que las operaciones de tratamiento de estos datos también deben respetar las condiciones y los límites establecidos por las normativas locales.

Por ejemplo, en Italia, las condiciones y los límites se establecen en las Autorizaciones Generales emitidas por el Supervisor de Protección de Datos y están a disposición en el sitio web del Supervisor (www.garanteprivacy.it).

Por lo tanto está prohibido realizar tratamientos no conformes a las normativas locales.

9.7. **Medidas de seguridad**

Todos los procesadores deben respetar puntualmente las normas en materia de seguridad previstas por la Sociedad. El incumplimiento puede causar consecuencias legales importantes, a veces incluso

penales. El respeto de estas medidas de seguridad depende exclusivamente del comportamiento de los procesadores.

9.8. **Circulación de datos y comunicación de datos a terceros**

Los datos personales pueden circular regularmente en las Sociedades del Grupo UE entre los procesadores que necesiten conocerlos por razones de trabajo *(need to know)* y que han recibido instrucciones al respecto. En cambio, no deben transmitirse, o ser de todas maneras accesibles, a terceros externos al Grupo UE, a menos que se verifique una de estas hipótesis:

- la transmisión al tercero es necesaria para cumplir con una obligación legal u orden de la autoridad pública;
- la transmisión al tercero es necesaria para realizar obligaciones que derivan de un contrato firmado con el interesado al que se refieren los datos personales;
- en caso de que el tercero haya sido nombrado Encargado del tratamiento, de conformidad con el art. 28 del GDPR, y los datos sirvan para la realización del servicio externalizado;
- la persona a la que se refieren los datos personales ha dado de manera explícita su consentimiento para la transmisión de los datos en cuestión al tercero.

Las eventuales necesidades de transmisión de datos a un tercero por razones diferentes de las que se han mencionado anteriormente deben obtener la autorización escrita por parte del Referente General de la Sociedad en ejercicio.

De todas maneras, no forma parte de la política del Grupo UE, bajo cualquier concepto o para cualquier fin, la cesión de listas o direcciones que se configuren como comercialización de datos personales.

9.9. **Nuevos tratamientos y tratamientos con riesgos elevados**

Bo pueden iniciarse nuevos tratamientos que presenten un riesgo elevado, sin una autorización previa, como se indica y regula en la política de la empresa relativa a la evaluación de impacto de los tratamientos previstos para la protección de los datos personales (Evaluación de impacto o **DPIA**). Los principales elementos que deben considerarse y que pueden causar riesgos elevados a los interesados son:

- Evaluación, asignación de una puntuación o elaboración de perfil
- Decisiones automatizadas con efecto jurídico o que influyen de manera análoga y significativa en las personas físicas
- Supervisión sistemática
- Tratamiento de categorías especiales de datos
- Tratamiento de datos a gran escala
- Creación de correspondencias o combinaciones de datos
- Tratamiento de datos relativos a intereses vulnerables
- Uso innovador o aplicación de nuevas soluciones tecnológicas u organizativas
- Tratamiento que «impide que los interesados ejerzan un derecho o que se valgan de un servicio o de un contrato»

Además de estos elementos, la normativa local podría prever más casos de riesgo o casos que exijan la obligatoriedad de la DPIA. En Italia, el Supervisor de Protección de Datos ha impuesto la obligatoriedad en una serie de casos como por ejemplo los tratamientos no ocasionales de datos relativos a sujetos vulnerables, tratamientos sistemáticos de datos biométricos etc.

9.10. **Violación de la seguridad de los datos personales (Data Breach)**

Una violación de datos personales significa «toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos» (a continuación también **«Data Breach»**).

En caso de Data Breach es obligatorio notificarla a la Autoridad de control (Supervisor local) dentro de 72 horas de su comprobación.

El Grupo UE tiene una política de gestión de las violaciones de datos personales que todos los procesadores deben conocer y que requiere, cuando ocurra esta situación, la inmediata comunicación a su Referente de función o, si estuviera ausente, al Referente General para que se respeten los términos de notificación.

9.11. **Privacidad por diseño y por defecto**

El Grupo UE tiene una política de privacidad por diseño y por defecto que deberá respetarse en caso de desarrollo de nuevas aplicaciones o tratamientos y transmitirse a todos los procesadores implicados en el diseño y desarrollo de estos tratamientos y aplicaciones.

9.12. **Gestión de los derechos de los interesados**

El GDPR reconoce los siguientes derechos a los interesados:

- Derecho de acceso a sus datos personales (art. 15);
- Derecho de rectificación (art. 16);
- Derecho de supresión (derecho al olvido) (art. 17);
- Derecho a la limitación del tratamiento (art. 18);
- Derecho a la portabilidad de los datos (art. 20);
- Derecho de oposición (art. 21);
- Derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado (art. 22);
- Derecho a retirar su consentimiento en cualquier momento sin afectar a la licitud del tratamiento basada en el consentimiento previo a su retirada (art. 7.3);

El Grupo UE tiene una política para la gestión de las solicitudes de ejercicio de los derechos antes mencionados, mostrando su contenido. Cada procesador implicado en la fase de gestión de estas solicitudes debe conocer esta política. Se recuerda que en ausencia de una gestión correcta de las solicitudes indicadas en la política, el interesado tiene derecho a presentar una reclamación al Supervisor o recurrir a acciones legales para proteger sus derechos.

10. FORMACIÓN

El GDPR prevé la obligación de concienciar a los procesadores sobre los riesgos que conlleva el tratamiento de datos personales. Cada Sociedad debe por lo tanto encargarse de la sensibilización de los procesadores mediante una formación apropiada y coherente con la tarea asignada.
La formación no podrá hacerse una sola vez, sino que deberá proponerse periódicamente sobre todo ante modificaciones de las normativas o nuevas interpretaciones.
Con referencia a la formación, podrán ponerse a disposición documentos y presentaciones que aclaren los aspectos principales de la normativa, programas de educación en línea, clases presenciales y sesiones de comunicación etc.

Esta actividad de formación debe documentarse de manera obligatoria (para cumplir con el principio de responsabilidad proactiva). Cada empleado debe profundizar sus conocimientos al respecto para operar respetando plenamente la normativa, esta política de privacidad y las instrucciones en materia de tratamiento de datos. Otras eventuales necesidades de formación deben indicarse a los Referentes de función o, en su ausencia, al Referente General, que deberá dar curso a las solicitudes.

11. CONTROLES PERIÓDICOS

Cada Sociedad, en virtud de las obligaciones del GDPR, deberá organizar controles periódicos, también mediante los Referentes internos nombrados (Referente General y eventuales Referentes de función), sobre el cumplimiento de las disposiciones del GDPR, de las normativas locales y de las políticas de privacidad del Grupo UE, además de las instrucciones emanadas en materia de tratamiento de datos.
Los controles deben documentarse. Los procesadores deben prestar la máxima colaboración para facilitar los controles.

12. SANCIONES

La violación parcial o total de las disposiciones de la política de privacidad puede causar sanciones penales, civiles y administrativas previstas para los tratamientos ilícitos o no conformes a la normativa de referencia.
En los casos más graves, la sanción administrativa aplicable de conformidad con el art. 83, párrafo 5 del GDPR puede ser de hasta 20.000.000 de Euros, o en el caso de una empresa, de hasta un 4 % de la facturación anual global del ejercicio financiero anterior, optándose por la de mayor cuantía.

Comportamientos ilícitos o no conformes a esta Política, a las políticas del Grupo UE y a las instrucciones en materia de tratamientos de datos personales pueden comportar medidas disciplinarias que dependen de la gravedad de los hechos.

*** *** ***