

Introducción

Crawford & Company y sus subsidiarias de propiedad mayoritaria y contratadas (en su conjunto, “Crawford” o “la Compañía”) han adoptado esta Política global de privacidad y protección de datos (“Política”). Crawford reconoce la importancia de la privacidad y la seguridad, y se compromete a cumplir con las leyes de protección de datos aplicables y los requisitos contractuales con el cliente para manejar los Datos personales.

Propósito

Aunque las leyes de protección de los datos varían según la jurisdicción, todo el personal de Crawford debe saber que existen leyes para proteger la privacidad y seguridad de los Datos personales, y estas leyes repercuten en cómo utilizan, acceden, divulgan o procesan de alguna forma tal información Crawford y su personal.

Esta Política global de privacidad y protección de datos (“Política”):

- expone los principios de aplicación para el tratamiento de Datos personales por parte de Crawford, y describe cómo respeta Crawford estos principios; y
- proporciona una descripción general de la estructura de gobierno de la privacidad de Crawford, y las funciones y responsabilidades de grupos y personas esenciales para llevar a cabo las tareas y obligaciones de cumplimiento de la privacidad de Crawford.

Esta Política se complementará mediante políticas, directrices y procedimientos adicionales para abordar áreas, jurisdicciones, leyes y requisitos específicos.

Ámbito de aplicación

Esta política es de aplicación para todos los Datos personales que Crawford procese como responsable del tratamiento o procesador de los datos, lo que incluye en relación con su personal, clientes, demandantes, proveedores y otras partes. Se requiere que todo el personal respete esta política. El personal que infrinja esta política puede ser objeto de medidas disciplinarias, con sujeción a los términos de empleo y legislación local.

Todo el personal tiene una función importante que desempeñar en la gestión y protección adecuada de los Datos personales, en la identificación de la protección de los datos y en los asuntos de gestión de los datos a medida que surjan, y en remitirlos inmediatamente a la Oficina de privacidad global. También se espera que todo el personal coopere según resulte necesario para implementar los principios, requisitos y componentes clave de esta política.

Principios

- 1. Tratamiento justo, transparente y lícito.** Los Datos personales se recogerán, conservarán y tratarán de una forma justa, lícita y transparente. Esto significa:
 - 1.1. El responsable del tratamiento informará a las personas de dicho tratamiento.
 - 1.2. Los Datos personales se procesan de acuerdo con los fines declarados para su recogida o fines compatibles similares, y están sujetos a una base jurídica lícita como el consentimiento cuando así lo exija la ley.
 - 1.3. Los Datos personales no se procesan de formas que el interesado no esperaría razonablemente.
 - 1.4. Al actuar como procesador de los datos, los Datos personales únicamente se procesarán según sea necesario para realizar los servicios según indiquen los clientes, o cuando así lo exija la legislación aplicable.
- 2. Minimización de datos.** Los Datos personales solamente se recogerán cuando sea razonable y necesario para los fines declarados para los que se procesan, y serán adecuados, relevantes y limitados a lo que sea necesario en relación con esos fines.
- 3. Limitación de la finalidad.** Los Datos personales se procesarán con fines específicos, explícitos ilegítimos, y de una forma compatible con el fin para los que inicialmente se recogieron los Datos personales.
- 4. Exactitud.** Los Datos personales serán exactos y actualizados.
 - 4.1. Se adoptarán medidas razonables para garantizar la exactitud de los Datos personales obtenidos.
 - 4.2. Los Datos personales inexactos (considerando los fines de su tratamiento) se eliminarán o rectificaran.
- 5. Conservación limitada.** Los Datos personales se conservarán únicamente mientras sea necesario para lograr los fines especificados, sujeto a las leyes de protección de datos aplicables y los requisitos contractuales del cliente.
- 6. Seguridad e integridad.** Estarán en vigor medidas de seguridad técnicas, administrativas y organizacionales apropiadas para proteger los Datos personales, contemplar un tratamiento seguro de los Datos personales e identificar, prevenir, detectar y mitigar riesgos para los Datos personales y los sistemas, herramientas y procesos utilizados para procesar Datos personales.
 - 6.1. Los Datos personales se procesarán de una forma que proporcione seguridad apropiada para los Datos personales.

- 6.2. Se deben elaborar y poner en práctica medidas de seguridad para proteger contra el procesamiento ilícito y no autorizado, y la destrucción, daño o pérdida accidental de Datos personales y sistemas relacionados.
- 6.3. Se diseñarán y pondrán en práctica controles para detectar, mitigar y solucionar incidentes y eventos de seguridad.
- 6.4. Se establecerán procedimientos y políticas para que se informe internamente y de forma rápida de los eventos, incidentes de seguridad e incidentes de privacidad, y para que se investiguen, evalúen y gestionen conforme a las leyes de protección de datos establecidas cuando puedan afectar a Datos personales o actividades de tratamiento relacionadas.

7. Privacidad desde el diseño (Privacy by Design). Se diseñarán, implementarán y llevarán a cabo actividades y procedimientos de forma que desde el principio proporcionen cumplimiento con los principios anteriores y las integración de las protecciones necesarias de los Datos personales.

8. Responsabilidad.

El cumplimiento con estos principios se evaluará, y las actividades de procedimientos se llevarán a cabo de una forma que demuestre el cumplimiento, y que se puedan auditar y evaluar.

- 8.1. Las consultas y reclamaciones relacionadas con el tratamiento de los Datos personales se evaluarán, responderán y solucionarán (cuando sea posible) de forma justa y sin demoras innecesarias.
- 8.2. Se establecen procesos razonables para recibir, gestionar y responder a preguntas, solicitudes y reclamaciones de personas y clientes para posibilitar respuestas justas, oportunas, coherentes y lícitas.
- 8.3. Se mantendrán registros precisos de actividades de tratamiento, lo que incluye registros de incidentes de seguridad, reclamaciones, solicitudes de interesados y otros registros obligatorios en virtud de las leyes de protección de datos aplicables.

Componentes esenciales de cumplimiento de la privacidad

Para cumplir con los principios expuestos anteriormente, Crawford debe adoptar medidas para garantizar que se abordan estos principios en todas las actividades y procesos empresariales relevantes, y para implementar determinados procesos y procedimientos, lo que incluye los siguientes componentes clave, y todos ellos se abordan más adelante en esta política:

- Aviso para las personas

Política global de privacidad y protección de datos

- Base jurídica para el tratamiento
- Mantenimiento de registros (y registros del procesamiento)
- Derechos del interesado
- Gestión de terceros y proveedores
- Respuesta ante incidentes
- Formación y concienciación sobre privacidad
- Evaluaciones de impacto en la privacidad
- Auditorías y evaluaciones continuas
- Gobierno

Aviso para las personas

Crawford avisará a los interesados acerca de los Datos personales que procesa sobre ellos según requieren la Ley de protección de datos, lo que incluye avisar de lo siguiente: Los tipos de Datos personales recogidos, los fines del tratamiento, los métodos de tratamiento, los derechos de los interesados con respecto a sus Datos personales, el periodo de conservación, posibles transferencias internacionales de los datos, si los datos se compartirán con terceros y las medidas de seguridad de la empresa para proteger los Datos personales.

Para los empleados, esta información se expondrá en un aviso de privacidad para empleados y avisos adicionales, según sea necesario en virtud de la ley de protección de datos aplicable. Cuando proceda, se proporcionarán a los nuevos empleados durante la incorporación los avisos de privacidad para empleados, y una copia del aviso de privacidad también se expondrá en línea cuando sea posible, y estará disponible a través de los contactos locales de recursos humanos. Se notificará a los empleados y se les proporcionará una copia de los avisos de privacidad para empleados pertinentes cuando se efectúen cambios materiales.

Se deberá proporcionar o poner a disposición de forma recuperable y fácilmente accesible un aviso de privacidad para clientes, proveedores y otros terceros relevantes, cuando sea factible en el momento de la recogida de los Datos personales o cuanto antes resulte razonable hacerlo.

Base jurídica para el tratamiento

Crawford solamente podrá recoger y procesar los Datos personales cumpliendo con las leyes de protección de datos aplicables, y cuando se requiera con el consentimiento del interesado. Al actuar como procesador de los datos, los Datos personales únicamente se procesarán según sea necesario para realizar los servicios según indiquen los clientes, o cuando así lo exija la legislación aplicable.

Siempre que el procesamiento de los Datos personales se base en el consentimiento explícito del interesado, se deberá realizar y mantener un registro de tal consentimiento.

Según la legislación, los Datos personales sujetos a las leyes de protección de los datos de la UE solamente se podrán procesar de conformidad con bases jurídicas específicas. Cuando Crawford sea responsable del tratamiento, estará bajo su responsabilidad asegurarse de que el procesamiento se lleva a cabo conforme a una o más bases jurídicas específicas (p. ej., consentimiento, necesario para realizar el contrato con la persona, finalidad comercial legítima, por imperativo legal, necesario para defender los derechos) y que se haya revelado a los interesados la base jurídica en el aviso de privacidad relevante.

Mantenimiento de registros

Crawford mantendrá registros exactos de sus actividades de procesamiento, lo que incluye registros obligatorios según se establece en las leyes de protección de datos aplicables. La Oficina de privacidad global mantiene un registro/inventario de datos del procesamiento relacionado con el tratamiento por parte de Crawford de Datos personales, según se requiera en virtud de las leyes de protección de datos de la UE. Es responsabilidad del responsable de la protección de datos del grupo en la UE asegurarse de que el registro del procesamiento se actualiza cuando proceda.

Derechos del interesado

Los interesados tienen derechos específicos relacionados con sus Datos personales y con cómo se procesan. Se proporcionará a los interesados un mecanismo razonable para que puedan acceder a sus Datos personales, ejercer cualquier otro derecho aplicable, como el derecho a actualizar, rectificar, borrarlo transmitir en formato portátil sus Datos personales, si procede o lo requiere la legislación (“Derechos del interesado”), y para consultar o enviar una reclamación en relación con el tratamiento de sus Datos personales.

Procesador de datos

Al actuar como procesador de los datos, Crawford, de conformidad con la legislación aplicable y los requisitos contractuales, notificará al responsable

Política global de privacidad y protección de datos

del tratamiento cualquier solicitud de los interesados para ejercer sus derechos de interesado y proporcionar a solicitud asistencia razonable para que el responsable del tratamiento responda a la solicitud como exigen las leyes de protección de datos.

Responsable del tratamiento

Al actuar como responsable del tratamiento, es responsabilidad de Crawford respetar los derechos del interesado y responder a las solicitudes relacionadas como exigen las leyes de protección de datos. El responsable de privacidad o un delegado proporcionarán pautas para responder a tales solicitudes; todo el personal es responsable de respetar tales pautas.

Transferencias transfronterizas de Datos personales

Las leyes de protección de datos aplicables y los compromisos con los clientes pueden requerir que Crawford adopte medidas para proteger los Datos personales antes de transferir los Datos personales fuera del país donde se recogieron.

Protección equivalente.

Crawford debe adoptar medidas para garantizar que las transferencias transfronterizas de los Datos personales están sujetas a protecciones apropiadas. Los Datos personales objeto de transferencias transfronterizas deben ser procesados por o en nombre de Crawford de conformidad con las leyes de protección de datos aplicables y los compromisos con los clientes.

Transferencias limitadas

Las transferencias ilimitadas de Datos personales deben llevarse a cabo de conformidad con las leyes de protección de datos aplicables y los compromisos con los clientes.

Para procesar apropiadamente tales Datos personales, Crawford ha adoptado diversas medidas para garantizar que los Datos personales se protegen adecuadamente cuando se transfieren fuera de la jurisdicción en donde se recogieron.

Cuando haya una transferencia limitada de Datos personales se deben emplear protecciones adecuadas, lo que incluye ejecutar las cláusulas contractuales tipo, si procede. Crawford evaluará si es necesaria autorización de las autoridades de control o clientes pertinentes.

Transferencias dentro del grupo Crawford

Crawford ha ejecutado un Acuerdo de procesamiento de datos intragrupo, que incorpora las cláusulas contractuales tipo, para proporcionar garantías adecuadas para las transferencias limitadas entre entidades del grupo Crawford, así como otros tratamientos de Datos personales por parte de una

o más entidades del grupo Crawford en nombre de una o más entidades del grupo Crawford.

Cada entidad del grupo Crawford firmará el acuerdo de transferencia de datos intragrupo, y cumplirá con dicho acuerdo con respecto a cualquier transferencia o procesamiento entre las entidades del grupo Crawford. A medida que nuevas entidades formen parte de Crawford, cada nueva entidad tendrá que firmar el acuerdo de transferencia de datos intragrupo.

Transferencias a proveedores

Antes de que tenga lugar alguna transferencia limitada a un proveedor, Crawford adoptará medidas para incorporar las cláusulas contractuales tipo en el acuerdo contractual pertinente entre Crawford y el proveedor.

Gestión de terceros y proveedores

Las relaciones comerciales con la contratación de terceros deben realizarse de una forma que cumpla con esta política, las leyes de protección de datos aplicables y los compromisos con los clientes.

Solamente se podrá contratar a proveedores y subprocesadores si pueden satisfacer estándares adecuados y proporcionar protecciones apropiadas de los Datos personales.

Como mínimo:

- Se realizará la diligencia debida apropiada de todos los proveedores y subprocesadores, antes de que procesen Datos personales (lo que incluye el acceso o almacenamiento), y de forma continuada posteriormente según sea necesario (sujeto al programa de gestión del riesgo de terceros de Crawford).
- Se deben implementar obligaciones contractuales apropiadas con cada proveedor, lo que incluye (cuando sea relevante) obligaciones contractuales que sean equivalentes a las que sean de aplicación para Crawford conforme con sus contratos con clientes pertinentes.
- Crawford debe adoptar medidas para incorporar las cláusulas contractuales tipo en el acuerdo contractual pertinente entre Crawford y el proveedor, si pudiese haber alguna transferencia limitada.
- Se completarán todas las medidas necesarias según las leyes de protección de datos aplicables y los compromisos contractuales con clientes.

Se debe evaluar, contratar y gestionar a proveedores y terceros de conformidad con el programa de gestión del riesgo de terceros de Crawford.

Respuesta ante incidentes Se necesitan controles adecuados para detectar, comunicar y gestionar los incidentes de seguridad que puedan afectar a los Datos personales, de acuerdo con las políticas y procedimientos establecidos, lo que incluye la Política de respuesta ante incidentes y las leyes de protección de datos aplicables.

Cuando un evento o un incidente de seguridad puede afectar a los Datos personales o indicar una violación de esta política, las leyes de protección de datos o los compromisos con clientes, se debe notificar inmediatamente a la oficina de privacidad global.

La oficina de privacidad global es responsable de evaluar, investigar y determinar la respuesta y obligaciones de notificación que surjan de un evento de privacidad o un incidente de privacidad, y se requiere a todo el personal que coopere con la oficina de privacidad según resulte necesario para evaluar, investigar, mitigar, informar y solucionar incidentes y eventos de privacidad. La oficina de privacidad global tiene autoridad exclusiva para determinar si un incidente o evento de privacidad es una violación de la seguridad; el personal no debe especular o identificar algún incidente como una violación de la seguridad, salvo si así se lo indica la Oficina de privacidad global.

Cuando se determine que se ha producido una violación de la seguridad, Crawford deberá actuar inmediatamente para proporcionar cualquier aviso necesario a clientes, autoridades de control e interesados relevantes.

Formación y sensibilización sobre privacidad

La administración de la privacidad y la protección de los datos son fundamentales para Crawford, y su capacidad para:

- Cumplir con las leyes y compromisos contractuales con clientes
- Controlar los riesgos
- Mantener la confianza
- Operar con efectividad
- Respalda objetivos estratégicos y el modelo de administración de los datos

Formación anual

Se exigirá a todo el personal formación obligatoria sobre privacidad y seguridad, como mínimo anualmente, en relación con la privacidad, la protección de datos y la seguridad de la información.

Política global de privacidad y protección de datos

Formación adicional basada en la función

Cuando proceda, el personal con funciones que esté involucrado en la gestión regular de Datos personales y aquel con responsabilidades específicas clave dentro de la estructura de gobierno de la privacidad recibirá recursos y formación adicional según la función.

Recursos de privacidad incorporados

Se identificarán enlaces de privacidad en toda la empresa para apoyar las iniciativas de privacidad, desarrollar el conocimiento entre los colegas y servir de enlace con la Oficina de privacidad global.

Evaluaciones de impacto en la privacidad

Es de importancia crítica que se diseñen, implementen y lleven a cabo actividades y procesos de forma que contemple el cumplimiento con las Leyes de protección de datos y las políticas de Crawford y la integración de las protecciones necesarias de los Datos personales. Este es un componente clave del principio de privacidad desde el diseño (*véase más arriba del Principio 7*).

Crawford ha desarrollado una política y procedimientos para llevar a cabo evaluaciones del impacto en la privacidad, y cuando sea necesario, evaluaciones formales del impacto en la protección de los datos.

Evaluaciones de impacto en la privacidad

Se deben realizar Evaluaciones de impacto en la privacidad (EIP) para evaluar la repercusión en la privacidad e identificar los riesgos para proyectos, actividades y proveedores que puedan afectar a la privacidad y seguridad de los Datos personales. Se debe realizar una EIP antes de contratar a un nuevo proveedor, iniciar un nuevo proyecto, diseñar o actualizar significativamente un nuevo sistema, combinar datos de dos sistemas o conjuntos de registros, o participar de alguna forma en un nuevo proceso o actividad que haya cambiado sustancialmente y que pueda afectar a los Datos personales o en cómo se procesan.

Evaluaciones del impacto en la protección de los datos

Cuando una EIP indique que es probable que el tratamiento de los Datos personales genere un elevado riesgo para las libertades y derechos de las personas, se llevará a cabo una evaluación formal del impacto en la protección de los datos (EIPD) antes de tal procesamiento, para determinar la naturaleza de esos riesgos y mitigarlos en la medida de lo posible. Tal tratamiento no empezará hasta que el Comité de asesoramiento sobre la privacidad haya determinado que se han mitigado de forma adecuada los riesgos del tratamiento.

Evaluaciones y actualizaciones continuas

Se realizarán evaluaciones continuas del riesgo de los sistemas y procesos comerciales relevantes para:

- verificar que están en marcha y se respetan los controles, políticas y procedimientos internos; e
- identificar cualquier laguna del cumplimiento.

Los procesos y procedimientos de cumplimiento sobre privacidad se actualizarán para explicar:

- nuevas amenazas o riesgos para el negocio que se hayan identificado;
- cambios en las operaciones y actividades;
- cambios en las leyes de privacidad; y
- áreas de mejora basadas en los resultados de evaluaciones del riesgo, EIP, auditorías, reclamaciones, lecciones aprendidas de las iniciativas de respuesta ante incidentes y/u otros medios.

Gobierno**Oficina de Privacidad Global**

Crawford ha establecido una Oficina de privacidad global, Diseñada para desarrollar, gestionar e impulsar iniciativas de privacidad para toda la empresa. A alto nivel, la Oficina de privacidad global:

- Inicia y fomenta una cultura de privacidad dentro de Crawford
- Garantiza que la privacidad se incluye en las metas y objetivos empresariales
- Gestiona el cumplimiento en un entorno normativo complejo

La Oficina de privacidad global lleva a cabo lo anterior con aportaciones y colaboración de las diversas funciones de Crawford, como Legal, Oficina de Ética y Cumplimiento, y Tecnología de la Información y Seguridad de la Información.

Director de privacidad

El director de privacidad dirige la Oficina de privacidad global, tiene responsabilidad general y rinde cuentas sobre la privacidad en Crawford. Esto incluye:

- Desarrollar y mantener esta política y respaldar los procedimientos y políticas;

Política global de privacidad y protección de datos

- Establecer la dirección y prioridades para el programa de cumplimiento de la privacidad de Crawford, lo que incluye implementar objetivos de privacidad para toda la empresa; y
- Gestión de presupuestos y recursos (responsables de la protección de datos incluidos).

Los departamentos y líneas de servicios globales y las entidades locales son responsables de iniciar e implementar los objetivos de privacidad para toda la empresa tras ser acordados en consultas con el director de privacidad.

Responsables de la protección de datos y Responsables de la privacidad de datos

Crawford ha creado funciones adicionales con responsabilidad formal sobre el cumplimiento con las leyes de protección de datos en jurisdicciones y regiones específicas, según queda definido más adelante. Crawford designará las personas responsables para estas funciones. Estas personas son responsables ante el director de privacidad en relación con sus obligaciones relevantes para supervisar el cumplimiento con esta política, las políticas y procedimientos de protección de datos relevantes y las leyes de protección de datos aplicables.

Unión Europea

El responsable de la protección de datos es una función reglamentaria obligatoria conforme con las leyes de protección de datos de la UE bajo determinadas condiciones. Crawford establecerá una o más funciones de responsable de la protección de datos en la UE, con responsabilidad respecto de las leyes de protección de datos de la UE en una jurisdicción en concreto o en nombre del grupo Crawford.

- Responsable de la protección de datos del grupo. El responsable de la protección de datos del grupo en la UE es responsable de supervisar y asesorar sobre el cumplimiento por parte de Crawford con las Leyes de protección de datos en la UE, así como de colaborar en la actualización regular de los registros obligatorios de tratamiento, y proporcionar aportaciones sobre EIPD obligatorias. Un responsable de la protección de datos del grupo en la UE será miembro de la Oficina de privacidad global, y dependerá del director de privacidad, pero debe ser capaz de desempeñar de forma independiente sus obligaciones. El responsable de la protección de datos del grupo en la UE contará con el apoyo de los jefes de privacidad en las jurisdicciones relevantes de la UE.
- Responsable de protección de los datos del país. Se puede designar interna o externamente un responsable de protección de los datos de la UE específico del país, y será responsable del cumplimiento con la protección de los datos en una jurisdicción en concreto y rendirá cuentas ante el gerente nacional para esa jurisdicción.

Política global de privacidad y protección de datos

Cada responsable de protección de los datos de la UE que se designe estará sujeto a términos que garanticen su independencia e imparcialidad. La función del responsable de protección de los datos no es comercial, y el responsable de protección de los datos no debe encontrarse en una situación que pueda crear un conflicto de intereses (p. ej., mediante la asignación de responsabilidades adicionales). Cada responsable de protección de los datos en la UE tendrá independencia para llevar a cabo sus obligaciones reglamentarias, y para informar acerca de los asuntos relacionados con el cumplimiento con las leyes de protección de datos de la UE ante los niveles de gestión más altos, de la siguiente manera:

- El responsable de protección de los datos en la UE puede comunicar al equipo de gestión ejecutiva global asuntos relacionados con el cumplimiento con las leyes de protección de datos de la UE.
- Un responsable de la protección de datos de un país específico de la UE puede comunicar al director nacional para esa jurisdicción los asuntos relacionados con el cumplimiento con las Leyes de protección de datos en una jurisdicción en concreto.

La Oficina de privacidad mantendrá un registro actualizado de las personas designadas por el actual responsable de la protección de datos en la UE, y esto también debe divulgarse en los avisos de privacidad para interesados relevantes, y notificar a las autoridades de control pertinentes según requieran las Leyes de protección de datos de la UE aplicables.

Filipinas

Se requiere un responsable de la protección de datos filipino para cada entidad de Crawford en Filipinas. En Filipinas se puede designar a un responsable de la protección de datos para una o más entidades filipinas, y tendrá como responsabilidad supervisar el cumplimiento con las leyes de protección de datos de Filipinas y presentar cualquier registro necesario en conformidad con las leyes de protección de datos aplicables ante la Comisión Nacional de Privacidad de Filipinas. Se puede designar un responsable del cumplimiento para cada entidad en Filipinas para proporcionar apoyo al responsable de la protección de datos en Filipinas. La Comisión Nacional de Privacidad de Filipinas recibirá notificación sobre el actual responsable de la protección de datos para cada entidad filipina.

Canadá

El responsable de privacidad de los datos en Canadá será designado para una o más entidades canadienses según requieran las leyes de protección de datos de Canadá, y será responsable de supervisar el cumplimiento con las Leyes de protección de datos de Canadá.

Otras jurisdicciones

Política global de privacidad y protección de datos

Cuando lo exijan las leyes de protección de datos aplicables, Crawford designará cargos adicionales con responsabilidad formal sobre la protección de los datos y la privacidad en jurisdicciones concretas, que serán responsables ante el director de privacidad en relación con sus tareas pertinentes de supervisar el cumplimiento con la privacidad.

Responsables de privacidad en la UE

Se designará un responsable de privacidad para cada entidad de Crawford en la UE, para proporcionar apoyo al responsable de la protección de datos del grupo en la UE para recibir, revisar y responder a consultas y reclamaciones de clientes, interesados y autoridades de control, y llevar a cabo cualquier EIPD necesaria.

Coordinadores de privacidad

Salvo si la Oficina de privacidad global otorga una excepción, cada empresa afiliada y departamento global asignará un coordinador de privacidad que será responsable de ser un punto de contacto compartido entre la Oficina de privacidad global y su entidad o departamento, de identificar los problemas de cumplimiento sobre el terreno y remitirlos a la Oficina de privacidad global, y de ayudar a la Oficina de privacidad global para que pueda implementar iniciativas de privacidad. Los coordinadores de privacidad son responsables ante el director de privacidad en relación con sus responsabilidades pertinentes.

Un jefe de privacidad en la UE también puede ejercer como coordinador de privacidad.

Comité de asesoramiento sobre privacidad

El Comité de asesoramiento sobre privacidad es un grupo superior e interdisciplinario establecido para tratar asuntos sobre gestión y cumplimiento de la protección de datos que justifiquen una decisión o examen interdisciplinario. El Comité de asesoramiento sobre privacidad lo dirige el Director de privacidad, y entre los miembros se incluyen todos los Responsables de la privacidad de datos y los Responsables de la privacidad de datos, así como representantes de departamentos clave, incluyendo la Oficina de ética y cumplimiento, Legal, y Tecnología de la información y Seguridad de la información.

El Comité se reúne como mínimo una vez cada trimestre y depende del equipo de Gestión ejecutiva global. El Comité preparará un informe anual que se presentará ante el Consejo de administración de Crawford, o el comité designado, en el que se resumirán eventos significativos que tuvieron lugar durante el año natural anterior (p. ej., metas alcanzadas).

El Comité de asesoramiento sobre privacidad tiene expresamente permitido plantear ante el equipo de Gestión ejecutiva global, y cuando proceda ante el

Consejo de administración (o comité designado) de Crawford, según sea necesario, asuntos o comentarios relacionados con proyectos que pueden ser de alto riesgo o posibles casos de incumplimiento importantes.

Definiciones

“Cliente” significa un cliente actual, previo o posible de Crawford, y cualquier otra parte en nombre de la cual Crawford actúe bajo indicación de tal cliente.

“Datos personales de cliente” significa Datos personales que Crawford procesa (como procesador de datos) en nombre de sus clientes.

“Responsable del tratamiento” o **“Responsable”** hace referencia a la persona física o jurídica que, de manera individual o junto con otros, determina las finalidades y los medios del tratamiento de Datos personales.

“Procesador de datos” o **“Procesador”** significa la entidad o persona natural o legal que procese Datos personales en nombre del responsable.

“Leyes de protección de datos” significa, en la medida aplicable para Crawford, las leyes, reglas y normativas relacionadas con la protección de los datos y la privacidad o que de alguna forma rijan el tratamiento de Datos personales (lo que incluye las Leyes de protección de datos de la UE).

“Interesado” significa la persona con la que están relacionados los Datos personales.

“EEE” significa “Espacio Económico Europeo”.

“Leyes de protección de datos de la UE” se refiere a la Directiva 95/46/CE de la UE, según se incorpore a la legislación nacional de cada Estado miembro y según se modifique, sustituya o reemplace cada cierto tiempo, lo que incluye por el Reglamento General de Protección de los Datos (“RGPD”) 2016/679 de la UE y las leyes que implementen o sean complemento del RGPD, así como cualquier legislación de protección de datos sucesora del RGPD en el Reino Unido si el Reino Unido abandona la Unión Europea.

“Datos personales” significa cualquier información relacionada con una persona física identificada o identificable e incluye información en cualquier medio o formato, independientemente de si la información está cifrada. Una persona puede ser identificada directamente a través de, por ejemplo, su nombre, dirección, identificador de empleado, número de reclamación, dirección de correo electrónico, número de teléfono o identificador gubernamental. Una persona puede ser identificada indirectamente vinculando o combinando información adicional que puede estar o no bajo control o custodia de Crawford, con información bajo control o custodia de Crawford, como, por ejemplo, dirección de IP, dirección MAC, identificador de dispositivo, identificador biométrico o cualquier otro identificador único, información de ubicación geográfica, información genética o ADN.

“Violación de la seguridad” significa cualquier acceso o utilización, divulgación u otro procesamiento de Datos personales, no autorizado conocido o del que razonablemente se sospeche así como cualquier pérdida, robo o adquisición de Datos personales, o cualquier incidente que ponga en peligro la seguridad de los Datos personales.

“Personal” se refiere a todos los empleados, consultores y trabajadores no empleados a jornada completa, jornada parcial, temporales, regulares y bajo contrato.

“Proceso” significa toda operación o conjunto de operaciones realizadas con Datos personales o conjuntos de Datos personales, bien sea o no por medios automáticos, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, uso, divulgación por transmisión, difusión o cualquier otra forma de habilitación de acceso, armonización o combinación, limitación, supresión o destrucción, armonizarla, combinarla, bloquearla, borrarla o destrucción de los datos.

“Transferencia limitada” significa una transferencia de Datos personales por, entre, o para Crawford (lo que incluye cualquier entidad del grupo Crawford) cruzando fronteras nacionales que las leyes de protección de datos aplicables o acuerdos con clientes prohíban, en ausencia de las cláusulas contractuales tipo.

“Datos delicados” se refiere a Datos personales que se consideren delicados o que estén sujetos de alguna forma a normas de control más estrictas en virtud de las Leyes de protección de datos (lo que incluye “Categorías de Datos personales especiales” conforme a las leyes de protección de datos de la UE), y Datos personales que, si se divulgan o acceden sin autorización, podrían dar origen a robo de identidad o daños materiales financieros, físicos o para la reputación, además de incluir: raza u origen étnico, creencias religiosas o filosóficas, afiliación sindical, afiliación política, orientación sexual o vida privada, información sanitaria, tratamiento médico, información sobre discapacidad, información sanitaria protegida, salud mental, genética, biometría, números de tarjetas de crédito o cuentas financieras, datos de tarjetas de pago, número de la Seguridad Social o identificadores públicos, verificaciones de antecedentes o informes crediticios, y procedimientos o historial penal.

“Cláusulas contractuales tipo” significa:

- (a) para Datos personales sujetos a las Leyes de protección de datos de la UE, las cláusulas contractuales tipo de la UE para la transferencia de Datos personales a procesadores ubicados en terceros países, o cualquier sucesor de los mismos o mecanismo alternativo de transferencia de datos, reconocido por la Comisión Europea de conformidad con el RGPD (Artículos 44-46); y/o

Política global de privacidad y protección de datos

(b) para Datos personales sujetos a las Leyes de protección de datos que no sean las Leyes de protección de datos de la UE, otros equivalentes nacionales establecidos para garantizar una protección adecuada de las transferencias transfronterizas de Datos personales.

“**Subprocesador**” significa un proveedor designado por o en nombre de una entidad de Crawford (en su calidad de procesador de datos) que procesará Datos personales de clientes.

“**Autoridad de control**” Significa la autoridad de regulación pertinente en relación con las Leyes de protección de datos, incluyendo la autoridad de control según se define conforme a las Leyes de protección de datos de la UE.

“Proveedor”

procesador de (incluido un que proporcione a una entidad de entidad o persona entidad de

[Grab your reader’s attention with a great quote from the document or use this space to emphasize a key point. To place this text box anywhere on the page, just drag it.]

significa un datos externo subprocesador) bienes o servicios Crawford o a otra en nombre de una Crawford.

Contacto

El responsable de esta política es el Director de privacidad. Para obtener más información, póngase en contacto con la Oficina de privacidad global (privacy@global.crawco.com).

Información del documento

Nombre del documento	Política global de privacidad y protección de datos
Categoría	Política global
Documentos y políticas relacionadas	Política de gestión de Datos personales Política global de gestión de riesgo de terceros Política de respuesta ante incidentes Política de gestión de la información y registros Código de conducta y ética empresarial
Aprobado por	Elizabeth Alaniz, responsable jefe de privacidad
Versión n.º: Fecha de entrada en vigor	1.0 - Mayo de 2018