KINGFISHER PLC

Normativa de protección de datos

Propietario del documento:	Director de protección de datos del grupo
Documento a la atención de:	Todas las empresas de Kingfisher
Política subyacente	Política de protección de datos
Próxima fecha de revisión:	9 de enero de 2019
Documentos pertinentes de la política:	Política de protección de datos, Política de mantenimiento de registros y conservación de documentos, Política de seguridad de la información sobre mantenimiento de registros y conservación de documentos y Política de uso correcto

Contenido

1. Resumen y objetivos

La finalidad de la presente Normativa sobre política es garantizar el cumplimiento de las legislaciones pertinentes en materia de protección de datos y confidencialidad, así como asegurar que los datos de nuestros clientes, empleados y proveedores se recopile y utilice siempre de forma correcta en cualquier jurisdicción en la que operen compañías del grupo Kingfisher.

En la presente Normativa sobre política, con "**Datos personales**" se hace referencia a aquella información recopilada por separado o conjuntamente con otra información que permite identificar a un individuo ("**Persona**"). Entre estos datos se incluyen, por ejemplo, direcciones de correo electrónicas profesionales de una Persona, su nombre junto con una dirección postal o fecha de nacimiento, la fotografía de una Persona, etc.

Los Datos personales deben mantenerse en condiciones de seguridad y tratarse de forma justa, transparente y legal en todo momento.

Todas las empresas del grupo deben conocer el marco legal pertinente para los territorios en los que opere.

- Dentro de la Unión Europea, el Reglamento General de Protección de Datos 2016/679 de la UE (RGPD) entrará en vigor el 25 de mayo de 2018, además de otras directivas y normativas de ámbito local relativas a la confidencialidad y la protección de los datos.
- Fuera de la Unión Europea, cualquier legislación pertinente de ámbito local o regional con la que deban cumplir las actividades de las empresas del grupo.

El Director de protección de datos del grupo establecerá y ejecutará procedimientos de cumplimiento con ayuda de la persona que, dentro de cada país en el que opere Kingfisher, esté encargada de cuestiones relativas a la protección de datos ("**Responsable nacional de protección de datos**").

2. Responsabilidad y gestión

2.1 EL DIRECTOR DE PROTECCIÓN DE DATOS DEL GRUPO es el encargado de la presente Normativa sobre política y su aplicación en todo el grupo.

El Director de protección de datos del grupo realiza las siguientes tareas y tiene las siguientes responsabilidades:

- Mantener debidamente informada a la Junta directiva en lo relativo a responsabilidades, riesgos y problemas de la protección de datos.
- Revisar y autorizar todos los procedimientos y las políticas de protección de datos con regularidad.
- Supervisar el cumplimiento de procedimientos, políticas y legislaciones pertinentes en materia de protección de datos.

- Disponer actividades de formación relacionadas con la protección de datos y ofrecer asesoramiento a empleados y otras personas incluidas en la presente política.
- Responder a dudas sobre protección de datos al personal, los miembros de la junta directiva y otras partes interesadas.
- Responder ante personas como clientes y empleados que quieran saber qué datos se conservan sobre ellos y comprobar y autorizar junto con los terceros que se encarguen de manipular los datos de la empresa cualquier contrato o acuerdo relativo al procesamiento de datos.
- Supervisar y revisar las evaluaciones de impacto de las actividades relacionadas con la confidencialidad.
- Actuar como persona de contacto con la autoridad supervisora pertinente y cooperar con las autoridades supervisoras locales.

La dirección de contacto del Director de protección de datos del grupo es dpo@kingfisher.com.

Tenga en cuenta que todas las empresas de Kingfisher y todas las funciones que formen parte del Grupo deben notificar, sin dilaciones indebidas, cualquier información que pueda necesitar el Director de protección de datos del grupo para la realización de sus actividades.

2.2 El Responsable nacional de protección de datos se encarga de:

- Ayudar al Director de protección de datos del grupo a conocer la legislación local pertinente en materia de confidencialidad y protección de datos.
- Ayudar al Director de protección de datos del grupo a establecer normas y procedimientos en algún país o territorio en el que operen empresas del grupo Kingfisher.
- Actuar de vínculo entre el Director de protección de datos del grupo y las correspondientes empresas del grupo Kingfisher de un país en lo relativo a protección de datos y confidencialidad.

Hay disponible una lista de Responsables nacionales de protección de datos en la Intranet. El equipo de Comunicaciones internas notificará cualquier cambio que se efectúe en ella.

2.3 El EQUIPO DE GESTIÓN DE TI se encarga de garantizar la seguridad de los datos almacenados en sistemas de Kingfisher y terceros.

Siempre debe consultarse al Equipo de gestión de TI cuando alguna empresa del grupo o tercero vaya a procesar datos. Las personas de contacto del Equipo de gestión de TI están indicadas en la Intranet. El equipo de Comunicaciones internas notificará cualquier cambio que se efectúe al respecto.

Tareas y responsabilidades del Equipo de gestión de TI:

- Garantizar que todos los sistemas, los servicios, los programas informáticos (software) y los equipos cumplan con las normativas de seguridad pertinentes.

- Garantizar que todos los sistemas, los servicios, los programas informáticos (software) y los equipos cumplan con las políticas, las directrices, los procedimientos y la legislación en vigor de cada país.
- Redactar políticas de seguridad sobre sistemas e información, así como documentos de carácter contractual.
- Aplicar la debida diligencia con terceros.

3. Normas mínimas del grupo

A menos que la legislación de una jurisdicción en la que operen compañías del grupo Kingfisher imponga requisitos más estrictos (en cuyo caso corresponde aplicarlos), debe cumplirse con las siguientes normas en todo momento en todo el grupo Kingfisher durante la manejo de Datos personales de empleados, clientes y proveedores. Se proporcionará información más detallada sobre las normativas específicas de cada país a cada empresa del grupo Kingfisher por medio del Director de protección de datos del grupo o el Responsable nacional de protección de datos correspondiente.

3.1 Recopilación de datos:

Antes de recopilar Datos personales:

- Debemos asegurarnos de recopilar únicamente aquellos Datos personales estrictamente necesarios para la finalidad correspondiente.
- Debemos asegurarnos de que la finalidad para la que se recopilen sea legan y que no constituya infracción alguna de los derechos de la Persona.
- Debemos notificar de forma clara a las Personas del uso que pretendemos hacer de sus Datos personales así como de los motivos por los que los recopilamos.
- Debemos garantizar que los Datos personales se recopilen y almacenen en condiciones de seguridad y que se apliquen medidas de protección pertinentes para evitar accesos no autorizados, pérdidas o daños en dichos Datos personales.

3.2 Manejo de datos:

- Debemos garantizar que los Datos personales no estén a disposición de personas que no necesiten acceder a ellos.
- Debemos garantizar que los Datos personales solo se utilicen para aquellas finalidades para las que se hayan recopilado y que, dentro de lo razonable, sean las conocidas por la Persona a la que corresponden.
- Debemos comprobar con regularidad y confirmar que los datos se manejen y almacenen en condiciones de seguridad suficientes y que estén protegidos de accesos no autorizados, daños y pérdidas.
- Debemos identificar y registrar la siguiente información en algún formato, que será comunicada por el Director de protección de datos del grupo: (i) categorías de los datos que vayan a recopilarse y manejarse; (ii) categorías de las Personas cuyos datos vayan a procesarse; (iii) categorías de destinatarios a los que se hayan comunicado o vayan a comunicarse los Datos personales; (iv) direcciones de los lugares donde estén almacenados los datos o vayan a almacenarse.
- Debe consultarse al Director de protección de datos del grupo o el Responsable nacional de protección de datos correspondiente antes de utilizar cualquier

herramienta de procesamiento automatizada que implique la toma de decisiones de forma automatizada relativas a una Persona, p. ej., evaluar ciertos aspectos personales de la Persona para analizar o predecir ciertos aspectos de su desempeño laboral, su situación económica, su estado de salud, sus preferencias personales, sus intereses, su grado de fiabilidad, su comportamiento, su ubicación o los desplazamientos que realice.

3.3 Transferencia de datos:

Antes de acceder a garantizar acceso (ya sea por transferencia o de forma remota) a los Datos personales a cualquier entidad procesadora no perteneciente al grupo Kingfisher:

- Debemos garantizar que la entidad procesadora a la que transfiramos Datos personales cumpla tanto con la presente Normativa como con la legislación en vigor pertinente.
- Debemos recopilar y registrar siempre la siguiente información: (i) el nombre y los datos de contacto del representante de la entidad procesante y del responsable de protección de datos correspondiente; (ii) las categorías de los datos procesados; (iii) las categorías de las Personas cuyos datos vayan a procesarse; (iv) la dirección de la ubicación a la que vayan a transferirse los datos o a la que vaya accederse para consultarlos; (v) la lista y los datos empresariales de cualquier entidad procesante secundaria, y (vi) las categorías de los destinatarios a los que se hayan comunicado o vayan a comunicarse los Datos personales.
- Debemos garantizar que no se transfiera ningún Dato personal ni se acceda a él desde cualquier país o territorio diferente a menos que en dicho país o territorio exista un grado de protección suficiente como para garantizar los derechos y libertades de las Personas relativos al procesamiento de datos personales, o bien que exista un contrato escrito con las garantías adecuadas firmado por ambas partes (u otras disposiciones que dispongan dichas garantías de conformidad con la legislación pertinente en materia de protección de datos).

3.4 Conservación de datos

Los Datos personales no deben mantenerse durante periodos superiores a lo estrictamente necesario para la finalidad para la que se hayan recopilado (véase la sección 3.1 anterior). Por tanto, los datos deben destruirse o desecharse como corresponda de los sistemas de la empresa cuando dejen de ser necesarios.

Ejemplo: Un cliente ha participado en un concurso para ganar una herramienta eléctrica, para lo que debe rellenar un formulario con su nombre, dirección y número de teléfono, y ha marcado una casilla para indicad que no desea recibir ninguna comunicación adicional de la empresa del grupo correspondiente. Una vez realizado el sorteo, la compañía del grupo debe eliminar los datos del cliente enviados por medio del formulario, ya que dejan de ser necesarios para la finalidad para la que se obtuvieron.

Debe cumplirse con la política de Kingfisher sobre conservación de documentos y la legislación pertinente relativa al tiempo de conservación.

3.5 Derechos de las Personas

El procesamiento de los datos debe realizarse de conformidad con los derechos de las Personas. Los derechos de las Personas varían en función del país. En la Unión Europea, las Personas tienen los siguientes derechos generales:

(a) a retirar su consentimiento sobre el procesamiento de sus Datos personales (en caso de que se haya dado consentimiento para la realización de dicho procesamiento);
(b) a denegar el procesamiento de sus Datos personales (en caso de que dicho procesamiento se efectúe conforme a intereses legítimos);
(c) a obtener acceso a cualquier Dato personal que se conserve sobre ellas;
(d) a la rectificación de cualquier error en sus Datos personales;
(e) a la eliminación de sus Datos personales de los sistemas de la empresa;
(f) a la transferencia de sus Datos personales a otras empresas;
(g) a impedir cualquier procesamiento que pudiera suponerle daños personales o incomodidades tanto a ellas como a otras Personas.

3.6 Reclamaciones y vulneraciones

Cualquier reclamación o vulneración, incluida cualquier vulneración de la seguridad que pudiera afectar a los Datos personales, debe comunicarse de inmediato al Director de protección de datos del grupo, al Responsable correspondiente o a ambos.

Cualquier reclamación relativa a alguna vulneración de la seguridad que pudiera afectar a los Datos personales debe comunicarse de inmediato al Encargado de gestión de TI.

Cualquier sustracción, uso incorrecto o vulneración de la seguridad que diera como resultado la destrucción, la pérdida, la alteración o la revelación no autorizada de Datos personales, o su acceso a estos, debe comunicarse de inmediato (en un plazo no superior a 2 horas) al Director de protección de datos del grupo y al Encargado de gestión de TI.

4. Auditorías y supervisión

El Director de protección de datos del grupo o los correspondientes Representantes nacionales de protección de datos realizarán periódicamente una auditoría de cumplimiento con la presente Normativa sobre políticas y cualquier otro proceso y normativa relativo a la protección de datos para garantizar dicho cumplimiento.

Si tuviera cualquier duda relacionada con la presente Normativa sobre políticas, consulte al Director de protección de datos del grupo o a su correspondiente Representante nacional de protección de datos.

También puede utilizar el número de teléfono de nuestro servicio de testimonios confidenciales para informar de las irregularidades que observe.

5. Descripción general de consentimientos y autorizaciones

Acción/situación	Comunicación		¿Por quién o para quién?
	Notificación (previa)	Autorización previa	
Vulneración de la seguridad de los datos	X		Director de protección de datos del grupo* + Encargado de gestión
Toma de decisiones automatizada (incluida la generación de perfiles)	X	X	Director de protección de datos del grupo + Encargado de gestión
Reclamaciones relativas al uso de datos	X		Director de protección de datos del grupo
Consultas efectuadas por organismos normativos	X		Director de protección de datos del grupo + Director de asuntos legales del grupo
Acción de aplicación normativa	X		Director de protección de datos del grupo + Director de asuntos legales del grupo
Ejercicio de derechos personales relativos a datos	X		Director de protección de datos del grupo
Nuevas actividades de procesamiento que requieran de una Evaluación de impacto de actividades relacionadas con la confidencialidad de los datos	X	X	Director de protección de datos del grupo + Encargado de gestión

* En todos los casos, bien de forma directa, bien por medio del Representante nacional de protección de datos.