Política General de Protección de Datos

1. Política de Cumplimiento

a) Cox desarrolla su actividad en el mercado con pleno respeto a los derechos individuales relativos a la protección del honor y la intimidad, en cada una de las jurisdicciones en que opera.

b) Los empleados no están facultados para llevar a cabo, autorizar ni tolerar conductas que infrinjan las normas de Protección de Datos, el honor y la intimidad, o la política de Cox al respecto.

c) Los empleados deben adoptar medidas razonables para asegurar que otros empleados bajo su autoridad y/o responsabilidad conozcan y cumplan esta política.

d) La tolerancia con el incumplimiento es cero; todo empleado que incumpla lo dispuesto en el presente Programa podrá ser sancionado al respecto, incluso con el despido.

e) La compañía velará para que todo empleado tenga acceso a la información y al entendimiento de lo dispuesto en el presente Programa y al asesoramiento legal necesario.

f) Existe un Canal de Denuncias para que todo empleado pueda poner en conocimiento aquellos comportamientos que indiciariamente fuesen ilícitos o dudosos, para su investigación y resolución.

g) La presente política es un resumen general. El órgano de administración ha facultado especialmente al Delegado de Protección de Datos como responsable del diseño, implantación y ejecución de la política y la gestión de riesgos derivadas de la Protección de Datos.

2. Normativa aplicable

Es el conjunto de leyes y otras normas positivas, convenios y prácticas voluntariamente asumidos y normativa interna de la compañía. Incluye entre otras y de forma meramente enunciativa la siguiente que ha sido tomada en cuenta de forma principal para la implantación del presente Programa sin perjuicio del necesario contraste que con cada legislación local de aquellas jurisdicciones en las que Cox opere debe llevarse a cabo de manera preventiva:

- ✓ El Tratado de la Unión Europea y la Directiva 95/46
- ✓ Reglamento de Protección de Datos de la UE, (en su texto modificado el 12 de marzo de 2014 por el Parlamento Europeo a propuesta de la Comisión de libertades Civiles, Justicia y Asuntos de Interior (LIBE).
- ✓ Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal
- ✓ Reglamento de la anterior, según el Real Decreto 1720/2007, ambas del Reino de España

- ✓ La Ley de Protección de Datos de México
- ✓ Data Protection Act del Reino Unido.
- ✓ La Global Electronic Commerce, Video Privacy Protection Act y la Fair Credit Reporting Act, de los EEUU.

3. Desarrollo

La mayoría de los países y jurisdicciones disponen de normativa de obligado cumplimiento o de normas orientativas sobre las prácticas de mercado en lo relativo a la tenencia y uso por una empresa de datos personales de personas físicas.

El objetivo de estar normas es garantizar y proteger las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal.

A los efectos de la presente Política se entiende por "datos", "datos de carácter personal" cualquier información numérica, alfabética, gráfica, fotográfica, audio – visual o de cualquier tipo concerniente a personas físicas que por dichos datos puedan ser identificadas o identificables.

Un "fichero", "fichero de datos" o "base de datos" se refiere a todo conjunto de datos de carácter personal, organizado de alguna manera que permita el acceso a los datos utilizando algún criterio determinado.

Aplica por tanto con independencia del soporte (listas en papel, bases de datos informáticos), del medio de su tratamiento (manual o automático) y del dato en sí (alfabéticos como nombres, numéricos como los números de pasaporte o imagines, como las cámaras de vigilancia de los accesos a oficinas).

Por ejemplo:

- Datos relativos a la formación, evaluaciones, nóminas y administración del personal.
- Selección y evaluación de candidatos.
- Datos relativos a clientes, proveedores y/o colaboradores.
- Datos de control y gestión de proyectos.
- Datos relativos a administración, financiera y contable.
- Grabación de imágenes por cámaras de seguridad en los accesos o instalaciones propias
- Base de datos de las fotografías de los empleados.

Están excluidos los ficheros de uso exclusivamente personal o doméstico limitados a la vida privada de los particulares.

Cada sociedad es responsable de

1) Organizar sus ficheros de datos (accesos, bajas/altas, etc.).
2) Inscribir o notificar si fuera preceptiva los ficheros ante la autoridad gubernamental supervisora, así como de la calidad de los datos, y de recabar el consentimiento del afectado

3) Notificar la existencia de la base de datos y, en su caso, el contenido de la misma, a la autoridad gubernamental (nacional/federal o estatal/ regional) encargada de la supervisión de la ley de protección de datos.
4) Mantenimiento de las medidas de seguridad aplicables para la protección del fichero.
5) Implantación de medidas técnicas y organizativas para la gestión del fichero.
6) Los datos son estrictamente confidenciales.
7) Todos los soportes, programas, cámaras o cualquier medio de captación de datos deben tener incorporado un aviso legal de los datos que capturan y de las advertencias al usuario y sus derechos de acceso a los mismos.

Puede contratarse con un tercero debidamente cualificado aquellas tareas relacionadas con el tratamiento del fichero tales como:

1. Declaración y actualización de los ficheros comunes entre sociedades de un mismo grupo o subgrupo.
2. Mantenimiento de las medidas de seguridad al nivel adecuado (bajo, medio, alto) mediante el análisis de evaluación de impacto de privacidad

Igualmente es recomendable en todos los casos y en algunas jurisdicciones puede ser obligatorio, contar con Delegado de Protección de Datos (DPO) en la empresa para los casos legalmente previstos. El DPO supervisará la implantación y uso de medidas y políticas de protección de datos, siendo el interlocutor entre las autoridades y la empresa y asistiendo al responsable del tratamiento en las cuestiones más especializadas.

4. Transferencias Internacionales

Es especialmente sensible la transferencia de datos de un país a otro, incluso si se realiza entre sociedades filiales de un mismo grupo. Es indispensable con carácter previo el asesoramiento legal y técnico al respecto, por cada sociedad.

Los contratos, en virtud de los cuales, se posibilitan transferencias internacionales de datos a un tercer país que no cuente con un nivel adecuado de protección (entendiendo por tal el establecido en la Directiva de la UE), deberán contener la obligación de informar de los accesos a datos a las autoridades públicas.

5. Derechos individuales de la persona cuyos datos son tratados

Dependiendo de cada legislación nacional, la persona cuyos datos son obtenidos, almacenados y tratados tiene el derecho irrenunciable de:

- Acceso a sus datos
- Rectificación si sus datos son incorrectos
- Cancelación (supresión, borrado y olvido) de sus datos una vez extinguida la relación.
- Oposición

Estos derechos garantizan a que una persona física puede ejercer el control sobre sus datos personales. Se trata de derechos cuyo ejercicio es personalísimo e irrenunciable.

El ejercicio de estos derechos se debe llevar a cabo mediante medios sencillos y gratuitos puestos a disposición por el responsable del fichero y que están sujetos a plazo, por lo que resulta necesario establecer procedimientos para su satisfacción.

Si la persona reclamante cree que sus derechos no han sido atendidos en forma y plazo podría acudir a la tutela de la agencia gubernamental supervisora de los mismos.

- **Derecho de Acceso**
  El derecho de acceso es el derecho del afectado a obtener información sobre si sus propios datos de carácter personal están siendo objeto de tratamiento, la finalidad del tratamiento que, en su caso, se esté realizando, así como la información disponible sobre el origen de dichos datos y las comunicaciones realizadas o previstas de los mismos.

- **Derecho de Rectificación:**
  Derecho del afectado a que se modifiquen los datos que resulten ser inexactos o incompletos.

- **Derecho de Cancelación:**
  Derecho del afectado a que se supriman los datos que resulten ser inadecuados o excesivos.

- **Derecho de Oposición:**
  Derecho del afectado a que no se lleve a cabo el tratamiento de sus datos de carácter personal o se cese en el mismo (en los supuestos en que no sea necesario su consentimiento para el tratamiento), cuando se trate de ficheros de prospección comercial, o que tengan la finalidad de adoptar decisiones referidas al interesado y basadas únicamente en el tratamiento automatizado de sus datos.

6. Relación de Conductas contrarias a la Normativa o de Riesgo

- Omisión de la inscripción o notificación si fuera preceptiva de los ficheros ante la autoridad gubernamental supervisora
- Tenencia o captación de datos sin consentimiento o con oposición del afectado
- Falta de las medidas de seguridad para el control de la calidad de los datos y su tratamiento.
- Cesión de datos no consentida.
- Manipulación de datos personales
- Divulgación o publicación de datos fuera de contexto.
- Creación de perfiles de usuarios basados en los datos previamente obtenidos.

Si se tiene evidencia, constancia o sospecha de que un empleado de Cox, competidores, clientes o proveedores están quebrantando las leyes de Competencia debe ser informado de acuerdo con lo dispuesto para el Canal de Denuncias.

7. Las conductas exigidas y las conductas prohibidas a los empleados son:

7.1. Conductas Exigidas:

- Organizar sus ficheros de datos (accesos, bajas/altas, etc.).
- Inscribir o notificar si fuera preceptiva los ficheros ante la autoridad gubernamental supervisora, así como de la calidad de los datos, y de recabar el consentimiento del afectado
- Notificar la existencia de la base de datos y, en su caso, el contenido de la misma, a la autoridad gubernamental (nacional/federal o estatal/ regional) encargada de la supervisión de la ley de protección de datos.
- Mantenimiento de las medidas de seguridad aplicables para la protección del fichero.
- Implantación de medidas técnicas y organizativas para la gestión del fichero.
- Los datos son estrictamente confidenciales.

7.2. Conductas Prohibidas

- Tenencia o captación de datos sin consentimiento o con oposición del afectado
- Cesión de datos no consentida.
- Manipulación de datos personales
- Divulgación o publicación de datos fuera de contexto.
- Creación de perfiles de usuarios basados en los datos previamente obtenidos.

Si se tiene evidencia, constancia o sospecha de que un empleado de Cox, competidores, clientes o proveedores están quebrantando las leyes de Competencia debe ser informado de acuerdo con la sección Canal de Denuncias.

El **canal de denuncias** de Cox es común para las cinco sociedades, y para las sociedades controladas por Cox. Se garantiza la confidencialidad del informante, y la transparencia y objetividad del

procedimiento de canalización de las denuncias y su resolución. El Procedimiento de Canalización regula en detalle este proceso.

Entrada en vigor: El presente documento entra en vigor con su aprobación por el Consejo de Administración y permanecerá vigente hasta su actualización, revisión o derogación. La versión actual, revisión de 29 de septiembre de 2024 es la vigente, aprobada por el Consejo de Administración de 21 de noviembre de 2024. Esta política habrá de mantenerse actualizada y podrá ser para ello revisada anualmente, y de forma extraordinaria, cada vez que se produzcan variaciones en los objetivos estratégicos o legislación aplicable, procediéndose a presentar una propuesta de modificación por parte del director de Cumplimiento a la Comisión de Cumplimiento, y de ahí al Consejo de Administración.

Cox ABG Cox		
Política	• General de Protección de Datos	
Responsable	• Consejo de Administración	
Área	• Corporativa – Cumplimiento Normativo	
Control de Versión	Fecha / Aprobación	Cambios
1	29 de septiembre de 2024 / 21-11-2024	majv