La Política de privacidad de datos de K-C del 25 de mayo de 2018 se aplica únicamente a los países de la UE. La Política de privacidad de datos existente del 1 de agosto de 2013 continúa aplicándose a todos los demás países hasta nuevo aviso.

Kimberly-Clark Corporation
POLÍTICA DE PRIVACIDAD DE LOS DATOS

Aplicable a partir del: 25 de mayo de 2018

PROPÓSITO

Es Política de Kimberly-Clark Corporation (incluidas sus filiales) ("**K-C**") proteger la privacidad de los datos personales y esta información contra el acceso, la divulgación, el uso, la modificación o la eliminación no autorizados. La presente Política de privacidad de los datos (la "**Política**") conforma las bases del programa de privacidad de K-C y se aplica a todas las empresas de K-C Group y a todo el personal a nivel mundial.

Esta Política establece los **Principios de privacidad de los datos** de K-C que todo el personal debe cumplir a la hora de procesar datos personales. También define las obligaciones de la Dirección en cada empresa de K-C Group a fin de implementar el programa de privacidad. Los Anexos a la presente Política incluyen instrucciones detalladas sobre cómo implementar el Programa global de privacidad de los datos de K-C.

CUMPLIMIENTO DE ESTA POLÍTICA

Las leyes de todo el mundo imponen responsabilidades a K-C para proteger y usar de forma lícita los datos personales que procesamos sobre nuestro personal, los consumidores, los socios comerciales y los proveedores de servicio. Además, en nuestro Código de conducta, nos comprometemos a manipular los datos personales de acuerdo con nuestras obligaciones contractuales y las leyes de protección de datos y privacidad aplicables.

El incumplimiento de nuestras responsabilidades podría tener como consecuencia importantes sanciones financieras, el daño de nuestra reputación y la confianza de los clientes, así como también posibles demandas. Por lo tanto, en todo momento, los datos personales deben gestionarse de acuerdo con las condiciones de la presente Política, sus Anexos y demás políticas, procedimientos, avisos y estándares relacionados.

Todo el personal que no cumpla con esta Política quedará sujeto a medidas disciplinarias, inclusive el despido.

LOS PRINCIPIOS DE LA PROTECCIÓN DE LOS DATOS DE K-C

Todo el personal debe cumplir con los 9 Principios de privacidad de los datos de K-C a la hora de procesar datos personales.

1.	**Equidad y transparencia:** K-C debe procesar los datos personales con equidad y brindar a las personas información sobre cómo y por qué se procesan sus datos personales.
2.	**Procesamiento lícito:** K-C solo debe procesar datos personales de forma lícita, incluidos los datos personales sensibles, de forma lícita en los casos que cuente con un fundamento legal válido.
3.	**Limitación de propósito:** K-C únicamente debe recopilar datos personales para un propósito específico, explícito y legítimo. Todo procesamiento subsiguiente deberá ser compatible con ese propósito, a menos que K-C haya obtenido el consentimiento de la persona o, de otro modo, el procesamiento esté permitido por la ley.
4.	**Minimización de datos:** K-C solo debe procesar los datos personales que sean adecuados, relevantes y se limiten a lo necesario para el propósito para el cual se recopilaron.
5.	**Precisión de los datos:** K-C debe implementar los pasos razonables para asegurarse de que los datos personales sean precisos, completos y, según sea necesario, se mantengan actualizados.
6.	**Derechos individuales:** K-C debe permitirles a las personas hacer ejercicio de sus derechos en relación con sus datos personales, incluidos los derechos de acceso y rectificación.
7.	**Limitación de almacenamiento:** K-C solo debe guardar datos personales durante el período que sea necesario para el propósito para el cual se recopilaron o para un propósito adicional permitido.

8.	**Seguridad de los datos:** K-C debe implementar las medidas de seguridad adecuadas a fin de proteger los datos personales, inclusive en los casos en que terceros procesan tales datos personales en nuestro nombre.
9.	**Responsabilidad:** K-C debe implementar los pasos a fin de cumplir, y poder demostrar el cumplimiento, con los Principios de la protección de los datos y el programa de privacidad de K-C Group.

PROCESOS DE DIRECCIÓN

A fin de garantizar que los Principios de privacidad de los datos de K-C Group se implementen en toda la empresa, K-C deberá mantener los siguientes procesos de Dirección como parte del programa de cumplimiento de la privacidad.

A. Políticas documentadas

K-C ha adoptado la presente Política y sus Anexos (los "**Documentos de privacidad de K-C**") a fin de poner en vigencia los Principios de la protección de los datos de K-C Group.

K-C deberá revisar periódicamente los Documentos de privacidad de K-C a fin de garantizar el cumplimiento continuo de los requisitos legales correspondientes.

B. Capacitación

K-C deberá mantener un programa de capacitación para asegurarse de que todo el personal que pueda tener acceso a los datos personales reciba la capacitación correspondiente al rol de la persona según los requisitos de los Documentos de privacidad de K-C.

Todo personal nuevo que tenga acceso a los datos personales deberá recibir la capacitación dentro de un período razonable tras la incorporación. Dicha capacitación deberá actualizarse de forma periódica.

C. Red de soporte global de privacidad de los datos

El equipo de Cumplimiento de K-C, junto con el equipo Jurídico de K-C, deberá supervisar y respaldar el programa de privacidad de K-C y el cumplimiento de las leyes de privacidad de los datos, y brindar asistencia a K-C con estos procesos de Dirección.

K-C ha designado una red de Líderes de privacidad de los datos en todo el mundo y que cumplen diferentes funciones comerciales a fin de ayudar con la implementación de los Documentos de Privacidad de K-C y la aplicación diaria del programa de privacidad. Los detalles de contacto de los Líderes de privacidad de los datos, junto con los detalles sobre el alcance de sus roles, puede encontrarse en la página de SharePoint del Programa global de privacidad de los datos (Global Data Privacy Program SharePoint). Los Líderes de privacidad de los datos recibirán la capacitación correspondiente y se les brindará los recursos adecuados para cumplir con su responsabilidad.

D. Evaluaciones del impacto de la protección de datos

Todo procesamiento que pueda tener como consecuencia un alto riesgo para los derechos de privacidad de los datos de las personas deberá estar sujeto a una Evaluación del impacto de la protección de datos (Data Protection Impact Assessment, **DPIA**) documentada, a fin de evaluar los riesgos asociados con el procesamiento propuesto e identificar toda protección que debería implementarse a fin de mitigar tales riesgos.

A continuación, se describe una lista no exhaustiva de las actividades de procesamiento que podrían considerarse de "alto riesgo" y que, probablemente, requerirán una DPIA:

- Introducción de un nuevo tipo de comprobación de antecedentes de los empleados.
- Realización de un monitoreo automatizado de las personas, incluido el circuito cerrado de televisión (CCTV) o el monitoreo del uso de equipo de TI por parte del personal.
- Iniciativas de comercialización minoristas que impliquen creación de perfiles, analítica, publicidad dirigida o segmentación.
- Presentación de un nuevo software que procesará los datos personales sobre el personal a gran escala.

Todo el personal será responsable de consultar con el Líder de privacidad de los datos correspondiente a fin de definir si se requiere una DPIA para un proyecto/una actividad de procesamiento en particular y, además, deberá participar en el proceso de la DPIA, según sea necesario. El equipo del Líder de privacidad de los datos llevará un registro centralizado de todas las DPIA. Con la aprobación del Líder de privacidad de los datos correspondiente, podrá realizarse una sola DPIA para un conjunto de operaciones de procesamiento similares en toda K-C.

Consulte el *Anexo 1 a la Política de privacidad y protección de datos de K-C (Evaluaciones del impacto de la protección de datos)* para obtener más información.

E. Mantenimiento de registros

Se deberá llevar un registro en nombre de cada empresa de K-C Group sobre sus actividades de procesamiento. Dicho registro deberá incluir una descripción general de lo siguiente:

- El propósito del procesamiento.
- Las categorías de datos personales y las personas con las cuales se relacionan dichos datos.
- Las categorías de destinatarios, incluidos los procesadores de datos personales (en caso de existir alguno), y toda transferencia fuera del Espacio Económico Europeo (European Economic Area, EEA).
- Cuando sea posible, el período de retención previsto de los datos personales.
- Cuando sea posible, una descripción general de las medidas de seguridad organizacionales y técnicas implementadas.

Cuando una empresa de K-C Group procese los datos personales en nombre de otra empresa de K-C Group (p. ej., si se brindan funciones de soporte de administración), K-C deberá llevar un registro de sus actividades como procesador de datos. Dicho registro deberá incluir una descripción general de lo siguiente:

- La identidad y los detalles de contacto de la otra empresa de K-C Group.
- Las categorías de procesamiento realizadas en nombre de la otra empresa de K-C Group.
- Toda transferencia fuera del EEA.
- Cuando sea posible, una descripción general de las medidas de seguridad organizacionales y técnicas implementadas.

Aquí podrá encontrar una plantilla de registro.

F. Privacidad por diseño

K-C deberá garantizar que toda actividad, herramienta o funcionalidad nueva de procesamiento de datos personales se diseñe y elabore de forma tal que permita cumplir con los Principios de la protección de los datos de K-C Group.

Consulte el *Anexo 4 a la Política de privacidad de los datos de K-C (Privacidad por diseño)* para obtener más información.

G. Gestión de quejas

K-C deberá tener un proceso para recibir y gestionar las consultas y quejas de las personas y las autoridades de protección de datos sobre el procesamiento de datos personales. Podrán aplicarse diferentes procesos para el personal (y el personal anterior), los consumidores, los clientes, los usuarios web y otros terceros. K-C deberá garantizar que se aborden todas las consultas y quejas de forma oportuna.

H. Garantía

K-C garantizará que su implementación de los Documentos de privacidad de K-C y el programa de privacidad esté sujeta a revisiones y auditorías periódicas, a fin de evaluar su cumplimiento interno.

INFORMACIÓN ADICIONAL

K-C podrá actualizar o modificar la presente Política de forma periódica. Esta Política no forma parte de ningún contrato de empleo del personal.

Podrá encontrar más información sobre esta Política y las obligaciones de K-C en la página de la intranet exclusiva aquí: página de SharePoint del Programa global de privacidad de los datos (Global Data Privacy Program SharePoint).

Para obtener más información sobre el programa de privacidad de K-C y los pasos que deben seguirse a fin de proteger los datos personales, o si tiene preguntas sobre el alcance legal permitido del uso y la divulgación de datos personales, comuníquese con la Línea de ayuda de K-C a la dirección KCHelpLine@kcc.com.

ANEXOS A LA PRESENTE POLÍTICA DE PRIVACIDAD Y PROTECCIÓN DE LOS DATOS

1. Evaluaciones del impacto de la protección de datos
2. Derechos individuales
3. Designación de Proveedores
4. Privacidad por diseño
5. Respuesta ante incidentes de datos
6. Comercialización
7. Datos del personal
8. Retención de datos
9. Modificaciones específicas de cada país

POLÍTICAS RELACIONADAS:

- Política de uso aceptable de los sistemas de TI
- Estándares de manejo y clasificación de información de TI
- Política de gestión de la seguridad de Proveedores: IT 115-01
- Estándar de gestión de Proveedores de seguridad: IT 240-01

APÉNDICE A: GLOSARIO

datos sin identificación	Datos que no se relacionan con ninguna persona identificada o identificable, o datos personales que se emitieron permanentemente de forma anónima de forma tal que ya no es posible identificar a la persona.
decisión automatizada	Decisión que genera un efecto legal, o un efecto similar significativo en la persona, y que depende solo del procesamiento automatizado (incluida la creación de perfiles) de sus datos personales (p. ej., sin ninguna intervención humana).
contralor	Parte que determinar los propósitos y los medios del procesamiento de datos.
datos	Toda información que se registre de forma electrónica o, si se registra en formato manual (p. ej., en papel), que se organiza en referencia a una persona.
sujetos de los datos	Persona con la cual se relacionan los datos personales, que podría ser, p. ej., un consumidor, un cliente, un empleado o un contacto comercial.
K-C Group	Kimberly-Clark Corporation y cualquiera de sus subsidiarias, que existan de manera periódica.
empresa de K-C Group	Todo integrante de K-C Group.
datos personales	Todos los datos que se relacionan con una persona identificada o con identificación (es decir, un ser humano). Pueden incluir, entre otros, nombres, direcciones de correo electrónico, fotografías, solicitudes laborales, historial de compras, información de cuentas, archivos de personal (en papel o formato digital), registros de salud ocupacional, opiniones y correspondencia enviada y recibida por una persona.
personal	Todos los empleados de KC de todos los niveles, incluidos directores, funcionarios, trabajadores de agencias, trabajadores tercerizados, voluntarios, pasantes, agentes, contratistas y consultores externos.
procesamiento	Toda operación realizada sobre los datos personales, como recopilación, registro, almacenamiento, recuperación, uso, combinación con otros datos, transmisión, divulgación y eliminación.
procesador	Parte que procesa los datos personales en nombre de un contralor, según las instrucciones del contralor.
datos personales sensibles	Datos personales que revelan o se relacionan con la raza o el origen étnico de una persona; opiniones políticas; creencias religiosas o filosóficas; participación sindical; información biométrica (p. ej., huellas digitales o reconocimiento facial) o genética; información sobre la salud, la vida sexual o la orientación sexual de la persona; delitos o condenas penales (incluidas las alegaciones).

ADENDA 1 DE LA POLÍTICA GLOBAL DE PRIVACIDAD DE DATOS DE K-C

EVALUACIONES DEL IMPACTO DE LA PROTECCIÓN DE DATOS

1. INTRODUCCIÓN

1.1 La Política de privacidad y protección de datos de K-C exige la realización de una Evaluación del impacto de la protección de datos (Data Protection Impact Assessment, "**DPIA**") cuando todo procesamiento de datos personales pueda generar "**alto riesgo**" para los derechos y las libertades de las personas.

1.2 Esta adenda define el proceso a seguir para ayudar a cumplir con esta obligación. Lo asistirá para: (a) decidir si se necesita una DPIA en algún caso en particular; y (b) realizar y registrar la DPIA.

1.3 **La PARTE 1** de la presente adenda se aplica a **todo el personal**. En ella se explica qué es una DPIA y se definen las circunstancias en las cuales un nuevo proyecto deberá enviarse al líder de privacidad de los datos correspondiente para que decida si es necesaria o no una DPIA completa. Al principio de cualquier proyecto nuevo que incluya datos personales, todo el personal deberá considerar si existe la posibilidad de generar procesamiento de datos de "alto riesgo".

1.4 **La PARTE 2** se aplica solo a los Líderes de privacidad de los datos (Data Privacy Champions, "**DPC**").

Consulte el Apéndice A de la Política global de privacidad de los datos de K-C para acceder a un Glosario de los términos que se definen en la presente adenda.

PARTE 1: APLICA A TODO EL PERSONAL

2. ¿QUÉ ES UNA DPIA?

2.1 Una DPIA es un proceso diseñado para evaluar el impacto que podría tener una actividad (o actividades) de procesamiento de datos en particular en la privacidad de las personas. La realización de una DPIA le permite a K-C decidir si esta se justifica en una actividad de procesamiento de datos en particular y determinar cómo hacerla de la manera más "respetuosa de la privacidad".

2.2 La DPIA consiste en identificar los beneficios de un proyecto propuesto, los posibles riesgos de privacidad y de protección de datos y toda salvaguarda que se haya implementado para mitigar esos riesgos. El líder de privacidad de datos que realice la DPIA podrá decidir si el proyecto continuará o si será necesaria alguna medida para mitigar cualquier riesgo de privacidad identificado. En algunos casos poco frecuentes, el líder de privacidad de los datos deberá consultar a la autoridad de protección de datos correspondiente antes de que el proyecto pueda continuar.

2.3 Todo el personal debe poder identificar cuándo se requiere una DPIA y tener la responsabilidad de colaborar con ella si el líder de protección de datos se lo solicitara. El líder de protección de datos deberá conocer detalles del proyecto, incluidos aquellos sobre el caso de negocios y la tecnología propuestas; por lo tanto, resulta esencial la cooperación de las unidades de negocios correspondientes.

3. ¿EL PROCESAMIENTO ES POTENCIALMENTE DE ALTO RIESGO?

3.1 Al principio de todo nuevo proyecto o actividad de procesamiento que incluya datos personales, todo el personal deberá considerar si existe la posibilidad de generar procesamiento de datos de "alto riesgo".

3.2 Los tipos de actividades que se describen a continuación se deberán tratar con el líder de protección de datos pertinente. Sin embargo, tenga en cuenta que son solo ejemplos de "disparadores de riesgo" y que no se trata de una lista exhaustiva. Se espera que el personal use su criterio para considerar si algún procesamiento nuevo puede ser de alto riesgo. Podrá usar el cuadro de mando de DPIA del Anexo 1 a modo de ayuda con esta evaluación. Si considera que una actividad puede ser de "alto

riesgo", deberá completar el formulario del Anexo 2 al presente Programa de Evaluaciones del impacto de la protección de datos y enviarlo al líder de privacidad de los datos correspondiente para que lo revise.

Actividad de procesamiento	Ejemplo
Evaluación o calificación, incluida la elaboración de perfiles y predicciones a partir de los datos sobre el comportamiento del sujeto en el trabajo, la situación económica, la salud, las preferencias personales o los intereses, la fiabilidad o la conducta, la ubicación o los movimientos.	– Uso de actividad de navegación en la web u otras interacciones con los clientes para evaluar las circunstancias sociales de un cliente (poder adquisitivo, estado familiar, etc.) con fines de marketing. – Iniciativas de marketing minorista que impliquen la elaboración de perfiles para permitir una optimización dirigida más enriquecedora (incluido el uso de público similar), la analítica, la publicidad dirigida y la segmentación. – Incorporación de datos, por ejemplo, unir los datos de nuestro programa de gestión de relación con los clientes (Customer Relationship Manager, CRM) con los datos obtenidos de fuentes externas para ayudarnos a crear perfiles más detallados de nuestros clientes. – Acceso y utilización de datos relacionados con patrones de compra de terceros, como empresas de tarjetas de crédito. – Utilización de datos de los dispositivos de las personas a fin de ayudar a predecir eventos de vida a los fines de la publicidad de comportamiento en línea o recomendaciones de productos.
Utilización de la toma de decisiones automatizada con efecto legal o significativo similar.	– Utilización de un programa automatizado para evaluar los CV en la selección.
Monitoreo sistemático.	– Instalación de circuito cerrado de televisión (Closed Circuit Television, CCTV) en las fábricas. – Implementación de tecnología de telemetría en los vehículos de entrega. – Monitoreo del uso de un sistema de tecnología de la información (Information Technology, IT) por parte del empleado (p. ej., software registrador de teclas, monitoreo del correo electrónico) o pruebas regulares de detección de drogas.
Recopilación de un nuevo tipo de datos personales sensibles o procesamiento de datos personales sensibles para un nuevo propósito.	– Permitir a los clientes agregar información de salud a sus cuentas.
Compartir datos personales sensibles con un tercero.	– Designar un proveedor de servicios externo que tendrá acceso a los datos de salud ocupacional del empleado.

Utilización de datos personales para un nuevo propósito.	– Presentación de una nueva forma de personalizar el servicio.
Toda nueva utilización o recopilación de datos de ubicación o información de la tarjeta de pago.	– Utilización de datos de ubicación capturados por un dispositivo propiedad de K-C a fin de medir la eficiencia del empleado.
Datos procesados a gran escala.	– Designación de un nuevo proveedor que tendrá acceso a todos los datos del consumidor de K-C.
Combinación de bases de datos que previamente se mantenían por separado.	– Combinación de los datos recopilados por *Huggies* con los datos recopilados por *Kleenex*.
Datos sobre sujetos vulnerables (p. ej., niños, personas mayores).	– Inicio de una campaña de marketing dirigida a adolescentes.
Uso innovador o aplicación de soluciones tecnológicas u organizacionales.	– Combinación del uso de reconocimiento facial y por huella digital para mejorar el control de acceso físico.
Transferencias de datos a través de las fronteras fuera de la UE.	– Designación de un proveedor de servicios en la India (p. ej., un proveedor de servicios en la nube o un centro de llamadas en el exterior).
Procesamiento que impida a los sujetos de los datos ejercer un derecho o usar un servicio o un contrato.	– Un proyecto que califique a los empleados por orden de desempeño, pero que no permita a los empleados acceder a la información.

Si aún tiene dudas, deberá comunicarse con el líder de privacidad de los datos pertinente. Puede que deban realizar su propia evaluación o podrán decirle de inmediato si la propuesta puede o no ser de alto riesgo potencial.

Los siguientes son ejemplos de actividades de procesamiento que ***poco probablemente*** sean de alto riesgo y, en la ausencia de circunstancias especiales, no requerirían una DPIA:

- Procesamiento del "negocio de forma habitual" que K-C ha implementado durante varios años, como el registro de los visitantes a las instalaciones de K-C, siempre que no exista un cambio significativo en el procesamiento.
- Procesamiento a medida de una pequeña cantidad de datos personales en respuesta a una solicitud específica por parte del sujeto de los datos (p. ej., en el contexto de una solicitud de muestra o una consulta similar).
- Divulgación u otro procesamiento de los detalles de contacto comercial del personal.

PARTE 2: SE APLICA SOLO A LÍDERES DE PROTECCIÓN DE DATOS

4. ¿EL PROCESAMIENTO ES DE "ALTO RIESGO"?

4.1 El siguiente paso del líder de protección de datos es decidir si es necesario realizar una DPIA, sobre la base de que el procesamiento **puede suponer un alto riesgo** para los derechos y las libertades de las personas. Se trata de una evaluación inicial a fin de determinar si se requiere un DPIA.

4.2 El líder de protección de datos deberá comprender los detalles clave del procesamiento propuesto a fin de realizar esta evaluación inicial. Como mínimo, usted deberá comprender:

- la naturaleza de los datos y los sujetos de los datos;
- la naturaleza, el alcance y el contexto del procesamiento;
- el propósito del procesamiento; y
- las identidades de las partes involucradas.

4.3 Es **obligatorio** que realice una DPIA en las siguientes circunstancias:

- Al tomar "decisiones automatizadas", las cuales se basan en la elaboración de perfiles o alguna otra evaluación sistemática de la conducta de la persona, p. ej., rastreo en línea o datos de geolocalización.
- Al procesar datos personales sensibles a "gran escala". El procesamiento será a "gran escala" si concierne a una parte significativa del personal o los clientes, y/o si concierne a una gran cantidad de datos (incluso si solo corresponden a una pequeña cantidad de personas), y/o si tiene lugar durante un período prolongado.
- Monitorear un espacio público (que no sea de forma individual).

4.4 Si bien usted deberá aplicar su criterio para determinar si el proyecto es de "alto riesgo", por lo general, cuanto más criterios (según se define en el párrafo 3.2 anterior) cumpla el procesamiento, más probabilidades tiene de presentar un alto riesgo para los derechos y las libertades de las personas, y por lo tanto requerirá una DPIA. Por regla general, un proyecto que cumpla menos de dos criterios no requerirá una DPIA debido al bajo nivel de riesgo, y los proyectos que cumplan, al menos, con dos de estos criterios requerirán una DPIA. Sin embargo, en algunos casos, un proyecto que cumpla solo con uno de estos criterios requerirá una DPIA. Si, luego de haber considerado los detalles clave del procesamiento propuesto, considera que es poco probable que el procesamiento propuesto suponga un alto riesgo para los derechos y las libertades de las personas, no será necesario que realice una DPIA. Si tiene alguna duda, deberá realizar una DPIA, que lo ayudará a aclarar su comprensión de los riesgos implicados.

4.5 Si decide no realizar una DPIA, deberá llevar un registro de la derivación, su decisión y los motivos de esta, y compartir este registro con el líder de privacidad de los datos pertinente, quien lleva un registro centralizado de las DPIA.

5. REALIZACIÓN DE LA DPIA

5.1 La DPIA deberá registrarse de forma que incluya todos los pasos anteriores. En el **Anexo 2**, se pone a su disposición un formulario modelo para que pueda usar. Al realizar una DPIA, deberá tener en cuenta los 9 principios de la protección de datos de la Política de privacidad y protección de datos de K-C.

5.2 Tenga en cuenta que, si bien siempre deberá completar todos los pasos, cada DPIA no siempre requerirá el mismo nivel de detalle. El alcance de la DPIA dependerá de la naturaleza del proyecto y de los riesgos implicados. Si se trata de un proyecto simple y no está seguro de si se necesita o no una DPIA, dicha DPIA puede ser relativamente breve. Por el contrario, una propuesta más grande, más complicada o más obviamente "riesgosa" probablemente requiera una DPIA más exhaustiva.

5.3 Deberá asegurarse de comprender las actividades de procesamiento propuestas, entre ellas:

- La naturaleza de los datos personales.
- La identidad de los sujetos de los datos y (aproximadamente) cuántos habrá.
- La naturaleza del procesamiento (es decir, qué se hará con los datos del personal).
- El propósito y los objetivos comerciales del procesamiento (es decir, por qué se propuso).

- La identidad y la ubicación de las partes, en particular si alguna se encuentra fuera del Espacio Económico Europeo (European Economic Area, EEA).

Quienes participen del proyecto, entre ellos, el propietario del negocio, los propietarios del sistema, los gerentes de proyectos, contratación e IT, deberán brindarle a usted esta información mediante la parte 1 del formulario del Anexo 2 del presente Programa de Evaluaciones del impacto de la protección de datos.

Paso (1): Identificar por qué fue necesario hacer la DPIA (es decir, por qué el procesamiento puede ser de alto riesgo). Básicamente, deberá explicar la decisión que tomó en la Sección 4 anterior.

Paso (2): Identificar el fundamento jurídico para el procesamiento en virtud de la ley de protección de datos.

En la mayoría de los casos, este será **uno** de los siguientes:

- Que K-C obtendrá el **consentimiento** de la persona de forma voluntaria e informada. Si los datos son datos personales sensibles, este consentimiento deberá ser **explícito**.
- Que el procesamiento sea **necesario para el cumplimiento de un contrato** con la persona (o los pasos precontractuales).
- Que el procesamiento sea necesario para respaldar los **intereses legítimos** de K-C, los cuales no se ven sobrepasados por ningún prejuicio hacia las personas. Si K-C confía en este fundamento, usted también debe especificar el interés legítimo (p. ej., aumento de las opiniones de los clientes, cobranza de deudas, garantizar la seguridad de la red y de la información). No puede basarse en este fundamento para procesar datos personales sensibles.

Identificar el fundamento jurídico lo ayudará a comprender los riesgos de privacidad y cómo protegerse de ellos. Si las personas pueden elegir de forma genuina si desean que sus datos personales se procesen para el proyecto (y entonces K-C podrá basarse en este consentimiento), usted podrá aceptar un nivel de riesgo más alto para esas personas que si no tuvieran esa opción.

Paso (3):

Identificar los riesgos de privacidad clave, es decir, los riesgos para los derechos y las libertades de los sujetos de los datos.
Deberá tener en cuenta las posibles amenazas que surjan del proceso. Entre los ejemplos se podrían encontrar:

- Menor control por parte de K-C respecto de cómo se utilizan los datos personales.
- Utilización o almacenamiento de datos imprecisos o desactualizados.
- Recopilación de datos excesiva o que no puede justificarse.
- Uso inadecuado o indebido de los datos.
- Destrucción o alteración de los datos.
- Un mayor riesgo de piratería o violación de seguridad.

Luego deberá evaluar la probabilidad y gravedad de cualquier daño que pudiera resultar del procesamiento. Entre los ejemplos se podrían encontrar:

- La identificación de robo, discriminación, fraude financiero o, simplemente, la exposición de información sensible sobre las personas si la información se hubiera hecho pública.
- Quejas o malestar en las personas.

También deberá registrar todo riesgo legal o comercial relacionado con K-C, como:

- Perjuicio en las relaciones con nuestros clientes.

- Mayor riesgo de investigación y/o sanciones por parte de alguna autoridad de protección de datos.
- Riesgo de atención negativa de parte de los medios de comunicación.
- Situación vergonzosa para K-C.

Paso (4): Identificar las salvaguardas necesarias que se deberán implementar a fin de abordar los riesgos que haya identificado en el Paso 4.

Esto requerirá que consulte con las partes interesadas pertinentes, a fin de garantizar que las salvaguardas propuestas sean viables comercialmente. A la hora de evaluar las salvaguardas apropiadas, deberá considerar los riesgos identificados en el Paso 3, el costo de la implementación de las medidas y su efectividad, así como su impacto en el propósito para el cual se realice el procesamiento. Cuando sea posible, deberá esquematizar cada riesgo a una salvaguarda a fin de asegurarse de abordar todos los riesgos. También deberá explicar de qué manera la salvaguarda mitiga ese riesgo (p. ej., mediante el cifrado de datos puede mitigar el riesgo de una violación de seguridad debido a que no se podrá acceder a los datos de forma significativa).

Tenga en cuenta que no tiene que eliminar necesariamente los riesgos por completo; el punto crítico es minimizar el riesgo en la mayor medida razonablemente posible, considerando el (los) propósito(s) identificado(s) en el Paso 1, la tecnología disponible y dentro de parámetros económicos razonables.

Algunos ejemplos de estos tipos de protecciones de seguridad que debe considerar incluyen:

- Implementar medidas de seguridad adecuadas, p. ej., cifrado, controles de acceso, cortafuegos, medidas de seguridad cibernética y medidas de seguridad física.
- Evaluar si es posible utilizar datos anónimos o seudónimos.
- Garantizar transparencia a los sujetos de los datos (¿K-C debe enmendar su Aviso de privacidad en línea o crear un nuevo aviso?)
- Implementar un enfoque de "privacidad por diseño" (¿de qué forma puede diseñarse la solución para abordar las inquietudes de privacidad?) (Consulte la *Adenda 4 de la POLÍTICA GLOBAL DE PRIVACIDAD DE LOS DATOS DE K-C [Privacidad por diseño]* para conocer más detalles).
- Considerar ofrecer una "opción de exclusión" o un enfoque basado en el consentimiento.
- Garantizar la implementación de salvaguardas contractuales sólidas con terceros.
- Garantizar que existan períodos de retención definidos para los datos, transcurrido el cual la información deberá eliminarse o anonimizarse.

Identifique los puntos de acción necesarios para implementar cada protección. Deberá asignar un propietario para cada punto y definir hitos para su implementación. Esto deberá realizarse en consulta con las partes interesadas pertinentes.

Paso (5): Evaluar la necesidad y proporcionalidad del procesamiento, en vistas del propósito que se prevé lograr.

Considere por qué K-C debe realizar el procesamiento y si existe algún método con menor impacto que pueda usarse en su lugar. Considere la proporcionalidad entre el riesgo o perjuicio identificado en el Paso 3 y los propósitos, intereses o beneficios que se persiguen, según lo identificado en el Paso 1. Los puntos que se deben tener en cuenta incluyen:

- ¿Cuáles son los beneficios para las partes interesadas, incluidos los sujetos de los datos o K-C? ¿Son suficientes para justificar los riesgos?
- ¿Podríamos lograr el mismo resultado con información anónima?
- ¿Debemos recopilar datos personales adicionales o podemos usar información que ya hemos recopilado? (Nota: antes de usar los datos existentes, deberá considerar cómo esperarían las personas que se use esta información)

PASO CRÍTICO: ¿Es posible continuar con el proyecto?

En esta etapa, puede decidir que los riesgos asociados con el proyecto pueden implicar no continuar de la forma actual. Si K-C no puede implementar salvaguardas suficientes para mitigar cualquier riesgo de privacidad, tiene la obligación de consultar a la autoridad de protección de datos pertinente y, en última instancia, no se podrá continuar con el proyecto.

Deberá consultar al líder de privacidad de los datos pertinente si no considera que los riesgos de privacidad puedan mitigarse de forma adecuada y el proyecto continúa siendo de "**alto riesgo**".

Paso (6): Verificar que el registro de la DPIA incluya con precisión todos los detalles de su evaluación y el resultado.

Luego deberá enviar una copia al líder de privacidad de los datos pertinente para que se guarde en un registro central.

Deberá tener en cuenta que el líder de privacidad de los datos pertinente podrá realizar "controles al azar" regulares de las DPIA a fin de confirmar que se hayan completado todos los puntos de acción identificados en la DPIA.

Las preguntas sobre esta adenda pueden remitirse a KC HelpLine en KCHelpLine@kcc.com.

ANEXO 1 A LA ADENDA 1 DE LA POLÍTICA GLOBAL DE PRIVACIDAD DE LOS DATOS DE K-C

https://archer.kcc.com/

ANEXO 2 A LA ADENDA 1 DE LA POLÍTICA GLOBAL DE PRIVACIDAD DE LOS DATOS DE K-C

PLANTILLA DE EVALUACIÓN DEL IMPACTO DE LA PROTECCIÓN DE DATOS

<table>
<tr><th colspan="6">PARTE 1: APLICA A TODO EL PERSONAL</th></tr>
<tr><td colspan="6">Equipo de la DPIA, resumen del proyecto y descripción del procesamiento</td></tr>
<tr><th colspan="2">Equipo de la DPIA</th><th>Nombre</th><th>Cargo</th><th colspan="2">Dirección de correo electrónico</th></tr>
<tr><td>1.</td><td>Gerente de proyectos de K-C que posee la DPIA</td><td></td><td></td><td colspan="2"></td></tr>
<tr><td>2.</td><td>Otros gerentes de proyecto de K-C que ayudan a realizar la DPIA</td><td></td><td></td><td colspan="2"></td></tr>
<tr><td>3.</td><td>Líder de protección de datos</td><td></td><td></td><td colspan="2"></td></tr>
<tr><th colspan="6">Resumen del proyecto</th></tr>
<tr><td>4.</td><td colspan="2">Nombre del proyecto</td><td colspan="3"></td></tr>
<tr><td>5.</td><td colspan="2">Descripción y objetivos del proyecto
Describa el proyecto y lo que pretende lograr. Describa los beneficios para la empresa de K-C Group y/o las personas u otras partes relevantes. Siéntase libre de adjuntar o colocar un enlace de cualquier otro documento relevante relacionado con el proyecto, por ejemplo, una propuesta de proyecto.</td><td colspan="3"></td></tr>
<tr><td>6.</td><td colspan="2">Fecha de implementación del proyecto</td><td colspan="3"></td></tr>
<tr><th colspan="6">Descripción del procesamiento</th></tr>
<tr><td>7.</td><td colspan="3">Describa los datos personales que podrán procesarse</td><td colspan="2"></td></tr>
<tr><td></td><td>☐ Nombre
☐Detalles de contacto profesional (teléfono, dirección de correo electrónico o dirección laboral)
☐Información de contacto personal (teléfono, dirección de correo electrónico, dirección particular)
☐ Cargo
☐ Lugar de trabajo
☐ Número de identificación nacional</td><td>☐ Información financiera
☐ Salario
☐ Fecha de nacimiento
☐ Año de nacimiento
☐ Credenciales de inicio de sesión
☐ Fotografía
☐ Sexo
☐ Información educativa
☐ Interacciones profesionales, redes,</td><td>☐ Número de identificación único (p. ej., número de empleado o cliente)
☐ Valoraciones y evaluaciones
☐ Datos relacionados con la condición migratoria
☐ Datos de la licencia de conducir
☐ Calificaciones profesionales
☐ Interacciones en redes sociales</td><td colspan="2">☐ Datos relacionados con la raza o el origen étnico
☐ Opinión política
☐ Creencias religiosas o creencias de una naturaleza similar
☐ Afiliación sindical
☐ Afecciones de salud mental o física (incluidos los datos genéticos)
☐ Vida sexual
☐ Delitos penales
☐ Datos biométricos</td></tr>
</table>

	☐ Información del pasaporte	membresías y participaciones	☐ Interacciones, hábitos y preferencias de navegación en internet ☐ Otros, especifique: ……	☐ Otros datos que considere sensibles, por favor especifique: ……
8.	¿Sobre quién recopilará datos personales?			
	☐ Empleados ☐ Contratistas ☐ Socios comerciales ☐ Clientes comerciales ☐ Consumidores		☐ Participantes de investigaciones de mercado y cuestionarios ☐ Niños ☐ Visitantes al sitio web ☐ Otros, por favor especifique: ……	
9.	¿Qué cantidad de datos personales sobre las personas se procesará (puede incluir una aproximación)?		Por favor especifique: ……	
10.	¿El proyecto involucrará a proveedores de servicios externos? Si la respuesta es sí, brinde detalles.		☐ Sí; por favor especifique: …… ☐ No	
11.	¿El proyecto tendrá como resultado el almacenamiento de datos personales en un país ubicado fuera de la UE o el Reino Unido, o el acceso a los mismos desde esos lugares? Por ejemplo, designación de un proveedor de servicios en la India (p. ej., un proveedor de servicios en la nube o un centro de llamadas en el exterior). Si la respuesta es sí, por favor especifique dónde.		☐ Sí; por favor especifique dónde: …… ☐ No	

PARTE 2: SE APLICA SOLO A LÍDERES DE PROTECCIÓN DE DATOS **La información sobre cómo completar cada "paso" que se menciona a continuación deberá considerarse junto al párrafo 5 del *Programa de las Evaluaciones del impacto de la protección de datos.***		
1.	**¿Es necesario realizar una DPIA? *(paso 1)***	
	☐	Sí; por favor brinde sus motivos: ……
	☐	No; brinde sus motivos y asegúrese de compartir esta parte 2 con el responsable de Cumplimiento de Europa, Oriente Medio y África (Europe, Middle East and Africa, EMEA): ……
2.	**¿Cuál es el fundamento jurídico para el procesamiento? *(paso 2)***	
	Datos personales	
	UE	
	☐	El sujeto de los datos ha otorgado su **consentimiento** para el procesamiento de sus datos personales para uno o más de los propósitos específicos.
	☐	El procesamiento es necesario para **cumplir con un contrato** del cual el sujeto de los datos forma parte o a fin de tomar medidas a pedido del sujeto de los datos antes de celebrar un contrato.
	☐	El procesamiento es necesario para cumplir una **obligación legal** de la cual el contralor es sujeto.
	☐	El procesamiento es necesario para proteger los **intereses vitales** del sujeto de los datos o de otra persona física.
	☐	El procesamiento es necesario para desempeñar una tarea realizada para el **interés público** o en el ejercicio de la autoridad oficial que se confirió al contralor.
	☐	El procesamiento es necesario a los fines de los **intereses legítimos** perseguidos por el contralor o por un tercero, excepto cuando tales intereses queden anulados por los intereses o los derechos y libertades fundamentales del sujeto de los datos, los cuales requieren la protección de los datos personales, en particular, cuando el sujeto de los datos sea un niño.
	☐	**Otros** fundamentos jurídicos según la legislación local. Por favor especifique: ……
	Fuera de la UE	
	☐	Especifique el fundamento jurídico (en virtud de la ley local) del procesamiento propuesto: ……
	Datos personales sensibles (o "especiales")	
	UE	
	☐	El sujeto de los datos ha otorgado su **consentimiento explícito** para el procesamiento de los datos personales para uno o más de los propósitos específicos.
	☐	El procesamiento es necesario a los fines de cumplir con las obligaciones y ejercer los derechos específicos del contralor o del sujeto de los datos en el **campo del empleo y de la seguridad social, como también la ley de protección social** en la medida que se cuente con la autorización de la Unión o la ley de Estados Miembros, o conforme a un acuerdo colectivo en virtud de la ley de Estados Miembros que brinden las salvaguardas adecuadas de los derechos fundamentales y los intereses del sujeto de los datos.
	☐	El procesamiento es necesario para proteger los **intereses vitales** del sujeto de los datos u otra persona física cuando el sujeto de los datos esté impedido física o legalmente para dar su consentimiento.
	☐	El procesamiento se relaciona con los datos personales que el sujeto de los datos **manifiestamente hace públicos**.

	☐	El procesamiento es necesario para presentar, ejercer o defenderse de **reclamaciones legales**, o cuando los tribunales actúen en su capacidad jurídica.
	☐	El procesamiento es necesario con fines **de interés público significativo**, sobre la base de la Unión o la ley de Estados Miembros, que deberán ser adecuados según el propósito deseado, para respetar la esencia del derecho a la protección de los datos y brindar las medidas adecuadas y específicas para proteger los derechos fundamentales y los intereses del sujeto de los datos.
	☐	El procesamiento es necesario a los fines de la medicina preventiva u ocupacional, para la **evaluación de la capacidad de trabajo del empleado**, el diagnóstico médico, el suministro de tratamiento o atención social o de salud o la administración de los servicios y sistemas de atención social o de salud con base en la Unión o la ley de Estados Miembros o conforme al contrato con un profesional de la salud.
	☐	El procesamiento es necesario a fines de archivado en el interés público, **de investigación científica o histórica o estadísticos** con base en la Unión o la ley de Estados Miembros, que deberán ser adecuados según el propósito deseado, para respetar la esencia del derecho a la protección de los datos y brindar las medidas adecuadas y específicas para proteger los derechos fundamentales y los intereses del sujeto de los datos.
	☐	**Otros** fundamentos jurídicos según la legislación local. Por favor especifique: ……
	Fuera de la UE	
	☐	Especifique el fundamento jurídico (en virtud de la ley local) del procesamiento propuesto: ……

3.	**¿Cuáles son los riesgos de privacidad (y otros riesgos asociados) del proyecto *(paso 3)* y qué salvaguardas o medidas propone usted para eliminar o reducir el riesgo *(paso 4)*?**				
	Riesgo de privacidad, riesgo organizacional asociado, riesgo corporativo	**Salvaguardas o acciones propuestas**	**Resultado: ¿las salvaguardas o medidas propuestas eliminan o reducen el riesgo o el riesgo es aceptable?**	**¿Quién es responsable de implementar las salvaguardas o medidas propuestas?**	**Plazo máximo para implementar las salvaguardas o medidas propuestas**
4.	**¿El procesamiento de datos es necesario y proporcionado en vista de los objetivos del proyecto *(paso 5)*?**				
5.	**¿Es necesario consultar a la autoridad de protección de datos pertinente? Brinde sus motivos para cualquier decisión *(paso 5)*.**				
6.	**Aprobación de la DPIA *(paso 6)***				
		Nombre en letra imprenta	**Firma**	**Fecha**	**Notas del responsable de Cumplimiento de EMEA**
	Gerente de proyectos de K-C que posee la DPIA				
	Líder de protección de datos				

Asegúrese de que la DPIA completada se guarde exitosamente en Archer.

ADENDA 2 DE LA POLÍTICA GLOBAL DE PRIVACIDAD DE LOS DATOS DE K-C

DERECHOS INDIVIDUALES

1. INTRODUCCIÓN

a. El principio 6 de la Política global de privacidad de los datos de K-C Group exige que todas las empresas de K-C Group les permitan a las personas ejercer derechos que puedan tener en virtud de la ley de protección de datos aplicable respecto del acceso, la eliminación, la rectificación, la objeción y la portabilidad de sus datos personales.

b. En esta adenda se brindan detalles adicionales sobre cómo cada empresa de K-C Group debe facilitar a las personas el ejercicio de sus derechos mediante el autoservicio y cómo responder a las solicitudes más complejas y específicas de las personas para ejercer sus derechos.

c. Consulte el Apéndice A de la Política global de privacidad de los datos de K-C Group para acceder a un Glosario de los términos definidos en esta adenda.

2. DESCRIPCIÓN GENERAL

Las personas de determinadas jurisdicciones tienen numerosos derechos en virtud de la ley de protección de los datos, entre ellos:

(i) **Acceso:** las personas tienen derecho a conocer qué datos personales K-C procesa sobre ellos y a solicitar una copia de tales datos personales.

(ii) **Rectificación:** las personas tienen derecho a que se corrijan los datos imprecisos y/o a que se completen los datos incompletos con información suplementaria.

(iii) **Objeción:** en algunas circunstancias, las personas tienen derecho a objetar la utilización de sus datos personales para un propósito en particular, por ejemplo, para enviarles marketing directo, elaborar perfiles de clientes o tomar decisiones automatizadas.

En determinadas circunstancias, las personas también podrán tener los siguientes derechos:

(iv) **Portabilidad:** las personas tiene derecho a recibir los datos personales *que proporcionaron* a K-C en un formato legible por una máquina de uso habitual, para que puedan compartilos con otra organización. Si bien es muy poco probable que K-C reciba tales solicitudes debido a la naturaleza del negocio, ocasionalmente K-C podrá verse obligada a compartir tales datos personales de forma directa con el tercero.

(v) **Eliminación:** a veces denominado “derecho al olvido”, las personas tienen derecho a solicitar que se borren sus datos personales si K-C no tiene un fundamento lícito para continuar procesando los datos. En algunos casos o para algunos tipos de datos personales, K-C podrá decidir no eliminar los datos sino restringir el uso (por ejemplo, a fin de que puedan utilizarse en caso de una reclamación judicial).

3. AUTOSERVICIO

Siempre que sea posible, K-C deberá permitir a las personas ejercer estos derechos mediante el **autoservicio**, sin la necesidad de presentar una solicitud específica a K-C. En consecuencia, K-C deberá intentar diseñar sus sistemas orientados hacia el usuario para que consumidores, empleados y usuarios de la web puedan, por iniciativa propia:

- observar los datos personales que K-C procesa sobre ellos;
- corregir toda información que sea imprecisa y actualizar toda información desactualizada;
- cambiar la configuración de su cuenta para que sus datos personales dejen de usarse para un propósito específico (p. ej., tener la opción de exclusión de las actividades de marketing); y

- eliminar toda información a la que deseen que K-C ya no tenga acceso.

El acceso a estos sistemas orientados al usuario debe estar sujeto a mecanismos de autenticación adecuados.

Al permitirles a las personas ejercer sus derechos mediante el autoservicio, K-C les otorgará mayor control de sus propios datos personales, acelerará el proceso por el cual los individuos puedan ejercer sus derechos y reducirá la carga para K-C.

Sin embargo, no siempre será posible que las personas ejerzan sus derechos mediante el autoservicio, por ejemplo, si sus datos personales no se almacenan en un sistema orientado al usuario. Por consiguiente, las personas también tienen derecho a **realizar una solicitud oral o por escrito** a K-C para ejercer sus derechos. Las solicitudes de las personas a K-C para ejercer estos derechos se denominan "Solicitudes de derechos individuales" (Individuals Rights Requests, **IRR**). En la parte restante de esta adenda se describe información adicional sobre cómo K-C puede cumplir con sus obligaciones con respecto a las IRR.

La PARTE 1 de la presente adenda se aplica a **todo el personal**. Explica en qué consiste una IRR y los pasos iniciales que debe seguir si cree que recibió una IRR.

La PARTE 2 se aplica solo al personal responsable de responder las IRR en nombre de K-C, como los Líderes de privacidad de los datos.

PARTE 1: APLICA A TODO EL PERSONAL

1. ¿QUÉ ES UNA SOLICITUD DE DERECHOS INDIVIDUALES (IRR)?

1.1 En términos generales, cualquier solicitud de una persona respecto de sus datos personales es una IRR. Las IRR pueden recibirse por teléfono, correo electrónico y correo postal. Las IRR también pueden realizarse a través de redes sociales o de forma oral a un miembro del personal; sin embargo, siembre debemos alentar a las personas a presentar cualquier IRR por escrito. No es necesario que la solicitud haga referencia a la ley de protección de los datos o los "datos personales". Sin embargo, las IRR no deben confundirse con las consultas de servicio normales y del día a día de los clientes.

1.2 Tal como se resumió brevemente con anterioridad, si K-C debe cumplir o no con una solicitud variará según el derecho que se ejerza. Las condiciones específicas de cada derecho se analizan más en detalle a continuación. En algunos casos, es posible que la persona busque ejercer más de un derecho y que K-C pueda cumplir con un aspecto de la solicitud (p. ej., otorgar acceso), pero no con otro (p. ej., eliminación).

1.3 K-C debe responder una IRR en el plazo de **un mes**. Si la solicitud es particularmente complicada, este plazo podrá extenderse a **dos meses**, pero K-C aún deberá responder al solicitante en el plazo de un mes y explicar por qué es necesaria la extensión. Por este motivo, es muy importante llevar un registro de la fecha en la que se recibió la IRR. En el Anexo 1 a la presente adenda, se ofrece una carta modelo para este propósito.

Tenga en cuenta que K-C NO tiene derecho a cobrar ningún honorario por manejar las solicitudes, salvo en las siguientes circunstancias excepcionales:

- si la persona solicita más de una copia de los datos personales; y
- si una solicitud es manifiestamente infundada o excesiva, por ejemplo, debido a que K-C haya respondido a una solicitud idéntica en los últimos dos meses y no se recopiló ningún dato personal nuevo en ese plazo. En estas circunstancias, K-C podrá decidir cobrar un honorario razonable o negarse a cumplir con la solicitud.

Es importante tener en cuenta que, el solo hecho de que una IRR sea de gran alcance (es decir, si una persona solicita copias de "todos" sus datos personales) no necesariamente significa que la IRR será considerada "excesiva" de forma automática.

Todo honorario deberá basarse en los costos administrativos razonables del suministro de la información (o tomar cualquier otra medida que se solicite). En ningún caso, el honorario deberá exceder el monto máximo que puede cobrarse conforme a la ley.

2. PASOS A SEGUIR EN CASO DE RECIBIR UNA IRR

PASO (1): CONFIRMAR LA IDENTIDAD DEL SOLICITANTE Y RESOLVER LA SOLICITUD DE MANERA INFORMAL

Antes de tomar cualquier medida en relación con una IRR, usted debe asegurarse de que provenga del sujeto de los datos o una persona autorizada para actuar en su nombre.

Existen diversas formas de comprobar la identidad del solicitante, tales como pedir información que solo el sujeto de los datos conocería (p. ej., sus preferencias de suscripción de alertas por correo electrónico o el historial de postulaciones de trabajo, en caso de que existieran), llamar por teléfono a la persona, solicitar una identificación (como una copia de la tarjeta de identidad nacional o del pasaporte) o preguntar el domicilio o el número de teléfono, etc. Si el solicitante no es el sujeto de los datos, pero actúa en su nombre, usted deberá solicitar un poder u otra prueba de autorización. Puede pedir al solicitante que complete el formulario del Anexo 2, en particular si considera que la IRR parece muy extensa o si tiene dudas respecto de la identidad del solicitante.

No deberá solicitar más información que la mínima razonablemente necesaria para identificar al solicitante. Si el solicitante es personal de K-C, usted no necesitará información adicional para verificar su identidad.

SOLICITUDES ORALES

Las IRR pueden realizarse de forma oral (p. ej., a un centro de llamadas o al personal de K-C en persona). Si la IRR se recibió de forma oral, usted deberá consultar al solicitante si realizará la solicitud por escrito (p. ej., completando el formulario del Anexo 2 a esta adenda). Usted no podrá insistir con esto ni tampoco puede negarse a responder a las IRR que solo se hagan de forma oral. Sin embargo, deberá explicar al solicitante que es más sencillo responder a las solicitudes por escrito y que ello podría significar que la respuesta se trate más rápidamente. Realizar la solicitud por escrito también puede ayudarle a usted a verificar la identidad del solicitante, ya que puede pedirle que incluya una copia de su documentación de identidad junto con la solicitud.

Si la persona se niega a realizar su solicitud por escrito, K-C deberá enviar a la persona una comunicación escrita lo antes posible a fin de confirmar la naturaleza y el alcance de su solicitud.

Resolución de la solicitud "informalmente"

A menudo, cuando la solicitud es muy simple y siempre que se verifique la identidad del solicitante con anticipación, podría ser más sencillo ayudar al solicitante de una manera más informal sin tener que seguir el procedimiento definido en la presente adenda. Si es posible responder a la consulta del solicitante rápidamente, sin escalar aún más el asunto, es más probable que K-C pueda limitar el alcance de la solicitud. Las IRR formales a menudo generan una carga mayor en términos de recursos y también pueden exponer al Grupo a un mayor riesgo de quejas regulatorias.

A modo de ejemplo práctico, si un cliente se comunica a un centro de llamadas y solicita una copia de un solo correo electrónico (p. ej., una carta de queja que hubiera enviado con anterioridad, pero que hubiera eliminado por accidente, es preferible que servicio al cliente simplemente reenvíe el correo electrónico (siempre y cuando el agente pueda estar seguro de la identidad de la persona). Al escalar la solicitud a un proceso formal, existe el riesgo significativo de que la persona amplíe el alcance de su solicitud (por ejemplo, solicitar copias de "todas las comunicaciones"). Claramente, a K-C le resulta mucho más oneroso cumplir con esta solicitud.

En consecuencia, siempre que sea posible, se debe intentar cumplir con las solicitudes informales y evitar convertirlas en solicitudes de derechos formales.

SOLICITUDES DE RECTIFICACIÓN

Como regla general, debería ser posible resolver las solicitudes de **rectificación** en una etapa informal. Puede hacer esto mediante la corrección del registro original o la incorporación de una declaración complementaria al registro. Por ejemplo, la solicitud de una muestra de un producto *Depend* podría no haberse entregado debido a una dirección inexacta en los archivos. Siempre que pueda verificar la identidad del solicitante, debería ser posible cumplir con la solicitud sin escalarla aún más.

Si tiene alguna inquietud sobre una solicitud de rectificación, deberá reenviar la solicitud al líder de privacidad de los datos correspondiente.

PASO (2): INFORMAR AL LÍDER DE PRIVACIDAD DE LOS DATOS

Si recibe una IRR que no pueda resolverse de manera informal o que fuera presentada por un miembro del personal de K-C, deberá informar de inmediato al líder de privacidad de los datos pertinente, inclusive si aún intenta resolver la solicitud de manera informal. Si la IRR se relaciona con información laboral, usted **siempre** deberá informar al líder de privacidad de los datos pertinente y al compañero de Recursos Humanos (HR Business Partner, **HRBP**), ya que a menudo estos tipos de solicitudes son más complicadas.

Si bien el líder de privacidad de los datos (y el HRBP, si correspondiera) asumirá el control del manejo de la respuesta a la IRR, usted deberá brindar asistencia y cooperación plenas cuando se soliciten; esto podría incluir asistir en la localización de los datos personales pertinentes, brindar detalles del contexto de la IRR o de la relación con las personas.

PARTE 2: APLICA SOLO A LOS LÍDERES DE PRIVACIDAD DE LOS DATOS (Y HRBP, SI CORRESPONDIERA)

Toda referencia a "usted" en la Parte 2 de esta adenda representa a cualquier líder de privacidad de los datos, cuyos detalles de contacto se encuentran en el Sitio global de SharePoint acerca de la privacidad de los datos.

PASO (3): ¿LA IRR ES CLARA?

El siguiente paso para usted consiste en evaluar si la solicitud incluye información suficiente a fin de poder comprenderla y considerarla. ¿Es suficiente para usted poder encontrar los datos personales que solicita la persona? Si la IRR es demasiado general o poco clara, deberá solicitar de inmediato a la persona que aclare su solicitud a fin de poder cumplirla.

PASO (4): IDENTIFICAR LA INFORMACIÓN

El siguiente paso consiste en identificar qué sistemas y bases de datos pueden incluir información relacionada con la persona y las unidades de negocios responsables de esos sistemas y bases de datos.

Esto dependerá de la naturaleza de la información solicitada. Sin embargo, es posible que usted y la(s) unidad(es) de negocio pertinente(s) deba(n) trabajar con Tecnología de la información (Information Technology, IT) a fin de identificar los sistemas o las bases de datos relevantes donde se alojan los documentos y la información en formato electrónico.

Las unidades de negocios responsables de cada uno de estos sistemas y/o bases de datos deberán realizar búsquedas de toda información que se relacione con la persona. Una vez que la unidad de negocios pertinente haya completado estas búsquedas, esa unidad de negocios deberá suministrarle a usted una copia de toda la información identificada.

PASO (5): ¿K-C TIENE LA OBLIGACIÓN DE CUMPLIR CON LA SOLICITUD (POR COMPLETO O EN PARTE)?

Existen diferentes excepciones legales que indican que K-C no tendrá la obligación de acceder a las IRR respecto de cierta información, por ejemplo, si se tratara de información legalmente privilegiada.

Esto dará lugar a la creación de un subconjunto de información (o, en algunos casos, ninguna información en absoluto).

Si considera que podría aplicarse alguna excepción, deberá consultar al Departamento Legal, ya que esto puede ayudar a reducir el tiempo dedicado a la revisión de la información, según el paso 6 a continuación**.**

PASO (6): REVISIÓN DE LA INFORMACIÓN PARA IDENTIFICAR DATOS PERSONALES

Una vez que haya recibido la información de las unidades de negocios correspondientes, deberá revisarla a fin de identificar todos los datos personales que se relacionen con el solicitante. Por regla general, deberá intentar identificar información ya sea de carácter biográfico sobre la persona o que tenga a la persona como su eje central.

Como parte de esta revisión, también deberá marcar toda información que K-C no desee divulgar fuera de la empresa, por ejemplo, información sensible desde el punto de vista comercial o crítica acerca de la persona u otro individuo. El siguiente paso consiste en determinar si tal información podría retenerse o suprimirse.

PASO (7): VERIFICAR DATOS DE TERCEROS

K-C no deberá divulgar, eliminar ni, de algún otro modo, afectar los datos personales que se relacionen con personas que no sean el propio solicitante, a menos que el tercero haya otorgado su consentimiento o que resulte razonable suministrar (o eliminar, rectificar, etc.) la información sin su consentimiento. En consecuencia, usted deberá revisar los datos personales a fin de advertir información sobre terceros (incluida la información tanto sobre el solicitante *como* un tercero).

A continuación, tendrá que decidir si tal información debería retenerse o suprimirse. Si usted decide que K-C no puede divulgar (o borrar o rectificar) la información del tercero, aun así deberá maximizar la cantidad de información que puede divulgarse mediante la supresión de la información del tercero.

Deberá entregar toda la información revisada al líder de privacidad de los datos para que tome la decisión final sobre cómo K-C debería cumplir con la solicitud.

SOLICITUDES DE ELIMINACIÓN Y OBJECIÓN

Los derechos de eliminación y objeción **no** son derechos absolutos.

K-C no tiene la necesidad de eliminar los datos personales que necesita retener: (i) para protegerse de una reclamación judicial (p. ej., un contrato, antecedentes laborales o correspondencia con un cliente sobre una queja); (ii) para cumplir con una obligación legal (p. ej., con fines regulatorios); o (iii) para cumplir con un contrato con la persona (p. ej., un contrato de empleo).

De manera similar, una persona no tiene derecho a objetar la utilización de su información para un propósito que resulte necesario para que K-C cumpla con sus obligaciones legales o cuando se deba cumplir con un contrato vigente con dicha persona (p. ej., un contrato de empleo).

En la mayoría de los casos, será cuestión de equilibrar la necesidad de K-C de retener o procesar los datos personales frente a la solicitud de la persona para que se borren o dejen de procesarse con ese fin y decidir los derechos de qué parte deberán prevalecer. A fin de colaborar con este ejercicio de equilibrio, usted deberá pedir al solicitante que brinde sus *motivos* de la solicitud de objeción o eliminación (si todavía no los hubiera brindado). **Nota: Una persona no tiene la obligación de brindar un motivo para objetar las actividades de marketing.**

Como regla general, K-C puede cumplir con las solicitudes de eliminación y/u objeción en relación con los siguientes datos (a menos que *ya* sean objeto de una queja o procedimiento judicial):

- información sobre la elaboración de perfiles de consumidores;
- cookies y/o bitácoras de red;
- marketing;
- postulaciones de trabajo no exitosas, después del período durante el cual podría presentarse una reclamación de discriminación.

En el caso de que usted decida no cumplir con la solicitud de eliminación u objeción, deberá considerar si, en su lugar, los datos personales pueden "restringirse a fin de que *solo* puedan usarse para ese propósito específico (pero que, por ejemplo, no estén visibles de otro modo en la cuenta del cliente). Una vez que la información deje de ser necesaria para ese propósito, deberá eliminarse de forma permanente.

Si decide cumplir con una solicitud de eliminación, siempre deberá conservar un registro de la solicitud. Por consiguiente, no es posible eliminar *todos* los datos personales del solicitante.

DECISIONES AUTOMATIZADAS

La ley de protección de los datos también confiere a las personas derechos específicos para objetar las decisiones automatizadas. Un ejemplo podría ser la decisión de contratar o no a una persona exclusivamente sobre la base de un proceso automatizado. Se deberá consultar al responsable de privacidad de los datos pertinente a la hora de evaluar cualquier solicitud de objeción de una decisión automatizada a fin de determinar si se clasifica dentro del alcance de este derecho.

PASO (8): BRINDAR LA RESPUESTA

Si decidió denegar una IRR (ya sea por completo o con respecto a un derecho específico), la respuesta deberá detallar los motivos de la denegación de la solicitud. Si decidió responder a una solicitud de eliminación mediante la "restricción" de los datos personales, esto deberá explicarse en la respuesta.

Si la solicitud se realiza por correo electrónico, también deberá brindar la respuesta por correo electrónico (o si la persona solicitó una respuesta por correo electrónico). En otros casos, sin embargo, la respuesta podrá enviarse por correo postal.

SOLICITUDES DE ACCESO

En respuesta a una **solicitud de acceso**, deberá enviar una copia de los datos personales solicitados por la persona. Deberá asegurarse de que la respuesta que acompañe a los datos personales incluya toda la información de la plantilla del Anexo 1.

SOLICITUDES DE PORTABILIDAD

El derecho de portabilidad tiene muchas superposiciones con el derecho de acceso, pero la portabilidad de los datos otorga al solicitante el derecho a tener una copia de los datos en un formato legible por máquina y de uso habitual. Esto no significa solamente brindar los datos en formato electrónico (una copia escaneada es formato electrónico), sino en un formato legible por computadora (p. ej., un archivo de Excel o Word).

Si no está seguro de si una IRR es una solicitud de portabilidad, deberá consultar al líder de privacidad de los datos correspondiente. Es posible que también deba comunicarse con IT a fin de averiguar en qué formato puede brindarse la información.

Las preguntas sobre esta adenda pueden remitirse a KC HelpLine en KCHelpLine@kcc.com.

ANEXO 1 A LA ADENDA 2 DE LA POLÍTICA DE PRIVACIDAD Y PROTECCIÓN DE DATOS DE K-C

DERECHOS INDIVIDUALES

PLANTILLA DE LA CARTA DE EXTENSIÓN DE LA SOLICITUD DE ACCESO DEL SUJETO

[*Por correo electrónico o correo postal*]

Estimado [*solicitante*]:

Le escribo en respuesta a su solicitud con fecha [*insertar*].

Estamos recopilando los datos para nuestra respuesta a su solicitud de acceso como sujeto. Sin embargo, le escribimos para informarle, tal como lo exige la ley vigente, que prevemos que finalizar nuestra respuesta a su solicitud nos llevará un período más prolongado. Esto se debe a [*insertar los motivos del retraso*].

De más está decir que nos esforzaremos para enviarle la respuesta a su solicitud lo antes posible. De cualquier modo, prevemos poder brindarle nuestra respuesta a su solicitud el [*insertar fecha*].

[*Cierre, incluida la información de contacto pertinente*]

ANEXO 2 A LA ADENDA 2 DE LA POLÍTICA DE PRIVACIDAD Y PROTECCIÓN DE DATOS DE K-C

DERECHOS INDIVIDUALES

PLANTILLA DEL FORMULARIO DE SOLICITUD DE ACCESO A LOS DATOS PERSONALES

SOLICITUD DE ACCESO A LOS DATOS PERSONALES	
1. Nombre completo	
2. Nombre anterior/otros nombres por los cuales se lo identifique para ayudar en nuestras búsquedas y la verificación de identidad	
3. Direcciones actual y anterior para ayudar en nuestras búsquedas y la verificación de identidad	
4. Información de contacto (p. ej. número de teléfono, dirección de correo electrónico)	
5. ¿Cómo desea recibir la respuesta a su solicitud de acceso como sujeto?	☐ Mediante [copia impresa] [USB cifrado] a la dirección indicada anteriormente ☐ Mediante [copia impresa] [USB cifrado] a la siguiente dirección:…… ☐ Por correo electrónico a la dirección de correo electrónico indicada anteriormente:…….
6. Información a la que desea acceder Proporcione una descripción de todos los parámetros que desea que apliquemos a nuestra búsqueda (p. ej., del 1 de marzo de 2016 al 5 de mayo de 2017; todas las notas del registro de clientes o "mi expediente de empleo"). Este no es un requisito, pero puede ayudarnos a encontrar sus datos personales de manera más eficiente.	
[<u>NOTA INTERNA</u>: Si ya hubiera verificado satisfactoriamente la identidad del solicitante, podrá eliminarse la sección 7 a continuación]	
7. [Verificación de identidad Proporcione una copia de **uno** de los documentos enumerados. Comuníquese con nosotros si tiene algún problema para obtener las copias de los documentos mencionados.**]**	☐ Pasaporte vigente firmado ☐ Licencia de conducir con fotografía ☐ Tarjeta de identidad nacional con fotografía ☐ Factura de servicios públicos (factura de gas, electricidad, televisión satelital, teléfono de línea) emitida dentro de los tres últimos meses) ☐ Cuota tributaria del consejo de autoridad local del año fiscal en curso del consejo ☐ Extracto de cuenta bancaria o en sociedad de crédito hipotecario ***Asegúrese de suprimir correctamente de la copia que nos envíe a nosotros toda información financiera o privada incluida en estos documentos.***
Declaración ☐ Declaro que la información incluida en este formulario es completa y precisa.	
Nombre: Fecha:	

ANEXO 3 A LA ADENDA 2 DE LA POLÍTICA DE PRIVACIDAD Y PROTECCIÓN DE DATOS DE K-C

DERECHOS INDIVIDUALES

PLANTILLA DE LA CARTA DE RESPUESTA A LA SOLICITUD DE ACCESO DEL SUJETO

[*Por correo electrónico o correo postal*]

Estimado [*solicitante*]:

Le escribo en respuesta a su solicitud con fecha [*insertar*].

He adjuntado una copia de los datos personales que usted solicitó. Estos son datos personales conformados por [*insertar una breve descripción de los datos, p. ej., su registro de empleo, la correspondencia con [empresa del Grupo], etc.*].

[Algunos de los datos personales que solicitó no se incluyeron en el adjunto, ya que [*empresa del Grupo*] tiene derecho a retener esta información conforme a la ley de protección de los datos. [*Nota: Evalúe la posibilidad de incluir un motivo, p. ej., porque está sujeto a privilegios legales o también se relaciona con un tercero*].

[*Empresa del Grupo*] procesó estos datos personales a los fines de [*insertar una breve descripción de los propósitos, p. ej., abordar una queja, administrar la relación laboral, llevar adelante un proceso disciplinario, enviarle información de marketing*].

[*Inserte detalles de los terceros que recibieron los datos:* Estos datos personales se compartieron con nuestros proveedores de servicios a fin de que pudieran prestarnos sus servicios. Además, se compartieron con [*insertar los demás terceros, p. ej., proveedor de atención médica privada*].]

[*Si los datos no se obtuvieron de la persona sino de un tercero, deberá indicar la fuente de los datos*].

[*Empresa del Grupo*] retendrá estos datos durante [*x años o hasta x años después de la finalización de nuestra relación con usted o información similar sobre cómo se determinará el período de retención*].

En algunas circunstancias, usted tiene derecho a solicitar que [*empresa del Grupo*] rectifique los datos personales imprecisos, elimine o restrinja sus datos personales, o a objetar que [*empresa del Grupo*] procese sus datos personales para ciertos propósitos. Sin embargo, no tendremos la obligación de cumplir con esta solicitud si contamos con un fundamento lícito para denegarla.

Para obtener más información sobre el procesamiento de datos personales por parte de [*empresa del Grupo*], por favor lea nuestra Política de privacidad, que se encuentra disponible en [*insertar URL*].

Por favor comuníquese con nosotros si considera que no hemos cumplido con la solicitud de manera satisfactoria. También tiene derecho a presentar una queja ante la [*Autoridad de protección de los datos (ICO, AEPD)*].

[*Cierre, incluida la información de contacto pertinente*]

ADENDA 3 DE LA POLÍTICA DE PRIVACIDAD Y PROTECCIÓN DE DATOS DE K-C

DESIGNACIÓN DE PROVEEDORES

1. INTRODUCCIÓN

La Política de privacidad y protección de datos de K-C define los 9 principios de la protección de datos que K-C debe cumplir a la hora de procesar datos personales.

Esta adenda es complementaria y suplementaria a la Política de gestión de proveedores de seguridad IT 115-01 y a la Norma de gestión de proveedores de seguridad IT 240-01 (la "**Política y Norma de gestión de proveedores de seguridad**"), los cuales se aplicarán, junto con el presente anexo, en caso de que un proveedor (según se define a continuación) procese datos personales en nombre de K-C.

Esta adenda incluye información sobre los pasos que usted debe seguir desde la perspectiva de la protección de datos cuando se contrate a un proveedor externo (el "**proveedor**") para prestar servicios a K-C que puedan implicar el procesamiento de datos personales por parte de dicho proveedor. Esta adenda también se aplicará si K-C vuelve a contratar a un proveedor existente.

Los pasos que deben seguirse son los siguientes:

Paso 1: Definir si el proveedor es Contralor de datos o Procesador de datos: Equipo Comercial o Funcional

Paso 2: Cumplir con los requisitos legales para la protección de datos al momento de designar al proveedor: Equipo Comercial o Funcional
Paso 3: Verificar si los datos personales se transferirán fuera del Espacio Económico Europeo (European Economic Area, EEA): Equipo Comercial o Funcional

Paso 4: Completar la Lista de verificación de autoevaluación a fin de garantizar el cumplimiento de esta adenda: Equipo Comercial o Funcional

Esta adenda no se aplica si los servicios del proveedor no implican el procesamiento de datos personales (por ejemplo en los casos en que se trate solamente de un contrato para la compra de mercaderías, como hardware y materias primas).

Consulte el Apéndice A de la Política de privacidad y protección de datos de K-C para acceder a un glosario de los términos que se definen en la presente adenda.

PASO 1: IDENTIFICAR SI EL PROVEEDOR ES CONTRALOR DE DATOS O PROCESADOR DE DATOS

Cada vez que se proponga la contratación de un proveedor al cual se aplique esta adenda, primero deberá identificar si el proveedor es "Contralor de datos" o "Procesador de datos". En caso de tener dudas acerca de si el proveedor es Contralor de datos o Procesador de datos, consulte al líder de privacidad de datos correspondiente, cuyos detalles de contacto pueden encontrarse aquí en la página de SharePoint del Programa global de privacidad de datos (Global Data Privacy Program SharePoint).

- Un **Contralor de datos** hace referencia a la parte que determina los propósitos (es decir, por qué se procesa la información) y los medios (es decir, cómo se procesa la información) de procesamiento. A fin de identificar esto, pregúntese: ¿el proveedor es la mente que controla la actividad propuesta? ¿Es el proveedor o K-C quien decide qué datos personales se recopilarán y para qué se usarán? Con frecuencia, es la persona que "posee" los datos personales. En términos generales, quien sea que "tome las decisiones" en relación con los datos personales probablemente sea el Contralor de datos.

- Un **Procesador de datos** hace referencia a la parte que procesa los datos personales en nombre del Contralor de datos. A fin de identificar esto, pregúntese: ¿el proveedor llevará adelante el

procesamiento *solamente* porque K-C le indicó que lo hiciera? Si es así, por lo general, el proveedor será un Procesador de datos.

Es importante identificar si el proveedor es Contralor de datos o Procesador de datos ya que:

- Si un proveedor es Contralor de datos que procesa los datos personales de ciudadanos de la Unión Europea (UE), tendrá la responsabilidad directa de cumplir con las leyes de protección de datos de la UE u otras leyes (por ejemplo, garantizar que el procesamiento de los datos personales sea justo y lícito y permitir a las personas que ejerzan sus derechos en virtud de las leyes de protección de datos).

- Si un proveedor es Procesador de datos que procesa los datos personales de ciudadanos de la UE en nombre de un Contralor de datos, aún tendrá algunas obligaciones directas en virtud de las leyes de protección de datos de la UE u otras leyes. Sin embargo, sus obligaciones principales se determinarán por contrato con el Contralor de datos (es decir, con K-C). K-C será legalmente responsable de todo procesamiento realizado por sus Procesadores de datos y, por consiguiente, resulta esencial que se implementen controles estrictos de las acciones del Procesador de datos.

EJEMPLOS

PROVEEDOR COMO CONTRALOR DE DATOS

- En el caso de que un proveedor preste servicios de seguros de atención médica privada al personal.
- En el caso de que un proveedor sea proveedor de pensiones del personal.
- En el caso de que un proveedor sea un agente de viajes, un hotel o una compañía de alquiler de automóviles.

PROVEEDOR COMO PROCESADOR DE DATOS

- En el caso de que un proveedor sea un proveedor de servicios de nómina que K-C haya contratado para agilizar su proceso de nómina.
- En el caso de que el proveedor sea proveedor de servicios en la nube.

Si el proveedor actúa como Contralor de datos:

Si el proveedor actúa como Contralor de datos:

- Usted deberá garantizar que el contrato con el proveedor incluya las condiciones estándar de K-C para los Contralores de datos, las cuales pueden encontrarse aquí.
- No es necesario que complete el Paso 2, pero puede continuar directamente con el Paso 3 relacionado con las transferencias de datos.

PASO 2: CUMPLIR CON LA LEY DE PROTECCIÓN DE DATOS O DE PRIVACIDAD AL MOMENTO DE DESIGNAR AL PROVEEDOR

Debido a que K-C será responsable de las acciones de sus Procesadores de datos, existen ciertos pasos que deben seguirse a fin de proteger a K-C a la hora de designar a un proveedor que sea Procesador de datos.

Además, cuando celebra un contrato con un proveedor que sea Procesador de datos, K-C tiene la obligación legal de garantizar ciertas **disposiciones obligatorias** respecto de los datos personales que se incluyen en el contrato con el Procesador de datos. Las condiciones estándar de K-C para los Procesadores de datos pueden encontrarse aquí.

En la siguiente tabla se describen los pasos prácticos que usted debe seguir al momento de **designar al proveedor** a fin de garantizar el cumplimiento de las obligaciones legales de K-C. La unidad de negocios pertinente tiene la responsabilidad general de este proceso.

PASO	¿QUÉ SIGNIFICA ESTO EN LA PRÁCTICA?
Comprender la naturaleza del procesamiento de datos	Identificar los tipos y las cantidades de datos personales a los cuales tendrá acceso el proveedor. El proveedor solamente deberá tener acceso a la cantidad mínima de datos personales que necesite para prestar servicios. Si el proveedor tiene acceso a los datos de la tarjeta de pago (como un proveedor de gastos y viajes), el acuerdo también deberá abordar el cumplimiento de la Norma de seguridad de datos de la industria de tarjetas de pago (Payment Card Industry Data Security Standard, PCI DSS).
Llevar adelante la diligencia debida sobre el proveedor	Elegir a un proveedor que brinde garantías suficientes respecto de la seguridad de la información y el manejo de datos personales y trabajar con Seguridad de Tecnología de la información (Information Technology, IT) en el proceso de diligencia debida. Recordar también que el dueño funcional o comercial podría tener que realizar una Evaluación del impacto de la protección de datos (Data Protection Impact Assessment, DPIA). Consulte la *Adenda 1 de la Política global de privacidad de los datos de K-C (Evaluaciones de impactos en la protección de datos)* para obtener más información. Usted también deberá garantizar que el proveedor pueda proporcionar el adecuado nivel de protección de seguridad de los datos y tener en cuenta la naturaleza de los datos personales y cualquier riesgo implicado (por ejemplo, las consecuencias de una violación de la seguridad). Una vez más, deberá trabajar de forma estrecha con Seguridad de IT en este aspecto y, si el proveedor fuera a alojar datos personales en nombre de K-C, usted deberá asegurarse de enviar una Solicitud de evaluación de riesgos de seguridad de la información alojada Consulte la Política y Norma de gestión de proveedores de seguridad para obtener más información.
Tomar precauciones adicionales con los datos personales sensibles y con los datos de la tarjeta de pago.	Seguridad de IT tiene sus propios requisitos de seguridad para los proveedores que procesan datos personales sensibles o datos de la tarjeta de pago. Por lo tanto, asegúrese de colaborar en consonancia con Seguridad de IT a fin de garantizar que las especificaciones de seguridad del contrato sean las adecuadas.
Garantizar que el contrato por escrito incluya o incorpore las cláusulas de protección de datos	El contrato con el proveedor debe incluir lenguaje específico sobre la protección de datos, ya que se trata de un **requisito legal** conforme a la UE y otras leyes de protección de datos. La Política y Norma de gestión de proveedores de seguridad define ciertos requisitos para los contratos con proveedores, pero resulta esencial que también se incorporen las cláusulas de protección de datos en los casos que el proveedor procese datos personales de K-C. K-C ha adoptado un conjunto de cláusulas de protección de datos estándar que refleja estas obligaciones Si el contrato es sobre las condiciones estándar del proveedor, usted aún deberá garantizar que se incluya en el contrato el lenguaje sobre la protección de datos necesario.

Advertir toda transferencia de datos fuera del EEA	Si cualquiera de los datos personales se transfiriera fuera del EEA (inclusive en caso de que sea posible acceder a dichos datos personales de forma remota desde fuera del EEA), por ejemplo, a cualquier proveedor de software como servicio (Software as a Service, SaaS), se deberán seguir ciertos pasos a fin de garantizar que la transferencia sea lícita. Consulte el Paso 3 a continuación.
Quitar el nombre, colocar seudónimos o agregar datos personales si es posible	Si el acuerdo con el proveedor puede incluir estas salvaguardas sin un detrimento significativo, tales salvaguardas deberán considerarse a fin de ayudar a eliminar o reducir los riesgos de la protección de datos.
Limitar el acceso a los datos personales	El proveedor debe tener los controles de acceso adecuados de forma tal que solo quienes presten los servicios puedan acceder a los datos personales y que los derechos de acceso se limiten a los necesarios para la función de cada individuo.
Garantizar que el proveedor pueda asistir en las solicitudes de derechos individuales	El lenguaje sobre la protección de datos en el contrato debe incluir la obligación del proveedor de ayudar a K-C a permitir que las personas ejerzan sus derechos individuales. Estos incluyen derechos a acceder, rectificar y borrar sus datos personales y objetar su uso para un propósito en particular. El proveedor debe garantizar que puede respetar estos derechos (p. ej., al rectificar o borrar datos personales), cuando una persona se lo solicite a K-C. El proveedor también debe garantizar que si recibe alguna solicitud en relación con los datos personales, esta se reenvíe de forma oportuna a K-C.
Verificar los subcontratistas del proveedor	Las obligaciones de procesamiento de datos incluidas en las cláusulas estándar de K-C para los Procesadores de datos abordan la subcontratación. Usted debe garantizar que todas las condiciones de procesamiento de datos se “transmitan” a cualquier subcontratista.
Dar aviso del uso compartido de los datos, a menos que esto ya se haya realizado	Garantizar que las personas cuyos datos personales se vean afectados por el acuerdo hayan recibido el aviso adecuado. Esto podrá realizarse mediante la comunicación del Aviso de privacidad sobre la selección de K-C, el Aviso para el personal sobre la protección de datos de K-C o el Aviso de privacidad en línea de K-C (según corresponda). Si los Avisos de privacidad existentes no son los adecuados o no cubren el acuerdo de forma correcta, evalúe cómo informar a las personas antes de brindar sus datos personales al proveedor.
K-C monitorea el cumplimiento del proveedor en toda la relación	Garantizar que se hayan implementado pasos razonables que le permitan a K-C monitorear el desempeño del proveedor respecto de sus obligaciones de seguridad y procesamiento, las cuales pueden incluir la solicitud y revisión de los informes de auditoría independiente del proveedor, o la realización de inspecciones a medida en el lugar.

Definir qué sucederá con los datos personales al final de la relación	Si dejara de ser necesario conservar los datos personales, debido a la finalización de la relación de servicios o porque la ley ya no lo exija, la información deberá devolverse a K-C o eliminarse de forma permanente en las instalaciones de K-C. Asegúrese de que las condiciones del contrato dispongan la devolución y/o la eliminación permanente de los datos personales a solicitud de K-C.

PASO 3: VERIFICAR SI LOS DATOS PERSONALES SE TRANSFERIRÁN FUERA DEL EEA

Este Paso 3 deberá completarse si el proveedor actuara como Contralor de datos o Procesador de datos.

Si está considerando la designación de un proveedor, debe definir lo siguiente:

- Si el proveedor, por sí mismo, se encuentra fuera del EEA.
- Si el proveedor, *subsecuentemente*, puede transferir datos personales fuera del EEA (por ejemplo, a las subsidiarias o a los subcontratistas del proveedor).

Una "transferencia" de datos personales incluye lo siguiente:

- permitir que sea posible **acceder de forma remota** a los datos personales **almacenados** en el EEA desde un país fuera de dicho EEA (p. ej., los EE. UU.);
- reubicar la base de datos fuera del EEA; o
- enviar un conjunto de datos (por ejemplo, un archivo de Excel) como adjunto en un correo electrónico dirigido a un destinatario fuera del EEA.

K-C (o cualquier proveedor que actúe en su nombre) no deberá transferir datos personales desde un país del EEA hacia un país fuera del EEA, a menos que existan los medios para brindar las salvaguardas necesarias a esos datos personales.

Un pequeño grupo de países (Andorra, Argentina, Canadá, Islas Feroe, Guernsey, Isla de Man, Israel, Jersey, Nueva Zelanda, Suiza y Uruguay) ha sido legalmente reconocido por brindar un nivel de protección adecuado y, por lo tanto, usted puede transferir datos personales desde el EEA hacia esos países. La lista de países "adecuados" puede encontrarse en el sitio web de la Comisión, aquí: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm

EE. UU. también se considera un país "adecuado" si el destinatario de los EE. UU. (ya sea el proveedor o un subcontratista) cuenta con la certificación del Escudo de Privacidad entre la UE y los EE. UU. y si dicha certificación abarca el tipo de datos personales que se transferirán. Si el proveedor desea ampararse en el Escudo de Privacidad, usted deberá verificar la certificación del destinatario en la lista en línea: https://www.privacyshield.gov/list. Si el proveedor se amparase en el Escudo de Privacidad, asegúrese de que esté sujeto a la obligación de mantener su condición según el Escudo de Privacidad durante el período que dure el acuerdo (o asegúrese de que lo haga el destinatario correspondiente de los EE. UU.) y que se encuentre obligado a ejecutar una solución de transferencia alternativa si el Escudo de Privacidad deja de ser válido.

En el caso de los países fuera del EEA y no incluidos anteriormente, se deberá adoptar una solución alternativa antes de que puedan transferirse los datos personales. Lo más adecuado para K-C probablemente sea solicitar que el destinatario fuera del EEA firme un conjunto aprobado de cláusulas de transferencia de datos internacionales, conocido como "Cláusulas modelo de la UE". En

Las cláusulas estándar de K-C, también incluyen una copia de los dos conjuntos de Cláusulas modelo de la UE, uno para las transferencias a los Contralores y otro para las transferencias a los Procesadores. Estos acuerdos deberán celebrarse con el destinatario fuera del EEA "tal cual están" y sin ninguna enmienda; de lo contrario, no cumplirán con los requisitos legales de la UE. Sin embargo, se deberán completar los apéndices a fin de incluir una descripción de los datos personales y del procesamiento, como también una descripción de las medidas de seguridad que el proveedor deberá implementar.

Resumen de los acuerdos contractuales que deben implementarse:

País en el cual se alojarán los datos personales de K-C, o desde el cual se podrá acceder a ellos	**Cómo regular el procesamiento por parte del proveedor**	**Cómo regular las transferencias fuera del EEA**
Países "adecuados" (Andorra, Argentina, Canadá, Islas Feroe, Guernsey, Isla de Man, Israel, Jersey, Nueva Zelanda, Suiza y Uruguay)	Obtener el acuerdo del proveedor respecto de las Condiciones estándar de protección de datos de K-C	N/C ya que los países ofrecen la "protección adecuada"
Países no adecuados (p. ej., Australia, India, China o compañía de los EE. UU. no registradas ante el Escudo de Privacidad)	Obtener el acuerdo del proveedor respecto de las Condiciones estándar de protección de datos de K-C	Ejecutar las Cláusulas modelo aplicables de la UE
Compañías de los EE. UU. que cuenten con la certificación del Escudo de Privacidad entre la UE y los EE. UU. y cuya certificación cubra el tipo de datos personales que se transfieran	Obtener el acuerdo del proveedor respecto de las Condiciones estándar de protección de datos de K-C	Garantizar que el proveedor esté obligado a mantener la certificación del Escudo de Privacidad durante todo el período de la contratación y a implementar un acuerdo alternativo si el Escudo de Privacidad deja de ser válido

PASO 4: LISTA DE VERIFICACIÓN DE AUTOEVALUACIÓN PARA EL CUMPLIMIENTO DE ESTA ADENDA

Con el fin de garantizar que haya cumplido con los requisitos de esta adenda, le resultará útil completar la lista de verificación de autoevaluación incluida en el Anexo 1 a este anexo.

Las preguntas sobre esta adenda pueden enviarse a: **KC HelpLine: HelpLine@kcc.com**

ANEXO 1 A LA ADENDA 3 DE LA POLÍTICA DE PRIVACIDAD Y PROTECCIÓN DE DATOS DE K-C:

LISTA DE VERIFICACIÓN DE DESIGNACIÓN DE PROVEEDORES

Esta lista de verificación está diseñada para ayudar a determinar si ha cumplido con los requisitos de la *Adenda 3 de la Política de privacidad y protección de datos de K-C (Requisitos del proveedor).* Si no puede responder "sí" a todas estas preguntas, deberá solicitar más información al proveedor. Si aun así no puede encontrar la respuesta, deberá consultar al líder de protección de datos correspondiente (cuyos detalles de contacto pueden encontrarse en la intranet de K-C antes de contratar al proveedor.

VERIFIQUE SI TOMÓ TODAS LAS MEDIDAS PARA GARANTIZAR EL CUMPLIMIENTO DE LA CONTRATACIÓN DE SU NUEVO PROVEEDOR	COMPLETADO
Identificamos qué tipos de datos personales (según se define en la POLÍTICA/el ENLACE) se divulgarán al proveedor.	☐
Identificamos si el proveedor actuará como Contralor de datos o Procesador de datos en este procesamiento.	☐
Garantizamos que nuestro contrato con el proveedor aborde el cumplimiento de la protección de datos en lugar de su rol en el procesamiento.	☐
Garantizamos que el proveedor o su solución requieran solamente la cantidad necesaria de datos personales a fin de lograr el propósito para el cual se contrata al proveedor y no más de dicha cantidad.	☐
Analizamos con el proveedor si brindar datos personales con seudónimos, sin nombre o información adicional es adecuado para el procesamiento.	☐
En el caso de los datos personales que son datos personales sensibles, garantizamos que el proveedor tomará las medidas de seguridad adicionales a fin de proteger estos datos personales.	☐
Hemos tomado las medidas para garantizar que el proveedor solamente otorgue acceso a los datos personales a quienes tengan una "necesidad de conocimiento" genuina.	☐
Hemos tomado las medidas para garantizar que el proveedor llevará registros del procesamiento de los datos personales, como quién accedió a los datos, cuándo lo hizo, si los datos se modificaron o se borraron, etc.	☐
Hemos tomado las medidas para garantizar que el proveedor almacenará los datos personales solamente durante el período necesario para el propósito y no más de este tiempo.	☐
Hemos tomado las medidas para garantizar que todos los datos personales serán depurados, eliminados de forma permanente o devueltos al final de la relación con el proveedor.	☐

Comprendemos que otras partes (en caso de existir alguna) participarán en la prestación de servicios y hemos asegurado que los requisitos de procesamiento de datos se transmitirán al subcontratista.	☐
El procesamiento exige que sea posible acceder a los datos personales desde afuera del EEA. Hemos implementado una solución de transferencia (véase el Paso 3).	☐
Hemos implementado un proceso interno para monitorear el cumplimiento del proveedor durante toda la relación con el proveedor.	☐

ADENDA 4 DE LA POLÍTICA GLOBAL DE PRIVACIDAD DE LOS DATOS DE K-C

PRIVACIDAD POR DISEÑO

1. INTRODUCCIÓN

1.1 La POLÍTICA GLOBAL DE PRIVACIDAD DE LOS DATOS DE K-C exige que K-C adopte un enfoque de "**Privacidad por diseño**". Privacidad por diseño significa que todo nuevo sistema, herramienta o funcionalidad que utilizará datos personales deberá desarrollarse de manera tal que:

- tenga en cuenta los derechos de privacidad de las personas; y
- le permita a K-C cumplir con los Principios de la protección de datos de K-C definidos en la Política de privacidad y protección de datos de K-C.

1.2 Privacidad por diseño significa garantizar que, desde el principio, las consideraciones de privacidad se incorporen a todo nuevo sistema, por ejemplo, en términos de qué datos se recopilan, durante cuánto tiempo se guardan, cómo se almacenan y quién tiene acceso a ellos. Sin la Privacidad por diseño, K-C corre el riesgo de no poder cumplir con sus obligaciones en virtud de las leyes de protección de los datos debido a las limitaciones técnicas de nuestros sistemas.

1.3 Consulte el Apéndice A de la POLÍTICA GLOBAL DE PRIVACIDAD DE LOS DATOS DE K-C para acceder a un Glosario de los términos definidos en esta adenda.

2. CUMPLIMIENTO DE ESTA ADENDA

2.1 Esta adenda aplica a todo el personal que participe en el diseño, el desarrollo o la puesta en funcionamiento de un nuevo sistema , herramienta o funcionalidad (ya sea de forma interna o por parte de un tercero) que implique el procesamiento de datos personales; esto incluye modificaciones o incorporaciones substanciales a los sistemas existentes. A los fines de esta adenda, se hace referencia al sistema o herramienta o funcionalidad como "**Cambio de IT**" (Tecnología de la información [Information Technology, IT]).

2.2 A la hora de diseñar, desarrollar o poner en funcionamiento un Cambio de IT, el personal deberá considerar cada uno de los requisitos de la Privacidad por diseño que se definen en la Sección 3. No todos los requisitos se aplicarán a todo nuevo proyecto, según la naturaleza del Cambio de IT. Al considerar cada requisito, le resultará útil completar la lista de verificación incluida en el Anexo 1.

2.3 Si se identifica que algún Cambio de IT pueda provocar un **alto riesgo** a los derechos y las libertades de las personas, cada empresa del Grupo deberá realizar además una Evaluación del impacto de la protección de datos (Data Protection Impact Assessment, **DPIA**) antes de que el proyecto pueda continuar. *La adenda 1 de la POLÍTICA GLOBAL DE PRIVACIDAD DE LOS DATOS DE K-C (DPIA)* ofrece lineamientos sobre cuándo una actividad de procesamiento podría considerarse de alto riesgo.

2.4 La DPIA podrá identificar requisitos más específicos de la Privacidad por diseño que se deberán evaluar en el proyecto a fin de mitigar los riesgos identificados. Para obtener más información, consulte la *adenda 1 de la POLÍTICA GLOBAL DE PRIVACIDAD DE LOS DATOS DE K-C (DPIA)*.

3. REQUISITOS DE LA PRIVACIDAD POR DISEÑO

3.1 Propósito(s)

Identifique el (los) propósito(s) del Cambio de IT, es decir, para qué es el Cambio de IT. ¿Con qué fin se diseña? Este es el requisito más importante, ya que lo ayudará a cumplir con todos los demás requisitos de la lista. Deberá tener una idea muy clara sobre el(los) propósito(s) específico(s) de todo nuevo Cambio de IT, de modo que todo el manejo de datos del Cambio de IT sea proporcionado para ese propósito.

3.2 **Recopilación y uso de datos**

3.2.1 Identifique qué datos personales necesita el Cambio de IT, es decir, qué campos de datos. El Cambio de IT debe diseñarse para conservar solo la cantidad mínima de datos necesarios para lograr el propósito que usted haya identificado en el punto 3.1 anterior. Si el propósito puede lograrse, por ejemplo, sin conocer el nombre, la dirección de correo electrónico o la dirección postal de la persona, no recopile ni use esta información.

3.2.2 Si el Cambio de IT procesara datos personales sensibles, datos de ubicación o información sobre menores, las consideraciones de privacidad serán particularmente importantes. Solo conserve esta información si la necesita de manera absoluta para el propósito que usted haya identificado en el punto 3.1 anterior y asegúrese de que no se utilice para ningún otro propósito. También es muy probable que el Cambio de IT requiera una DPIA.

3.2.3 Cuando corresponda, deberá distinguir entre campos obligatorios y opcionales. Si los datos recopilados pudieran ser *útiles* para el propósito, pero no fueran estrictamente necesarios, deberá establecer la disposición de su carácter opcional (y dejarlo claro para la persona).

3.2.4 Cuando corresponda, no deberán utilizarse campos de texto, ya que estos conllevan el riesgo de recopilar datos que K-C tal vez no necesite y que hacen dificultoso anonimizar los datos. Cuando sea posible, en su lugar, deberá proporcionar casillas de verificación u opciones desplegables.

3.2.5 Si fuera posible, los registros deberán incluir un identificador único (p. ej., la identificación de un cliente o empleado). Esto hace que resulte más fácil anonimizar, compartir y analizar los registros sin divulgar el nombre de una persona. Sin embargo, no deberá usar identificadores emitidos por el gobierno, como el pasaporte, el número del seguro nacional o del seguro social (a menos que resulte necesario para el propósito).

3.3 **Acceso a los datos y calidad de los mismos**

3.3.1 Tenga en cuenta quién dentro de K-C necesita acceder a los datos personales que conserva el Cambio de IT. Solo debería poder acceder el personal con una necesidad de acceso a la información con un propósito legítimo. Si no todas las personas necesitan acceso a los mismos datos y/o a la totalidad del conjunto de datos, diseñe el Cambio de IT de forma tal que los privilegios de acceso puedan segmentarse y/o dividirse en niveles.

3.3.2 Diseñe el Cambio de IT de manera que la información pueda ser editada o eliminada por una persona con responsabilidad sobre los datos, por ejemplo, en el caso de una Solicitud de derechos individuales. Si K-C necesita llevar un registro de lo que se hubiera recopilado inicialmente, considere si será posible agregar notas o anotaciones a fin de hacer las subsiguientes correcciones o aclaraciones.

3.3.3 Entre el personal con una necesidad de acceso a la información, considere quién necesita poder editarla y/o eliminarla, y/o descargarla a su propio equipo. Si se trata de un grupo más pequeño de personas que las personas que solo necesitan tener acceso, una vez más, los permisos deberán habilitar esta opción. Decida desde el principio quién tendrá derecho a otorgar y a quitar los derechos de acceso.

3.3.4 Si fuera posible, el Cambio de IT debe permitir el autoservicio (con la autenticación correspondiente) para que las personas puedan ver, enmendar, actualizar y eliminar la información que hayan brindado, por ejemplo, mediante el cambio de una dirección o la eliminación de una tarjeta de pago guardada. Si no resultara adecuado ofrecer un mecanismo de autoservicio, debería ser sencillo generar un informe que registre toda la información sobre una persona conocida.

3.3.5 El Cambio de IT deberá llevar un control de cuándo se creó un registro y/o de la última actualización. Por ejemplo, el personal correspondiente deberá poder identificar que, hace cinco años se creó un registro, pero que hace dos años se agregó un nuevo número de teléfono celular.

3.4 **Retención y eliminación**

3.4.1 Considere si necesita almacenar la información por completo o si puede eliminarla de inmediato una vez que el proceso esté completo. Por ejemplo, en un sitio web, ¿la información debe conservarse una vez que el cliente haya dejado de navegar?

3.4.2 Los datos solo deberán conservarse durante el plazo necesario para el propósito que usted haya identificado con anterioridad. Es posible que algunos datos del Cambio de IT se necesiten durante más tiempo que otros, por lo cual deberá definir diferentes períodos para las distintas categorías de datos. Si ya no necesita los datos en el Cambio de IT en línea, pero desea conservarlos con fines de archivado, deberá colocarlos fuera de línea (p. ej., en un archivo o una cinta). Para obtener más lineamientos sobre la retención de datos, deberá consultar la *adenda 8 de la POLÍTICA GLOBAL DE PRIVACIDAD DE LOS DATOS DE K-C (Retención)*.

3.4.3 Si es posible, el Cambio de IT deberá configurarse para que elimine los datos automáticamente cuando se cumpla el período de retención. Sin embargo, asegúrese de que la eliminación automática pueda suspenderse si resultara necesario, por ejemplo, si los datos debieran retenerse durante períodos más prolongados debido a litigios.

3.4.4 Si, después de cierto período, solo necesitara los datos de forma anónima, se deberán eliminar todos los identificadores. Esto incluye nombre, dirección de correo electrónico, fecha de nacimiento y todo identificador que se use en los Cambios de IT.

3.4.5 Si el Cambio de IT es una cuenta del cliente, considere la implementación de una política de suspensión o de cierre después de un período de inactividad.

3.5 **Seguridad y proveedores**

3.5.1 Evalúe las protecciones de seguridad de los datos y si son adecuadas en vistas de la naturaleza de los datos. Cuando sea posible y corresponda, use técnicas de cifrado para proteger los datos, en tránsito y/o en reposo.

3.5.2 Si utiliza los servicios de un proveedor externo, lleve a cabo la diligencia debida apropiada, según se define en la *adenda 3 de la POLÍTICA GLOBAL DE PRIVACIDAD DE LOS DATOS DE K-C (Designación de Proveedores)* a fin de confirmar que sea un proveedor confiable. ¿Existe un contrato? ¿Tiene alguna acreditación de seguridad? Si el Cambio de IT recopilara información de pago, ¿el proveedor cumple con el Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago (Payment Card Industry Data Security Standard, PCI DSS)? Para obtener más detalles sobre la diligencia debida y la designación de proveedores, deberá consultar la *Adenda 3 de la POLÍTICA GLOBAL DE PRIVACIDAD DE LOS DATOS DE K-C (Designación de Proveedores)*.

3.5.3 Si utiliza un proveedor de Software como servicio (Software as a Service, SaaS), verifique si la funcionalidad del servicio le permite cumplir con los demás requisitos de esta lista de verificación. Por ejemplo, ¿le permite eliminar los datos? ¿Qué sucede al finalizar la contratación?

Las preguntas sobre esta adenda pueden remitirse a KC HelpLine en KCHelpLine@kcc.com.

ANEXO 1 A LA ADENDA 4 DE LA POLÍTICA DE PRIVACIDAD Y PROTECCIÓN DE DATOS DE K-C

LISTA DE VERIFICACIÓN DE LA PRIVACIDAD POR DISEÑO

La presente lista de verificación está diseñada para ayudar a garantizar que se dé la debida atención a las consideraciones de la Privacidad por diseño como parte de un Cambio de IT. Si tiene alguna pregunta, deberá consultar al líder de privacidad de los datos pertinente (cuyos detalles de contacto pueden encontrarse en la intranet de K-C.

CONSIDERACIONES DE LA PRIVACIDAD POR DISEÑO	¿SE CONSIDERÓ ESTE PUNTO Y, SI CORRESPONDIERA, SE ABORDÓ COMO PARTE DEL DISEÑO DEL CAMBIO DE IT?
El objetivo del Cambio de IT	☐
Los datos personales necesarios	☐
Todos los datos personales sensibles, datos sobre menores o datos de ubicación	☐
Datos personales obligatorios u opcionales	☐
Campos de texto libre	☐
Identificadores únicos	☐
Derechos de acceso para cada miembro del personal de K-C	☐
Edición o eliminación de los datos personales	☐
Edición o eliminación de derechos para el personal de todas las empresas del Grupo	☐
Mecanismos de autoservicio	☐

Creación y edición de archivos de registro	☐
Almacenamiento o eliminación inmediata	☐
Períodos de retención	☐
Eliminación automática	☐
Anonimización	☐
Suspensión automática por inactividad	☐
Protecciones de seguridad	☐
Proveedores externos	☐
Proveedores de SaaS	☐
Evaluación del impacto de la protección de datos	☐

ADENDA 5 DE LA POLÍTICA GLOBAL DE PRIVACIDAD DE LOS DATOS DE K-C

RESPUESTA A INCIDENTES DE DATOS

1. INTRODUCCIÓN

El Principio 8 de la POLÍTICA GLOBAL DE PRIVACIDAD DE LOS DATOS DE K-C exige que K-C utilice medidas de seguridad adecuadas a fin de proteger los datos personales, incluso si terceros procesaran datos personales en nombre de la empresa. A fin de cumplir con esta obligación, es esencial que K-C responda adecuadamente en caso de divulgación, pérdida, robo u otro procesamiento de datos personales no autorizado reales o presuntos.

Esta adenda es complementaria y suplementaria a la Política de gestión de incidentes de tecnología de la información (Information Technology, IT) IT 106-01 y al Estándar de gestión de incidentes de seguridad de la información IT 250-01 (la "**Política y el estándar de gestión de incidentes de IT**"), que se aplicarán, junto con este anexo, en caso de un incidente por el cual se comprometan datos personales a través de los sistemas informáticos, los sistemas de redes y los dispositivos de K-C.

Esta adenda también se aplica a los incidentes de datos que ocurran fuera de los sistemas informáticos, las redes y los dispositivos de K-C, cuando se hayan comprometidos datos personales, por ejemplo, la pérdida o el robo de documentos impresos con datos personales relacionados con empleados, clientes o consumidores.

Esta adenda define lineamientos adicionales para permitirle al personal: (a) identificar los incidentes de datos reales o presuntos; y (b) responder rápidamente y de forma adecuada a tales incidentes.

La PARTE 1 de la presente adenda aplica a **todo el personal**. Explica en qué consiste un "incidente de datos" y los primeros pasos que usted deberá seguir en caso de advertir un incidente de datos real o presunto.

La PARTE 2 aplica solamente al personal que participa en la investigación y la gestión de un incidente de datos, denominado "Equipo de Gestión de Filtración de Datos", conformado por las siguientes partes:

- el Equipo de Respuesta a Incidentes de Seguridad Informática (Computer Security Incident Response Team, "**CSIRT**"), que se formará bajo el mando del director de seguridad de la información de K-C, en los casos que se apliquen la Política y la Norma de gestión de incidentes de IT;
- el Equipo de Gestión de Crisis Corporativas;
- un miembro del Equipo de Comunicaciones;
- un miembro del [equipo de apoyo del centro o de las instalaciones] si la filtración de datos hubiera derivado de una violación de la seguridad física y/u organizacional;
- el líder de privacidad de los datos pertinente;
- el gerente de Cumplimiento Regional correspondiente; y
- los miembros pertinentes del Departamento Legal de K-C.

El Equipo de Gestión de Filtración de Datos también podrá comprender:

- el personal de K-C que haya provocado o detectado el incidente de datos;
- un miembro del equipo donde haya ocurrido el incidente de datos;
- el abogado externo que brinde asesoramiento respecto de las obligaciones legales de K-C después del incidente de datos y a fin de preservar el privilegio legal profesional en la mayor medida que lo permita la ley;
- un integrante del equipo de Recursos Humanos (si se hubieran comprometido datos relacionados con el personal); y
- Otras entidades externas, como especialistas en informática forense, asesores de gestión de crisis y proveedores de almacenamiento de datos (p. ej., socios de Software como servicio [Software as a Service, SaaS]).

Consulte el Apéndice A de la POLÍTICA GLOBAL DE PRIVACIDAD DE LOS DATOS DE K-C para acceder a un Glosario de los términos definidos en esta adenda.

NOTA IMPORTANTE: Es deber de todo el personal de K-C informar de inmediato todo incidente de datos presunto o confirmado (según se definen a continuación) a [Nota: Se deberá analizar en el

Departamento Legal, de Cumplimiento, y Seguridad de la información de K-C] lo antes posible. Consulte la Parte 1 para conocer más detalles.

El incumplimiento de esta obligación puede exponer legalmente a K-C y podría traer como resultado una medida disciplinaria contra usted.

2. ¿QUÉ ES UN INCIDENTE DE DATOS?

Esta adenda se aplica en caso de cualquier **procesamiento no autorizado** de **datos personales**. Esto podría incluir divulgación no autorizada, robo, pérdida o piratería. Si bien es posible que existan similitudes en el enfoque, podrán aplicarse diferentes consideraciones si la información es **información comercial confidencial** de K-C que no se relacione con las personas (p. ej., planes de negocios, publicaciones no comunicadas, estados financieros, etc.). Si tiene alguna duda respecto de la aplicación de esta adenda, deberá comunicarse con el líder de privacidad de los datos pertinente cuyos detalles de contacto se encuentran en el sitio de SharePoint del Programa global de privacidad de los datos de K-C.

A los fines de esta adenda, un "**incidente de datos**" es todo evento que pueda comprometer significativamente la privacidad, confidencialidad, seguridad o integridad de los **datos personales**, incluida toda divulgación o todo acceso no autorizados a los datos del personal, la pérdida de datos personales o el uso o la manipulación no autorizadas de datos personales.

Algunos ejemplos de incidentes de datos incluyen (entre otros):

- Descubrimiento de un acceso no autorizado a los sistemas que contienen datos personales (p. ej., piratería en un sitio web o uso indebido de las credenciales de acceso de otra persona).
- Pérdida o robo de registros impresos con una cantidad significativa de datos personales, como pérdida o robo de un bolso o una carpeta con documentos. Si los registros impresos solo contienen una pequeña cantidad de datos personales (p. ej., una pequeña cantidad de direcciones de correo electrónico del personal), no será necesario que K-C considere este evento como un incidente de datos (aunque los documentos puedan contener información comercial confidencial de K-C). Sin embargo, si los documentos incluyen datos personales más sustanciales como correspondencia con clientes individuales, listas de marketing o registros de RR. HH., la situación deberá manejarse conforme a esta adenda.
- Pérdida o robo de activos físicos de IT sin salvaguardas de datos activadas (p. ej., cifrado) incluidas computadoras portátiles o dispositivos de almacenamiento (como memorias USB) o dispositivos móviles. Tenga en cuenta que esto podría incluir su propio dispositivo, el cual usa para desempeñar actividades relacionadas con el trabajo.
- Eliminación indebida de registros, archivos multimedia o equipos con datos personales.
- Transmisión accidental o intencional de datos personales a una persona equivocada (ya sea de forma interna dentro de K-C o de manera externa), como el envío por correo electrónico de un archivo al destinatario incorrecto.
- Pérdida de datos personales mientras en tránsito, como paquetes perdidos o entregados a destinatarios incorrectos.
- Pérdida de control de los datos personales, como la imposibilidad de encontrar computadoras, medios de almacenamiento o registros impresos.
- Evidencia de que virus, programas espía o códigos maliciosos hayan interceptado los datos personales.
- Transmisión de datos personales a un tercero no autorizado.

PARTE 1: APLICA A TODO EL PERSONAL DE K-C

1. DENUNCIE EL INCIDENTE DE INMEDIATO

1.1 Si sospecha que ocurrió un incidente de datos, deberá informar de inmediato al líder de protección de datos pertinente (quien informará al Departamento Legal de K-C, según corresponda) y bríndele la mayor cantidad de detalles posible sobre el incidente. Si no puede comunicarse con el líder de protección de datos por teléfono de inmediato, envíe un correo electrónico marcado como "urgente" con el asunto "Incidente de datos".

1.2 Esta obligación aplica ya sea porque haya descubierto personalmente el presunto incidente de datos o porque otra persona le haya informado la posible ocurrencia de una incidente de datos, por ejemplo, si recibió una notificación de cualquiera de nuestros proveedores o socios comerciales, o de alguno de sus subordinados.

1.3 Tenga en cuenta que, aunque sus medidas hayan sido de algún modo responsables del incidente de datos, si no informa a las unidades de negocios apropiadas de inmediato, la situación empeorará. Cuando antes se informe a las personas pertinentes acerca del incidente, más probabilidades habrá de que pueda contenerse y de que se minimicen los riesgos para las personas y/o el daño para K-C.

1.4 En algunos casos, K-C también tendrá la obligación legal de informar a una autoridad de protección de datos (Data Protection Authority, **DPA**) en un plazo de 72 horas, por lo cual es de vital importancia que K-C responda rápidamente a cualquier presunto incidente. Si el incidente ocurre un día viernes o durante el fin de semana, no espere hasta el lunes para denunciarlo.

1.5 Una vez que haya realizado la denuncia inicial, es posible que deba colaborar con la investigación subsiguiente. Se espera que todo el personal brinde cooperación plena con cualquier investigación de incidente de datos.

PARTE 2: APLICA SOLO AL EQUIPO DE GESTIÓN DE FILTRACIÓN DE DATOS

PASOS A SEGUIR EN CASO DE QUE RECIBA UNA DENUNCIA DE UN POSIBLE INCIDENTE DE DATOS

El Anexo 1 incluye una lista de verificación para que usted use a fin de asegurarse de que se completen todos los pasos y se lleve un registro según corresponda.

PASO (1): EVALUACIÓN INICIAL: DEFINIR SI HA OCURRIDO UN INCIDENTE

El primer paso es definir si realmente ha ocurrido un incidente de datos. Como mínimo, esto implicará hablar con la persona que primero denunció el incidente, así como también con el propietario de la aplicación o el de los datos (es decir, la persona con responsabilidad general sobre la aplicación o la base de datos en particular).

Si bien en la mayoría de los casos es "mejor estar seguro que arrepentirse", vale la pena seguir algunos pasos a fin de confirmar que haya ocurrido un incidente y garantizar que no se desperdicien recursos de forma innecesaria.

Al responder rápidamente, también podrá tomar medidas inmediatas para evitar cualquier riesgo para las personas y/o perjuicios para K-C.

PASO (2): REUNIR AL EQUIPO DE GESTIÓN DE FILTRACIÓN DE DATOS

El siguiente paso será reunir al Equipo de Gestión de Filtración de Datos. El gerente de Cumplimiento Regional correspondiente actuará como jefe investigador y será responsable de gestionar el proceso y completar la lista de verificación del Anexo 1.

PASO (3): CONTENCIÓN Y RECUPERACIÓN

El siguiente paso es identificar e implementar las medidas necesarias para contener el incidente y minimizar cualquier perjuicio que ya haya ocurrido. El Equipo de Gestión de Filtración de Datos también deberá determinar si se puede tomar alguna medida para recuperar las pérdidas y limitar cualquier perjuicio adicional que pueda provocar el incidente de datos. Según la naturaleza del incidente de datos, es posible que corresponda informar a la policía.

PASO (4): REALIZAR UNA INVESTIGACIÓN FORMAL

NOTA IMPORTANTE: Con frecuencia, el Paso (3) y el Paso (4) deberán seguirse al mismo tiempo, según la naturaleza y el alcance de la investigación. En algunos casos, K-C deberá informar a su DPA en un plazo de 72 horas, lo cual podría tener lugar antes de que se complete la investigación formal.

El Departamento Legal de K-C deberá encomendar un informe por escrito al Equipo de Gestión de Filtración de Datos sobre el presunto incidente de datos a fin de determinar objetivamente cómo ocurrió el incidente y cuáles pueden ser las posibles consecuencias. Se deberá redactar un informe por escrito. En ***algunas*** jurisdicciones, este informe ***podrá*** gozar de privilegio legal. En consecuencia, el informe deberá: (i) nombrarse de forma clara como "borrador" hasta que sea aprobado por el Departamento Legal de K-C; (ii) identificarse de forma clara con la leyenda "Elaborado según el asesoramiento del abogado de K-C y contiene información privilegiada"; y (iii) informar que no se puede reenviar.

La investigación deberá intentar determinar lo siguiente:

- los hechos que dieron origen al incidente;
- si se debe designar a especialistas en informática forense;
- si la evidencia relacionada con el incidente deberá conservarse y cómo;
- la causa del incidente;
- las categorías de datos afectados;
- las categorías de personas (clientes, consumidores, empleados, otros) afectadas y la cantidad de individuos damnificados;

- todo riesgo potencial para las personas cuyos datos se hayan visto implicados; y
- todo factor de mitigación que resulte relevante, como el uso de cifrado.

El informe deberá ser una descripción objetiva del presunto incidente y, como tal, deberá limitarse a declaraciones objetivas en la medida de lo posible. En particular, el informe no deberá incluir lenguaje emotivo, expresar ninguna opinión ni especular sobre la situación jurídica que resulte del asunto (por ejemplo, el siguiente enunciado no es apropiado: "el incidente violó la ley de protección de los datos").

En ningún caso se deberá transmitir externamente ninguna copia del informe (excepto en el caso del abogado externo), ni internamente fuera del Equipo de Gestión de Filtración de Datos sin la aprobación expresa del Departamento Legal de K-C. Toda comunicación interna del informe (inclusive por correo electrónico) deberá incluir al Departamento Legal de K-C como uno de sus destinatarios.

PASO (5): NOTIFICACIÓN DE INCIDENTES

El Equipo de Gestión de Filtración de Datos deberá evaluar si es necesario notificar el incidente a la DPA y/o a las personas afectadas. Esto dependerá del nivel de riesgo para las personas que resulte del incidente.

¿Debe notificar a alguna parte?

Parte	**Prueba de notificación**	**Plazo**
DPA	Notificar a menos que sea poco probable que el incidente implique un riesgo para las personas.	Dentro de las **72 horas** de la confirmación del incidente de datos, a menos que existan motivos excepcionales para un retraso.
Personas afectadas	Notificar siempre si es probable que el incidente implique un **alto** riesgo para las personas. Independientemente de esta prueba, es posible que existan otros motivos válidos para informar a las personas. Por ejemplo: • Si pueden tomar las medidas para minimizar el riesgo para sí mimas, por ejemplo, al cambiar su contraseña o estar alertas de cualquier actividad fraudulenta en una cuenta. • Si resulta mejor para las relaciones con el cliente o la percepción pública de K-C que la empresa informe proactivamente a las personas en lugar de que se considere que "oculta" el problema. • Cuando se hayan comprometido datos relacionados con el empleo, notificar a los afectados podría ayudar a mantener la confianza del personal de K-C. • En algunas circunstancias, K-C podrá verse obligada por un compromiso contractual a informar a las personas (p. ej., si K-C recibió los datos de un tercero, podrá hacerlo según las condiciones del acuerdo de uso compartido de datos). Sin embargo, usted deberá comparar estas consideraciones con el riesgo de brindar "notificación excesiva", la cual podría provocar una alarma indebida si solo una pequeña cantidad de personas se hubiera visto afectada y/o los datos ya se hubieran recuperado.	Sin retraso indebido (tenga en cuenta que esto podría ser en menos de 72 horas).

Tenga en cuenta que el umbral para notificar a la DPA es más bajo que el umbral para informar a las personas afectadas, por lo cual, tal vez deba informar a la DPA aunque no notifique a las personas. La siguiente orientación

sobre evaluación de riesgos lo ayudará a decidir si uno o ambos pasos son necesarios.

CÓMO REALIZAR UNA EVALUACIÓN DE RIESGOS

Toda evaluación de riesgos deberá enfocarse en estos dos elementos clave:

1) qué tan graves o significativas son las consecuencias adversas; y

2) qué probabilidades hay de que ocurran.

Las siguientes preguntas podrían formar parte de la evaluación de riesgos:

- ¿Qué tipos de datos están implicados y, en particular, que tan "sensibles" son? Algunos datos pueden ser sensibles debido a su naturaleza muy personal (p. ej., algunos registros de empleo) mientras que otros datos son sensibles debido a lo que podría ocurrir si se usaran de forma indebida (p. ej., información de la cuenta bancaria). Otra información, como una lista de nombres sin contexto, claramente presentaría un riesgo mucho más bajo.
- En caso de pérdida o robo de datos, ¿se cuenta con alguna protección, como por ejemplo el cifrado? Tenga en cuenta que si los datos están cifrados, es muy poco probable que deba informar a las personas (a menos que la contraseña de cifrado también se haya comprometido).
- ¿Qué ha sucedido con los datos? Si los datos hubieran sido robados, podrían usarse con fines que podrían afectar a las personas con las cuales se relacionan esos datos; si los datos se hubieran perdido, esto representaría un tipo diferente de nivel de riesgo.
- Independientemente de lo que haya sucedido con los datos, ¿qué información darían a un tercero sobre la persona? Los datos sensibles podrían significar muy poco para un ladrón oportunista de computadoras portátiles mientras que la pérdida de fragmentos de información aparentemente trivial podría ayudar a un estafador determinado a construir una imagen detallada de otras personas.
- ¿Cuántas personas se vieron afectadas por el incidente? No es necesariamente los riesgos más grandes resultarán de la pérdida de grandes cantidades de datos, pero sí es un factor importante y determinante en la evaluación del riesgo general.
- ¿Quiénes son las personas cuyos datos se vieron afectados? El hecho de que sean clientes, personal o empleados de un proveedor en cierta medida determinará el nivel de riesgo del incidente y, por consiguiente, sus medidas para intentar mitigar dichos riesgos.
- ¿Qué daño puede generarse a las personas? Por ejemplo, ¿pérdida financiera si los datos pudieran usarse para cometer un fraude?
- ¿Qué medidas se tomaron para remediar el incidente? ¿Qué tan seguro está de que fueron efectivas? Por ejemplo, si se hubiera recuperado el dispositivo perdido y no hubiera evidencia de que se hubiera accedido a los datos mientras estaban perdidos, entonces el riesgo para las personas será muy bajo.

Puede suceder que no toda la información que necesita para realizar la evaluación de riesgos esté a su disposición dentro de las 72 horas. Deberá usar la información que esté disponible para realizar la mejor evaluación posible.

Si aún tiene dudas, siempre será mejor notificar a la DPA, aunque con posterioridad el incidente de datos resulte ser de bajo riesgo. A la hora de decidir si notificar a las personas, deberá tener en cuenta el riesgo de brindar "notificación excesiva" (consulte la información anterior).

Cómo notificar a la DPA

Si decide informar a la DPA, la notificación deberá incluir la siguiente información, en la medida que esté disponible, cuando realice la notificación:

- la naturaleza de los datos personales, incluida la cantidad aproximada de registros;
- las categorías y la cantidad aproximada de personas potencialmente afectadas;
- las posibles consecuencias del incidente;
- las medidas que se tomaron y que se tomarán para contener y recuperar el incidente y cualquier otro paso para mitigar la situación;
- si, por motivos excepcionales, la notificación se hubiera enviado después de las 72 horas, una explicación

de los motivos de la demora; y
- los detalles de contacto de algún miembro del Equipo de Gestión de Filtración de Datos.

Es posible que la DPA tenga un formulario estándar para enviar la notificación, por lo cual deberá consultar el sitio web de la DPA antes de hacer la notificación.

El Departamento Legal de K-C siempre deberá revisar la notificación antes de su envío. Si parte de la información se basa en los hallazgos iniciales que aún no se confirmaron, esto deberá aclararse en la notificación. Recuerde que la DPA usará la notificación para decidir si tomar o no medidas formales en contra de K-C, lo cual puede incluir una multa. Por lo tanto, es importante que no diga nada que pueda resultar engañoso o que dañe innecesariamente a K-C.

Si parte de la información anterior no está disponible al momento de la notificación inicial, es mejor solo explicar la situación en lugar de brindar información poco precisa. Puede actualizar a la DPA apenas disponga de la información.

Notificación a las personas afectadas

Si decide informar a las personas afectadas, deberá considerar la forma más adecuada de notificación. Esto variará según las circunstancias del incidente, la logística práctica (es decir, la cantidad de personas afectadas) y la manera en que K-C se comunica habitualmente con las personas.

Si, por cualquier motivo, K-C no puede informar a las personas afectadas, por ejemplo, porque no cuenta con su información de contacto, será necesario emitir una comunicación al público en general. Sin embargo, este paso solo deberá seguirse después de una evaluación muy meditada por parte del Departamento Legal de K-C y el Equipo de Gestión de Crisis Corporativas.

En términos del contenido del aviso, se deberá incluir:

- una breve descripción de cuándo y cómo ocurrió el incidente (y siempre teniendo en cuenta las consideraciones de la seguridad saliente de los sistemas y la confidencialidad de K-C);
- una descripción de los datos implicados;
- detalles de las acciones que ya haya tomado K-C en materia de contención y recuperación;
- consejos sobre el accionar de las personas para protegerse (por ejemplo, cambiar sus contraseñas, etc.); y
- un punto de contacto para enviar consultas adicionales que las personas puedan tener.

PASO (6): EVALUACIÓN DE PROCESOS EXISTENTES Y RESPUESTA

El último paso del Equipo de Gestión de Filtración de Datos es evaluar sus procesos y sistemas actuales, y observar:
- si el incidente fue resultado de una falla sistémica que deba abordarse; y
- qué tan eficaz fue K-C a la hora de responder al incidente.

Estos son dos asuntos distintos, uno relacionado con la prevención y el otro relacionado con la solución.

Si, tras haber realizado la evaluación, el Equipo de Gestión de Filtración de Datos considera que existen debilidades en los sistemas o procedimientos de K-C, este Equipo de Gestión de Filtración de Datos deberá evaluar cómo solucionar estas debilidades a fin de aprender las lecciones de la experiencia pasada. Esto podrá registrarse como un caso del Código de conducta.

Las medidas posibles que podrían tomarse a fin de mejorar las fallas sistémicas incluyen:

- Capacitación en seguridad de los datos y en la respuesta a los incidentes de datos.
- Garantizar líneas de denuncia adecuadas, a fin de que los incidentes puedan identificarse rápidamente y sea posible tomar medidas inmediatas.
- Realizar una auditoría de seguridad a fin de identificar debilidades en los sistemas de K-C. ¿Existen medidas inmediatas que pudieran tomarse para mejorar la seguridad?
- Evaluar los flujos de datos de K-C a fin de garantizar que los datos no se compartan de forma innecesaria y que solo las personas con necesidad de conocimiento tengan acceso a los datos.

- Identificar a un grupo de personas con la responsabilidad continua de gestionar incidentes de datos.

Las preguntas sobre esta adenda pueden remitirse a KC HelpLine en KCHelpLine@kcc.com.

ANEXO 1 A LA ADENDA 5 DE LA POLÍTICA DE PRIVACIDAD Y PROTECCIÓN DE DATOS DE K-C
LISTA DE VERIFICACIÓN DE RESPUESTA A INCIDENTES DE DATOS

Esta lista de verificación está diseñada para ayudar al jefe investigador a garantizar que se completen todas las medidas de la presente adenda.

ACCIÓN	¿COMPLETADA?
PASO (1): BÚSQUEDA INICIAL DE DATOS; DEFINIR SI HA OCURRIDO UN INCIDENTE	
Definir si hubo un incidente que amerite una investigación adicional.	☐
Enviar un registro de la búsqueda inicial de datos al Departamento Legal.	☐
PASO (2): REUNIR AL EQUIPO DE RESPUESTA A INCIDENTES	
Reunir al Equipo de Gestión de Filtración de Datos.	☐
PASO (3): CONTENCIÓN Y RECUPERACIÓN	
Investigar más a fondo el incidente a fin de establecer qué puede hacerse para contener la situación.	☐
Establecer si existe algo que usted pueda hacer para recuperar las pérdidas y limitar el daño que el incidente pueda provocar.	☐
Cuando corresponda, informar a la policía.	☐
PASO (4): REALIZAR UNA INVESTIGACIÓN FORMAL	
Documentar los resultados de la investigación en un informe por escrito para el Departamento Legal de K-C.	☐

PASO (5): NOTIFICACIÓN DE INCIDENTES	
Realizar una evaluación de riesgos para decidir si debe informar a la DPA.	☐
Realizar una evaluación de riesgos para decidir si debe informar a las personas afectadas.	☐
Actualizar el informe de investigación a fin de registrar los resultados de las evaluaciones de riesgos.	☐
Completar la notificación.	☐
Decidir la forma y el contenido de las notificaciones a las personas.	☐
Enviar o publicar (según corresponda) la notificación a las personas.	☐
PASO (6): EVALUACIÓN DE PROCESOS EXISTENTES Y RESPUESTA	
Identificar y documentar los cambios necesarios en los sistemas y/o procedimientos existentes.	☐
Designar responsables para cada cambio y garantizar que se implementen.	☐

ADENDA 6 DE LA POLÍTICA DE PRIVACIDAD Y PROTECCIÓN DE DATOS DE K-C

ACTIVIDADES DE MARKETING DIRECTO

INTRODUCCIÓN Y ALCANCE

La Política de privacidad y protección de datos de K-C define los 9 principios de la protección de datos que K-C deberá cumplir a la hora de procesar datos personales.

Esta adenda incluye información adicional sobre cómo aplicar cada uno de los 9 principios de la protección de datos a la hora de procesar datos personales a los fines de realizar **marketing directo**. Entre otros aspectos, la adenda aborda la recopilación de datos personales que se usarán con fines de marketing, el mantenimiento de un registro de los consentimientos de marketing, la selección de los destinatarios de una campaña de marketing, el envío de comunicaciones de marketing y la gestión de las opciones de exclusión.

"**Marketing directo**" significa comunicarse con los consumidores de K-C que interactúan directamente con las marcas de K-C (los "**clientes**") a fin de promocionar los productos de K-C. Esto incluye, entre otros, el contacto por correo electrónico, SMS, mensajes push, redes sociales o correo postal. Esta adenda **no** abarca el uso de datos personales con fines de publicidad en línea con minoristas o publicidad no dirigida (p. ej., periódico, anuncios de televisión o páginas de redes sociales).

Esta adenda se aplica a todo el personal que procesa datos personales con fines de marketing.

Consulte el Apéndice A de la Política de privacidad y protección de datos de K-C para acceder a un glosario de los términos que se definen en la presente adenda.

RECOPILACIÓN DE DATOS PERSONALES CON FINES DE MARKETING

1. DAR AVISO DEL MARKETING

Cuando se recopilen datos personales a través del sitio web de K-C o cualquier otro medio, la forma que se utilice para recopilar los detalles de contacto del consumidor deberá dejar clara al cliente la siguiente información:

- que, si otorga su consentimiento, sus datos personales se usarán con fines de marketing;
- de quiénes podrá recibir información de marketing (p. ej., K-C solamente, otras marcas u otros socios de K-C);
- cómo puede retirar su consentimiento para recibir información de marketing; y
- un enlace al Aviso de privacidad en línea de K-C.

2. OBTENER LA AUTORIZACIÓN PARA LAS ACTIVIDADES DE MARKETING

K-C solo deberá enviar información de marketing a los clientes cuando haya obtenido el **consentimiento previo** del cliente. Este consentimiento debe otorgarse de forma voluntaria, ser específico e informado.

- **Otorgado de forma voluntaria:** el cliente debe hacer una elección genuina de otorgar o no el consentimiento para participar en las actividades de marketing. Esta podría ser la elección de brindar o no sus detalles de contacto de forma plena (por ejemplo, la opción de brindar una dirección de correo electrónico para recibir correos electrónicos de marketing), o la opción "Sí" para recibir información de marketing. No debe obligarse al cliente a otorgar su consentimiento para participar en las actividades de marketing a fin de recibir, por ejemplo, una muestra del producto *Depend* y, en este ejemplo, K-C deberá obtener un consentimiento de marketing por separado (por lo general, mediante una casilla de selección o una pregunta por separado).

- **Específico:** este consentimiento deberá limitarse al marketing de una parte o de partes específicas. K-C podría obtener el consentimiento para comercializar en nombre de otras marcas de K-C, siempre y cuando esto sea aclarado y aquellas empresas de K-C Group que puedan enviar información de marketing se mencionen ya sea en la redacción del consentimiento o sea posible acceder a ellas a través de un enlace. Consulte a continuación para obtener más lineamientos sobre el uso compartido dentro de K-C Group con fines de marketing.
  El consentimiento también deberá especificar qué canales de comunicaciones se utilizarán para enviar información de marketing al cliente; se deberá permitir a los clientes elegir de qué canales de comunicación desean recibir información de marketing (p. ej., casillas de selección separadas en el caso de correo electrónico o mensajes de texto [Short Message Service, SMS]). El consentimiento para participar en actividades de marketing no debe "combinarse" con otros consentimientos, por ejemplo, el consentimiento de los Términos y condiciones, o para recibir encuestas para el cliente.

- **Informado:** el cliente deberá recibir la información definida anteriormente, incluido un enlace al Aviso de privacidad en línea de K-C o cómo encontrarlo. La redacción del formulario, el guion del centro de llamadas o la interacción con el cliente deberán dejar en claro al cliente que, por medio de su accionar, otorga su consentimiento para recibir información de marketing. Usted debe evitar el uso de negaciones dobles u otro lenguaje que pueda dar lugar a confusión.

Tenga en cuenta que una comunicación directa a los clientes para preguntarles si desean recibir mensajes de marketing será, por sí misma, una comunicación de marketing. Por lo tanto, aún se aplicarán los mismos requisitos para dar aviso, obtener el consentimiento y respetar cualquier opción de exclusión.

En los caso en que K-C contrate a un tercero para recopilar consentimientos de marketing en su nombre, K-C deberá asegurarse de que dicho tercero pueda brindar prueba documental de que se obtuvieron tales consentimientos conforme a los requisitos de esta adenda.

DECIDIR QUÉ DATOS PERSONALES RECOPILAR

Recopile solamente datos personales que sean adecuados, pertinentes y que no resulten excesivos a los fines del envío de información de marketing. Toda información que se recopile exclusivamente con fines de personalizar el marketing según el individuo deberá ser opcional e identificarse como tal de forma clara (por ejemplo, información sobre sus intereses, preferencias o circunstancias familiares).

No recopile datos personales simplemente porque pudieran ser útiles para una campaña de marketing aún no especificada. Por ejemplo, no deberá solicitar a los clientes su dirección postal si no existe una perspectiva realista de que K-C envíe comunicaciones de marketing por correo postal.

No use datos personales sensibles, incluida la información de salud, con fines de marketing. Pero puede enviarle a un cliente algo que este haya solicitado específicamente (p. ej., un muestra de *Depend*).

REALIZACIÓN DE UNA CAMPAÑA DE MARKETING DIRECTO (POR CORREO POSTAL, CORREO ELECTRÓNICO, TELÉFONO O REDES SOCIALES)

No debe llevar adelante campañas de marketing dirigidas a niños menores de 16 años.

Si envía comunicaciones de marketing por correo electrónico, mensajes de texto o redes sociales, solo deberá enviar la comunicación cuando los detalles de contacto se hayan recopilado de conformidad con esta adenda (véase la información anterior).

Cada mensaje de marketing deberá:

- identificar claramente a K-C como el remitente; y

- proporcionar al cliente una opción de exclusión sencilla, a través del mismo canal de comunicación que el de la comunicación propiamente dicha. Por consiguiente:

  - Correo electrónico: incluya un enlace para "eliminar la suscripción" en la parte inferior del correo electrónico.
  - Mensajes de texto: los usuarios deben poder enviar la palabra "STOP" (Detener) a un número (y el único costo deberá ser el costo del mensaje).
  - Teléfono: el personal del centro de llamadas deberá estar capacitado y poder registrar las solicitudes de opción de exclusión que se realicen durante la llamada telefónica.
  - Correo postal: incluya una dirección postal y una dirección de correo electrónico o un número de teléfono gratuito que el cliente pueda utilizar para eliminar su suscripción.
  - Redes sociales: permita a las personas eliminar la suscripción mediante un mensaje de respuesta o dé instrucciones sobre cómo una persona puede eliminar su suscripción (p. ej., por medio de una solicitud por correo electrónico).

Gestión de las opciones de exclusión

Resulta esencial que toda campaña de marketing directo tenga un proceso para responder rápidamente a las solicitudes de opción de exclusión. Se deberá llevar un registro de todas las opciones de exclusión, a fin de que pueda usarse para filtrar cualquier campaña de marketing subsiguiente. Es importante que no elimine los datos del cliente por completo, ya que no puede asegurarse de que la persona no recibirá con posterioridad información de marketing de otra fuente. A la hora de gestionar las opciones de exclusión:

- Envíe al cliente un mensaje (por el mismo medio de comunicación) para confirmar que la opción de exclusión se haya procesado con éxito. En el caso de un enlace de "eliminar la suscripción" automatizado o cuando un cliente actualice sus preferencias dentro de una cuenta, es suficiente mostrar una confirmación en la pantalla en el momento. También se deberá informar al cliente si existiera la posibilidad de algún retraso hasta que la opción de exclusión entrara en vigencia (es decir, si continuará recibiendo información de marketing durante un período breve).

- No se contacte con posterioridad con el cliente para consultarle si desea recibir marketing directo.

CREACIÓN DE PERFILES DE CLIENTES CON FINES DE MARKETING

La "**creación de perfiles**" hace referencia al uso de datos personales para evaluar o sacar conclusiones sobre los intereses, la conducta o las circunstancias de los clientes. Los ejemplos incluyen inferir las circunstancias sociales o familiares de un cliente o el posible poder adquisitivo.

Se deberá **informar** a los clientes que sus datos personales podrán utilizarse para crear un perfil suyo, el cual podrá emplearse con fines de marketing (así como también con otros fines). Cuando el cliente haya interactuado con K-C en línea, resulta suficiente ampararse en el Aviso de privacidad en línea de K-C, el cual deberá incluir información específica sobre la creación de perfiles de clientes por parte de K-C a los fines de enviar comunicaciones de marketing.

En el caso de que el cliente haya interactuado con K-C solamente fuera de línea, se le deberá indicar que revise el Aviso de privacidad en línea de K-C.

K-C lleva adelante la creación de perfiles de clientes sobre la base de que esto resulta necesario para el interés legítimo de K-C, para decidir (entre otros aspectos) qué comunicaciones de marketing enviar a un cliente en particular. A fin de que este interés legítimo no sea invalidado por ningún prejuicio hacia los clientes, toda creación de perfiles de clientes debe estar sujeta a las siguientes salvaguardas:

- La creación de perfiles de clientes solo deberá basarse en la información que el cliente tenga la expectativa razonable de que pueda usarse con fines de marketing y que esté clasificada dentro de las actividades de creación de perfiles descritas en el Aviso de privacidad en línea de K-C (o cualquier aviso adicional).

- No deberán usarse datos personales sensibles para la creación de perfiles de clientes.

- Los clientes tienen derecho a objetar el uso de su información para crear un perfil suyo con fines de marketing. Siempre que sea posible, K-C deberá permitir a los clientes objetar la creación de perfiles mediante el autoservicio, por ejemplo, a través de la configuración de una cuenta en línea. Sin embargo, en el caso de que un cliente se comunique directamente con K-C para objetar la creación de perfiles (p. ej., una solicitud por escrito), K-C deberá cumplir con dicha solicitud y responder al cliente para confirmar esto dentro de los 30 días. Usted deberá conservar un registro de la objeción. Para obtener más información, consulte la *Adenda 2 de la Política de privacidad y protección de datos de K-C* (*Derechos individuales*).

- Antes de llevar adelante cualquier actividad nueva relacionada con la creación de perfiles de clientes, K-C deberá completar una Evaluación del impacto de la protección de datos. Para obtener más información, consulte la *Adenda 1 de la Política de privacidad y protección de datos de K-C* (*Evaluaciones del impacto de la protección de datos*).

PUBLICIDAD PROGRAMÁTICA (TAMBIÉN CONOCIDA COMO "PUBLICIDAD DIRIGIDA EN LÍNEA")

La "publicidad programática" o "publicidad dirigida en línea" es la utilización de la información sobre las actividades en línea de un individuo a fin de personalizar la publicidad en línea que se brinda a ese individuo según sus intereses. La publicidad programática funciona mediante el uso de "cookies" y otras tecnologías de rastreo similares. Las cookies son pequeños archivos de texto que un servidor coloca en la computadora de un individuo (y que se enlazan al navegador de la persona), los cuales transmiten información al servidor sobre los sitios que la persona visita. Por lo general, la información recopilada incluye los sitios y las páginas web específicas que la persona visita, el tiempo dedicado a la navegación en esos sitios o páginas, la fecha y hora de las visitas y si la persona observó los anuncios que se le brindaron.

K-C podrá colocar estos tipos de tecnologías de seguimiento en los dispositivos de los clientes cuando visiten un sitio web de K-C. De forma alternativa, K-C podrá también contratar a proveedores externos de servicio publicitario en línea, como "redes de publicidad", quienes podrán colocar publicidades dirigidas relacionadas con productos de K-C en otros sitios web. Debido a que este tipo de publicidad tiene la posibilidad de recopilar datos personales y crear perfiles detallados de las personas, es importante que:

- solo trabajemos con proveedores con reputación con programas de privacidad y protección de datos definidos.
- garanticemos que comprendemos las medidas que dichos proveedores han implementado a fin de proteger los derechos de privacidad de las personas.
- solo trabajemos con proveedores que brinden a las personas un mecanismo adecuado para otorgar y retirar su consentimiento respecto de las cookies (y tecnologías similares) usadas para recibir publicidades dirigidas.
- garanticemos que todo publicista mediante el cual se definen las cookies de K-C incluya un aviso de privacidad/cookies adecuado que describa tales cookies de terceros y que obtengamos el consentimiento correspondiente de los usuarios finales.

MANTENER DATOS DE MARKETING PRECISOS Y ACTUALIZADOS

Los datos personales que se utilizarán con fines de marketing deben ser precisos, completos y estar lo más actualizados posible. Además de exponer a K-C a riesgos de acciones regulatorias, conservar grandes cantidades de datos personales que podrían ser inexactos, estar desactualizados o que K-C ya no necesite expone a la empresa a mayores riesgos en términos de una violación de seguridad.

Depuración de datos

Cuando tenga en su poder datos personales que se usen con fines de marketing, deberá revisarlos periódicamente a fin de determinar si continúan siendo precisos. Es poco probable que la información poco precisa o desactualizada resulte útil a los fines de marketing y puede generar comunicaciones desperdiciadas y posibles quejas de los clientes.

Cuando sea posible, los clientes deben poder actualizar o rectificar su propia información de marketing. Por ejemplo, los clientes deben poder actualizar sus preferencias de marketing y cambiar sus detalles de contacto dentro de su cuenta en línea. Además, los clientes podrán solicitar que K-C rectifique todos los datos personales imprecisos a través de una comunicación directa con K-C (p. ej., mediante los detalles de contacto de la Política de privacidad). K-C deberá cumplir con la solicitud y responder al cliente a fin de confirmar esto dentro de los 30 días. Para obtener más información, consulte la *Adenda 2 de la Política de privacidad y protección de datos de K-C* (*Derechos individuales*).

Plazos y eliminación

Si K-C deja de necesitar un conjunto de datos personales con fines de marketing, usted deberá eliminarlos de forma permanente (o anonimizarla, si K-C aún tiene el propósito legítimo de conservar la información anónima).

COMPARTIR DATOS PERSONALES CON OTRAS EMPRESAS DE K-C GROUP CON FINES DE MARKETING

Los datos personales podrán compartirse con otros integrantes de K-C Group para que otras empresas de K-C Group los utilicen ***para sus propios*** fines de marketing en las siguientes circunstancias:

- si se ha **informado** al cliente que los datos personales se compartirán con otras marcas/empresas de K-C Group con fines de marketing; ***y***

- si el cliente ha otorgado su **consentimiento** general para recibir información de marketing de otras marcas/empresas de K-C Group, o el consentimiento específico para recibir información de marketing de la empresa de K-C Group destinataria, conforme a los requisitos de consentimiento antes mencionados.

Usted solo deberá compartir la cantidad mínima de datos personales necesaria para la actividad de marketing específica que se haya acordado entre las empresas de K-C Group. Por ejemplo, si la empresa de K-C Group destinataria solo tiene previsto realizar una campaña de marketing por correo electrónico, usted no deberá compartir además los números de teléfono celular de los clientes.

No deberá compartir datos personales sensibles con otras empresas de K-C Group con fines de marketing.

Cuando el uso compartido sea del tipo que K-C no haya realizado con anterioridad (ya sea un nuevo conjunto de datos o para un nuevo fin de marketing), K-C deberá realizar una Evaluación del impacto de la protección de datos. Para obtener más información, consulte la *Adenda 1 de la Política de privacidad y protección de datos de K-C* (*Evaluaciones del impacto de la protección de datos*).

K-C puede compartir datos personales con otra empresa de K-C Group, o recibirlos de esta, con fines de marketing sin el consentimiento previo del cliente cuando la empresa de K-C Group destinataria actúe en calidad de proveedor, realice actividades de marketing en nombre de K-C y conforme a sus instrucciones. En estas circunstancias, usted deberá cumplir con los requisitos de contratación de un proveedor que se definen a continuación.

COMPARTIR DATOS PERSONALES CON UN PROVEEDOR QUE BRINDA SERVICIOS DE MARKETING

A la hora de contratar a un proveedor que procesará datos personales en nombre de K-C a fin de brindar servicios de marketing, usted deberá garantizar que el proveedor también cumplirá con los requisitos de esta adenda y que no impedirá que K-C también los cumpla. En resumen, usted deberá:

- llevar adelante la diligencia debida correspondiente antes de contratar al proveedor a fin de garantizar que pueda cumplir con los altos estándares que K-C espera de sus proveedores en términos de la protección de datos y la seguridad de la información;

- celebrar un contrato por escrito con el proveedor que incluya las condiciones del procesamiento de datos, las cuales deberán cumplir con los requisitos de la ley aplicable;

- monitorear el cumplimiento continuo de las obligaciones del proveedor y garantizar que todo incumplimiento se solucione de forma oportuna o que se interrumpa la contratación; y

- si el proveedor se encuentra fuera del Espacio Económico Europeo (European Economic Area, **EEA**), implementar una solución de transferencia de datos que cumpla con los requisitos de la ley aplicable.

Para obtener instrucciones más detalladas sobre la designación de proveedores que tendrán acceso a datos personales, deberá consultar la *Adenda 3 de la Política de privacidad y protección de datos de K-C* (*Designación de proveedores*).

Solo comparta datos personales con el proveedor en la medida que resulte necesario para que este brinde los servicios a K-C. Por ejemplo, si el tercero solo enviara marketing por correo electrónico, no habrá necesidad de compartir además los números de teléfono.

Si el proveedor recopila datos personales en nombre de K-C (es decir, interactúa con los clientes de forma directa), usted deberá asignar obligaciones del proveedor que reflejen las obligaciones de K-C, por ejemplo para dar aviso a los clientes y (cuando sea necesario) obtener el consentimiento en nombre de K-C. Por ejemplo, si el proveedor opera un centro de llamadas donde se obtienen los consentimientos de marketing, usted deberá garantizar que tales consentimientos obtenidos por el personal del proveedor, en nombre de K-C, cumplan con los requisitos de esta adenda.

Si el proveedor envía comunicaciones de marketing por sí mismo en nombre de K-C, usted deberá asignar obligaciones del proveedor que reflejen las obligaciones de K-C, por ejemplo, para identificar a K-C como emisor y ofrecer una opción de exclusión.

Es importante que no se permita al proveedor el uso de los datos personales a fin de comercializar en su propio nombre, ni que los comparta con nadie más (por ejemplo, con sus otros clientes).

Proveedores fuera del EEA

Si los servicios que brinda el proveedor implican el procesamiento de datos personales fuera del EEA (incluidas las circunstancias en las que se pueda acceder a estos datos de forma remota desde afuera del EEA), usted deberá continuar solo si se ha implementado un mecanismo adecuado de transferencia de datos. Deberá consultar a su líder de protección de datos para obtener información sobre el mecanismo de transferencia más adecuado para el acuerdo.

Las preguntas sobre esta adenda pueden enviarse al líder de protección de datos correspondiente.

ADENDA 7 DE LA POLÍTICA DE PRIVACIDAD Y PROTECCIÓN DE DATOS DE K-C
DATOS DEL PERSONAL

1. INTRODUCCIÓN

1.1 La Política de privacidad y protección de datos de K-C define los Principios de la protección de datos que K-C debe cumplir a la hora de procesar datos personales, incluida su recopilación, uso, divulgación y eliminación.

1.2 Esta adenda incluye información adicional sobre cómo garantizar el cumplimiento de los 9 principios de la protección de datos de K-C en el contexto del **empleo y la selección** ("**Datos del personal**"). Esto abarca los datos personales del personal de K-C así como también de nuestro personal externo (p. ej., consultores, contratistas, trabajadores de agencias temporales, estudiantes y asesores externos) y de beneficiarios o dependientes del personal actual y del pasado.

1.3 En esta adenda se brindan ejemplos y orientación de problemas comunes de protección de datos a la hora de manejar los datos del personal. Se divide en las siguientes secciones:

- Procesamiento de datos del personal para la selección;
- Procesamiento de datos del personal dentro de K-C;
- Compartir datos del personal fuera de K-C.

1.4 Esta adenda se aplica a todo el personal que procesa datos del personal.

1.5 Consulte el Apéndice A de la Política de privacidad y protección de datos de K-C para acceder a un Glosario de los términos que se definen en la presente adenda.

1. PROCESAMIENTO DE DATOS DEL PERSONAL PARA LA SELECCIÓN

1. ANUNCIO DE VACANTES

Todas las vacantes, cuando sea posible, deberán anunciarse a través de WorkDay en Kimberly-Clark.com. Esto se debe a que WorkDay ha sido configurado para cumplir con los requisitos de la ley de protección de datos.

Sin embargo, es posible que existan ocasiones en las que una vacante se anuncie a través de otros métodos, p. ej., formularios de postulación impresos. En estas circunstancias, usted deberá asegurarse de que el anuncio de trabajo identifique a la entidad de K-C que será la empleadora. Si, por algún motivo en particular, no se identificara a la entidad de K-C correspondiente en el anuncio, se deberá notificar a los postulantes la identidad del empleador dentro de un período razonable de la recepción de la postulación.

2. FORMULARIOS DE POSTULACIÓN

2.1 Dar aviso

Cuando se recopilen datos del personal, se deberá brindar el *Aviso de privacidad de selección de K-C* para ayudar a garantizar que se **informe** adecuadamente a las personas cómo se utilizarán sus datos personales. Si por algún motivo esto no pudiera brindarse al principio, deberá proporcionarse al postulante lo antes posible después de ese momento.

El *Aviso de privacidad de selección de K-C* se brinda automáticamente a los postulantes que se postulen para un trabajo con nosotros a través de nuestro sitio web.

2.2 Postulaciones recibidas a través de un tercero

2.2.1 Cuando los datos del personal se obtengan de un tercero (p. ej., una agencia de selección), K-C deberá otorgar al postulante el Aviso de privacidad de selección de K-C dentro de un período razonable tras recibir los datos personales y al menos: (a) al momento del primer contacto directo de K-C con el postulante; o (b) dentro de un mes después de recibir los datos del personal, lo que suceda primero.

2.2.2 K-C no tiene la obligación de proporcionar la información anterior si fuera imposible o si implicara un esfuerzo desproporcionado (p. ej., debido a que no contáramos con los detalles de contacto del postulante).

2.2.3 Si está trabajando con una nueva agencia de selección por primera vez, asegúrese de cumplir con la *Adenda 3 de la Política de privacidad y protección de datos de K-C* (*Designación de proveedores*).

2.3 Decidir qué datos del personal recopilar

2.3.1 WorkDay ha sido configurado para ayudar a garantizar que, cuando recopilemos datos del personal, solo solicitemos datos personales que sean adecuados, relevantes y no excesivos. Estos mismos principios se aplican si usted recopila datos del personal a través de cualquier otro medio alternativo. Esto significa que solo debe recopilar información que sea **necesaria para evaluar** a la persona para el puesto para el cual se postula. Las personas podrán proporcionar información no necesaria **de forma voluntaria**, pero, cuando sea posible, usted deberá limitar esto (por ejemplo, proporcionando una lista de opciones en lugar de campos de texto libre).

2.3.2 No deberá recopilarse información sobre condenas penales (cumplidas y no cumplidas) ni datos personales sensibles de la persona, a menos que K-C cuente con el permiso legal para hacerlo. Si tiene alguna duda, consulte al abogado superior de Empleo y Trabajo para Europa, Oriente Medio y África (Europe, the Middle East and Africa, EMEA) del Departamento Legal de K-C.

2.3.3 Solo deberá recopilar datos personales sensibles cuando sean absolutamente necesarios y cuente con el permiso legal para ello y solo en la etapa más avanzada posible del proceso de selección.

3. PRESELECCIÓN Y SELECCIÓN DE CANDIDATOS

3.1 Verificación de antecedentes

3.1.1 La “Verificación de antecedentes” es el proceso por el cual K-C verifica los datos del personal provistos durante el proceso de selección, por ejemplo, mediante la comprobación de las calificaciones académicas y /o la recopilación de información de fuentes externas, como exempleadores. K-C debe informar a las personas que estarán sujetas a la Verificación de antecedentes. En algunos casos, también será necesario obtener el consentimiento de la persona antes de comunicarse con la parte que verificará la información.

3.1.2 Si se debe realizar una Verificación de antecedentes, se deberán seguir los siguientes pasos:

- Dar aviso a las personas con anticipación que se hará la Verificación de antecedentes.
- La información sobre condenas penales (si se recopila) solo deberá obtenerse a través de fuentes autorizadas y cuando se cuente con el permiso legal correspondiente (si tiene alguna duda, comuníquese con el abogado superior de Empleo y Trabajo para EMEA del Departamento Legal de K-C), inclusive cuando la persona haya otorgado su consentimiento explícito e informado y la información pueda justificarse para el puesto específico ofrecido.

- Comuníquese con fuentes externas únicamente cuando la persona haya otorgado su consentimiento primero (si la fuente externa en cuestión exige este consentimiento). Si la persona no ha otorgado ese consentimiento, usted no podrá comunicarse con la fuente externa (si tiene alguna duda, comuníquese con el abogado superior de Empleo y Trabajo para EMEA del Departamento Legal de K-C).

- Se deberá informar a las personas si la Verificación de antecedentes mostrara alguna discrepancia que tenga un impacto negativo en su postulación. Las personas también deben tener la oportunidad de explicar estas discrepancias.

Además, toda Verificación de antecedentes también deberá:

- llevarse a cabo ***solamente*** cuando sea genuinamente necesario. No será proporcionado ni necesario realizar la Verificación de antecedentes cuando una persona se postule para un puesto administrativo sin acceso a información confidencial o sensible, mientras que la Verificación de antecedentes puede ser adecuada para los puestos con acceso a información comercial y financiera sensible; y

- estar dirigida a la recopilación de información específica y no general.

3.2 Pruebas de detección de drogas y alcohol

Están estrictamente prohibidas las pruebas de detección de drogas y alcohol de los postulantes en determinadas jurisdicciones, a menos que exista la necesidad genuina debido a la posición para la cual se postulen. Por ejemplo, podrán justificarse las pruebas a los postulantes que, si realizan una postulación exitosa, tendrían acceso a maquinarias o a quienes se les podría solicitar que conduzcan para cumplir con su función. En estas circunstancias continúan aplicándose las pautas según se definen en el párrafo 1 anterior. En cambio, resulta poco probable que se consideren adecuadas las pruebas a postulantes que se postulen para funciones en una oficina en determinadas jurisdicciones. Si tiene alguna duda con respecto a si es o no adecuado solicitarle a un postulante que se someta a una prueba de detección de drogas y/o alcohol, comuníquese con el abogado superior de Empleo y Trabajo para EMEA del Departamento Legal de K-C.

3.3 Entrevistas a los candidatos

Durante el proceso de entrevistas, solamente recopile la información que sea relevante para el trabajo para el cual se postula el candidato. Recuerde que la persona tiene derecho a solicitar una copia de sus datos personales que puedan estar incluidos en cualquier nota de la entrevista.

4. RETENCIÓN DE LOS REGISTROS DE SELECCIÓN

Los documentos de selección (p. ej., postulaciones por escrito, CV, notas de la entrevista) deben manejarse de acuerdo con la *Adenda 8 de la Política de privacidad y protección de datos de K-C (Retención de datos)* la cual hace referencia a la Política de retención de documentos de K-C.

El plazo durante el cual pueden retenerse los documentos de selección dependerá de si la persona tiene un resultado exitoso o no en su postulación de trabajo.

- Si una persona tiene un resultado **exitoso** en su postulación de trabajo y acepta el puesto, los datos del personal recopilados durante su selección se deberán almacenar en el archivo de personal del individuo. El período de retención de este archivo, por lo general, será el plazo de empleo de la persona más 7 años.

- Si una persona tiene un resultado **no exitoso** en su postulación de trabajo (o rechaza el puesto), la mayoría de sus datos del personal deberá destruirse después de 7 meses (a menos que la persona otorgue su permiso para que se retenga su CV o currículum en el archivo).

2. PROCESAMIENTO DE DATOS DEL PERSONAL DENTRO DE K-C

Esto incluye actividades relacionadas con la relación laboral, como las siguientes:

- asignación del personal a los proyectos o la programación de trabajo;
- gestión de activos y pasivos de la empresa;
- evaluación y capacitación;
- pago de salarios y administración de beneficios (incluidos los viajes de personal);
- administración de esquemas de pensión y seguro de salud privado;
- administración y desarrollo de carreras (incluida la administración de talentos);
- análisis de empleo (por ejemplo, comparación del éxito de diferentes programas de selección y/o retención de personal);
- manejo de quejas formales o procedimientos disciplinarios;
- monitoreo de igualdad de oportunidades;
- planificación de carrera profesional y ascensos; y
- prevención de fraude y otros delitos.

1. <u>RECOPILACIÓN DE DATOS DEL PERSONAL DURANTE LA RELACIÓN LABORAL</u>

1.1 Dar aviso

1.1.1 Cada vez que se recopilen datos del personal, de forma directa o indirecta, se deberá **informar** adecuadamente al personal cómo se usarán sus datos personales. Por lo general, este requisito se cumplirá al proporcionar el acceso al Aviso para el personal sobre la protección de datos de K-C, el cual está disponible en la intranet de K-C. Usted deberá garantizar que se indique a los nuevos empleados que revisen este Aviso.

1.1.2 Cuando los datos personales se obtengan de forma indirecta, es decir, de otro individuo que no sea la persona en cuestión, usted no tiene la obligación de dar aviso si fuera imposible hacerlo (p. ej., cuando se desconoce la dirección de correo electrónico o el domicilio particular de la persona) o si hacerlo implicara un esfuerzo desproporcionado (p. ej., cuando hay un gran volumen de información no intrusiva, como detalles de contacto de emergencia de terceros provistos por el personal de K-C).

1.2 ¿Con qué propósitos pueden recopilarse los datos del personal?

1.2.1 Los datos del personal solo deberán recopilarse para actividades relacionadas con la relación laboral (se brinda una lista ilustrativa de tales actividades al inicio de la sección 2). Recopile solamente datos del personal que sean necesarios para propósitos específicos. Por ejemplo, no recopile datos del personal solamente porque podrían ser útiles en el futuro, para un propósito aún no especificado.

1.2.2 Si tiene la intención de usar los datos del personal de una forma diferente del (de los) propósito(s) comunicado(s) a la persona cuando se recopilaron, deberá dar al individuo un aviso adicional a fin de explicar el (los) cambio(s) propuesto(s), los motivos para hacerlo y toda posible consecuencia para esta persona. Según la naturaleza del nuevo uso, es posible que sea necesario obtener el consentimiento de la persona antes de implementar el cambio propuesto.

1.2.3 Si existe la posibilidad de que el nuevo propósito cause alto riesgo para el personal, K-C deberá realizar una Evaluación del impacto de la protección de datos. Para obtener más información, consulte la *Adenda 1 de la Política de privacidad y protección de datos de K-C (Evaluaciones del impacto de la protección de datos)*.

1.3 Registros de inasistencia y enfermedad

La información relacionada con los registros de inasistencia y enfermedad deberá manejarse con particular referencia a lo siguiente:

1.3.1 El acceso debe limitarse estrictamente al personal con una "necesidad de conocimiento" comercial legítima o legal (inclusive en los casos en que tales registros sean administrados por un proveedor externo), por ejemplo, si un gerente de línea necesita acceder al registro de una persona bajo su responsabilidad a fin de investigar las inasistencias repetidas o prolongadas.

1.3.2 Deberá registrarse la cantidad mínima de información necesaria. En muchas circunstancias, no será necesario registrar detalles de la enfermedad particular de la persona, solamente un registro de su inasistencia (por ejemplo, vacaciones, licencia por maternidad o paternidad, enfermedad, etc.). Deberán recopilarse detalles adicionales de la inasistencia si fuera necesario ayudar a que K-C cumpla con su obligaciones de conformidad con la legislación en materia de igualdad (por ejemplo, a fin de brindar los ajustes razonables) o con su deber de cuidado como empleador.

1.3.3 Los registros de inasistencia y enfermedad solo deben divulgarse fuera de K-C si:

- existe una obligación jurídica para hacerlo;
- fuera necesario para procedimientos judiciales;
- la persona hubiera otorgado el consentimiento explícito para la divulgación. Esto significa que se le debe haber dado a la persona la opción genuina acerca de la posibilidad de compartir los registros con un tercero especificado, para un propósito particular; o
- de lo contrario, con la aprobación del abogado superior de Empleo y Trabajo para EMEA del Departamento Legal de K-C.

1.4 Monitoreo de igualdad de oportunidades

1.4.1 Los datos del personal recopilados para el monitoreo de igualdad de oportunidades pueden incluir datos personales sensibles. Tales datos personales solo deben usarse para el propósito de monitoreo de igualdad de oportunidades o, de otro modo, según lo exija la legislación vigente.

1.4.2 Asegúrese de que las preguntas se diseñen de forma tal que la información recopilada no resulte excesiva. Cuando sea posible, utilice campos predefinidos en lugar de casillas de texto libre. Sin embargo, asegúrese de que los campos predefinidos tengan opciones suficientes para permitirle elegir al personal la opción que los refleje de forma precisa. Para cada pregunta siempre deberá proporcionar una opción para el personal que prefiere no responder.

1.5 Monitoreo del personal

1.5.1 Se debe informar al personal si estará sujeto a monitoreo. Algunos ejemplos de monitoreo incluyen el control de internet y del correo electrónico, como también el uso del circuito cerrado de televisión (Closed Circuit Television, CCTV). La información que se brinde a las personas debe ser lo suficientemente detallada para asegurarse de que el personal comprenda lo siguiente:

- cuándo podrá obtenerse información sobre las personas, por ejemplo:
  - el uso del correo electrónico, incluido (cuando lo permita la legislación vigente) el contenido de los correos electrónicos;
  - la actividad de navegación en la red e internet;
  - el uso de otros equipos de K-C (p. ej., teléfonos celulares); y/o
  - sus movimientos dentro de las instalaciones de K-C;

- por qué se realiza el monitoreo;
- cómo puede usarse esta información; y
- a quién puede divulgarse.

1.6 Limitación de propósitos y mantenimiento de datos del personal de forma precisa y segura

1.6.1 **Limitación de propósitos**: no acceda a los datos del personal ni los utilice para propósitos que no sean compatibles con los propósitos para los cuales se obtuvieron originalmente (por ejemplo, no acceda a los datos del personal ni los use en relación con una investigación disciplinaria o de quejas formales si esto no fuera compatible con el fin para el cual se hayan obtenido, o si resultara desproporcionado para el asunto en investigación).

1.6.2 **Precisión**: K-C le permite al personal enmendar y corregir algunos de sus propios datos personales mediante el "autoservicio" a través de WorkDay. Se deberá recordar al personal que revise su información dentro de WorkDay con regularidad e informar a RR. HH. si fuera necesario actualizar otra información que no pudiera actualizarse a través de WorkDay.

No deberán retenerse registros de acusaciones sin fundamentos a menos que existan motivos excepcionales para hacerlo (si necesitara confirmarlo, debería comunicarse con el abogado superior de Empleo y Trabajo para EMEA del Departamento Legal de K-C).

1.6.3 **Seguridad**: se deben implementar medidas apropiadas de seguridad físicas (p. ej., gabinetes con llave), técnicas (p. ej., contraseñas, cifrado) y organizacionales (p. ej., controles de acceso, seguimiento de auditoría) a fin de limitar el riesgo de acceso no autorizado o el daño a los datos del personal, como también la pérdida accidental o la destrucción de los mismos. Las medidas adecuadas dependerán de la naturaleza y la sensibilidad de los datos del personal en cuestión. Para obtener más información sobre cómo debe gestionarse el acceso a los datos personales y su seguridad, incluidos los datos del personal, consulte nuestras Normas y políticas de seguridad de IT.

1.6.4 **Controles de acceso**: el personal solo deberá tener acceso a datos del personal con base en la "necesidad de conocimiento" por motivos empresariales. El acceso a los datos del personal incluidos en WorkDay se otorga de acuerdo con el Procedimiento de control interno de WorkDay titulado "*Control y administración de acceso al sistema*" (System Access Control and Administration).

2. SOLICITUDES DE INDIVIDUOS EN RELACIÓN CON SUS DATOS DEL PERSONAL

Consulte la *Adenda 2 de la Política de privacidad y protección de datos de K-C (Solicitudes de derechos individuales)* para obtener información sobre cómo manejar una solicitud de derechos individuales de un postulante, del personal de K-C o de exempleados.

Es importante tener en cuenta que si un integrante del personal solicita una copia de sus datos del personal, es muy probable que, en ciertas jurisdicciones, toda la información incluida en la página "*Evaluación de potencial*" (Assess Potential) de WorkDay deba divulgarse como parte de la respuesta a esa solicitud, ***aunque*** esa información no sea visible para ese integrante del personal cuando acceda a WorkDay. Por lo tanto, resulta esencial que solo se ingrese información precisa y objetiva en esta página.

3. USO COMPARTIDO DE DATOS DEL PERSONAL DENTRO DE K-C GROUP

Usted podrá compartir los datos del personal dentro de K-C Group si se cumplen las siguientes condiciones:

- se informó a la persona acerca del uso compartido en el Grupo. Esto podría suceder porque los datos estuvieran incluidos en el Aviso para el personal sobre la protección de datos de K-C, mediante un aviso en la intranet o a través de un correo electrónico de la empresa;
- se explicó a la persona el propósito del uso compartido de datos;
- los datos del personal a compartir se limitarán a los necesarios para cumplir con el propósito; y
- el destinatario tiene una "necesidad de conocimiento" empresarial respecto de los datos del personal.

A la hora de decidir si puede compartir los datos del personal dentro de K-C Group, deberá estar seguro acerca de la razón por la cual la empresa de K-C Group necesita la información. Solamente deberá compartir datos del personal si este propósito es compatible con el propósito para el cual los datos del personal se recopilaron inicialmente. Si no está seguro de que el uso compartido cumpla con las condiciones anteriores, comuníquese con el Departamento Legal de K-C. Puede ser necesario realizar una Evaluación del impacto de la protección de datos; consulte la *Adenda 1 de la Política de privacidad y protección de datos de K-C (Evaluaciones del impacto de la protección de datos)*.

3. USO COMPARTIDO DE DATOS DEL PERSONAL FUERA DEL GRUPO

1. PRINCIPIO GENERAL

Por lo general, los datos del personal no deben compartirse fuera de K-C. Sin embargo, los datos del personal pueden compartirse fuera de K-C en las siguientes circunstancias:

- si la persona otorgó su consentimiento informado y de forma voluntaria;
- para contratar a un proveedor externo (consulte la *Adenda 3 de la Política de privacidad y protección de datos de K-C [Designación de proveedores]* para obtener más información);
- a fin de proteger los intereses vitales de una persona (es decir, si es un asunto de vida o muerte);
- cuando lo requiera la ley, la reglamentación o por orden judicial;
- en relación con una solicitud legítima de asistencia de parte de la policía u otra agencia de cumplimiento de la ley;
- para solicitar el asesoramiento legal de los abogados externos de K-C;

- en relación con una disputa legal o un reclamo administrativo entre K-C y un tercero (p. ej., con ese tercero y los abogados que lo representen);

- para contratar asesores profesionales (p. ej., abogados, contadores, auditores externos) y colaborar con potenciales compradores y proveedores en relación con la eliminación o adquisición por parte de K-C de una compañía o de sus activos;

- a fin de administrar la relación contractual de K-C con organizaciones que ofrecen "personal externo" mediante la divulgación de información relevante sobre las personas en cuestión (p. ej., cantidad de días trabajados);

- a fin de brindarle a un tercero (como un cliente o proveedor potencial) un medio para comunicarse con K-C en el desarrollo de las actividades comerciales habituales, p. ej., brindar los detalles de contacto comercial del personal, como los que se encuentran en una tarjeta personal; o

- para contratar auditores externos para validar las cuentas financieras de K-C.

En todos los casos, al compartir los datos se debe cumplir con las siguientes condiciones:

- cuando el tercero se encuentre fuera del Espacio Económico Europeo (European Economic Area, "**EEA**"), Suiza o el Reino Unido, se debe haber implementado una solución de transferencia de datos que cumpla con los requisitos de la legislación vigente (consulte al líder de protección de datos correspondiente, quien podrá ayudarlo con este requisito); y

- usted solo debe compartir la cantidad mínima de datos personales necesaria para cumplir con el propósito para el cual se comparte.

Si existe la posibilidad de que compartir los datos genere un riesgo alto para el personal, K-C deberá realizar una Evaluación del impacto de la protección de datos. Si considera que compartir algún dato tiene el potencial de representar un riesgo alto, deberá consultar al líder de protección de datos correspondiente. Consulte la *Adenda 1 de la Política de privacidad y protección de datos de K-C (Evaluaciones del impacto de la protección de datos)* para conocer más detalles.

La parte restante de esta adenda brinda más detalles sobre los pasos necesarios a seguir si K-C compartiera datos del personal fuera de K-C en las circunstancias antes definidas.

2. SOLICITUDES DE AUTORIDADES DEL CUMPLIMIENTO DE LA LEY U OTRAS AUTORIDADES REGULATORIAS

2.1 En ocasiones, será necesario que K-C brinde información sobre el pasaporte y la nacionalidad a autoridades de inmigración y de aduana a fin de facilitar el ingreso del personal al país correspondiente, cuando viaje con fines de trabajo. En otras circunstancias, siempre deberá consultar al abogado superior de Empleo y Trabajo para EMEA del Departamento Legal de K-C antes de responder a una solicitud de una autoridad de cumplimiento de la ley u otra autoridad regulatoria para acceder a los datos del personal.

2.2 Si el abogado superior de Empleo y Trabajo para EMEA del Departamento Legal de K-C autoriza la divulgación de datos del personal, dicha divulgación deberá limitarse a lo necesario para satisfacer el propósito especificado del solicitante. Garantice que, como parte de este proceso, se lleve un registro de la información divulgada, las conversaciones con el Departamento Legal de K-C y los pasos que se siguieron.

2.3 No divulgue datos del personal a terceros para la prevención o detección de un delito o fraude, excepto:

- que la divulgación sea requerida por la ley;

- que se considere de forma razonable que la falta de divulgación en una instancia en particular probablemente perjudique la prevención o detección del fraude o delito; o

- que la divulgación tenga lugar en el contrato de empleo de la persona.

3. ESQUEMAS DE PENSIÓN Y SEGURO Y OTROS BENEFICIOS

3.1 Cuando una persona se una a un esquema de salud, seguro u otros beneficios, asegúrese de que quede claro para la persona qué datos del personal, en caso de existir alguno, se transmiten entre el proveedor del esquema de beneficios y K-C, y cómo se utilizarán.

3.2 No se debe acceder a los datos del personal requeridos por un tercero para administrar un esquema o beneficio con fines generales del empleo, ni tampoco se deberán utilizar para ello. Por ejemplo, el informe médico de una persona necesario para el esquema de pensión no podrá usarse en relación con las decisiones sobre la elegibilidad de la persona para recibir el pago por enfermedad. En consecuencia, utilice formas confidenciales para prevenir la filtración de datos del personal de un esquema (p. ej., un sobre sellado).

3.3 Limite su intercambio de datos del personal con un proveedor de beneficios a aquellos datos necesarios para el funcionamiento del esquema.

4. REESTRUCTURACIÓN DEL NEGOCIO, FUSIONES Y ADQUISICIONES

4.1 Cuando sea posible, asegúrese de que la divulgación de los datos del personal como parte de una reestructuración del negocio, fusión o adquisición sea de forma anonimizada o con el uso de seudónimos. Los datos del personal solo deben divulgarse en formato no anonimizado en situaciones limitadas, en las que sea necesario para la evaluación de activos y pasivos o para la reestructuración del negocio y cuando se cuente con la aprobación del Departamento Legal de K-C.

4.2 Cuando deban divulgarse datos del personal, se deberán obtener las garantías de la entidad que adquiere el negocio para que todos los datos del personal suministrados:

- se traten de forma confidencia y de conformidad con la legislación de protección de datos vigente;

- no se divulguen a otros terceros;

- se usen solamente con el fin de la divulgación (p. ej., evaluación de activos y pasivos o reestructuración del negocio); y

- se destruyan o se devuelvan después de utilizarlos.

4.3 Asegúrese de que se haya informado a las personas acerca de la divulgación de sus datos del personal antes de dicha divulgación, a menos que resulte imposible hacerlo. Esto se puede hacer mediante la entrega a las personas del Aviso de privacidad sobre la selección de K-C (en caso de que todavía no lo hubieran recibido). Cuando se adquiera nuevo personal como resultado de una fusión, adquisición o reestructuración, asegúrese de dar aviso a las personas acerca de cómo se utilizarán sus datos del personal.

4.4 Si la fusión, adquisición o reestructuración implica la transferencia de datos del personal a otra organización fuera del EEA, asegúrese de que exista el fundamento correspondiente para hacer la transferencia (consulte la sección 3 anterior: “Uso compartido de datos del personal fuera del Grupo”).

5. TRANSFERENCIA DE DATOS DEL PERSONAL FUERA DEL EEA

Si compartir datos del personal implicase su transferencia a un país fuera del EEA, Suiza o el Reino Unido, K-C (el "**Exportador de datos**") solo podrá transferir datos del personal a una entidad ubicada fuera de esas jurisdicciones (el "**Importador de datos**") si se cumple alguna de las siguientes condiciones:

- el Importador de datos se encontrara en un país que la Comisión Europea haya considerado que brinda la protección adecuada de los datos personales (consulte la Adenda 1 a este anexo para acceder a un enlace a esta lista); o

- K-C y el Importador de datos hubieran firmado el acuerdo de transferencia de datos correspondiente, ya sea para las transferencias de contralor a contralor o las transferencias de contralor a procesador (consulte la Adenda 1 a este anexo para acceder a un enlace a los acuerdos de transferencia de datos correspondientes); o

- las personas hayan otorgado su consentimiento, después de haber sido informadas de los propósitos de la transferencia, las categorías de los destinatarios y el hecho de que los países a los cuales se transfieran los datos puedan tener diferentes estándares de privacidad de los datos; o

- la transferencia esté permitida de alguna otra forma de conformidad con la legislación vigente.

Deberá consultar al líder de protección de datos correspondiente y/o al abogado superior de Empleo y Trabajo para EMEA del Departamento Legal de K-C para obtener información sobre el mecanismo de transferencia más adecuado según el acuerdo.

Las preguntas sobre esta adenda pueden enviarse al: abogado superior de Empleo y Trabajo para EMEA del Departamento Legal de K-C.

ANEXO 1 A LA ADENDA 7 DE LA POLÍTICA DE PROTECCIÓN DE DATOS DE K-C

TRANSFERENCIAS DE DATOS

Para acceder a una lista de los países fuera del EEA con constataciones de adecuación, visite este sitio web.

Para solicitar copias de los acuerdos vigentes de transferencia de datos de contralor a contralor y de contralor a procesador, visite este sitio web.

ADENDA 8 DE LA POLÍTICA GLOBAL DE PRIVACIDAD DE DATOS DE KIMBERLY-CLARK

RETENCIÓN DE DATOS PERSONALES

1. INTRODUCCIÓN

La Política global de privacidad de los datos de K-C requiere que K-C implemente un proceso para la retención y eliminación de datos personales. En esta adenda se define el marco acerca de cómo K-C puede cumplir con sus obligaciones de una manera que satisfaga la Limitación de almacenamiento del Principio de protección de datos. En términos prácticos, esto significa garantizar que K-C solo guarde los datos personales mientras sea necesario para el propósito que se recopilaron (o para un propósito adicional permitido) y además:

- que retenga posibles evidencias que puedan requerirse durante un litigio;
- que destruya de forma segura los registros desactualizados;
- que optimice el uso del espacio; y
- que minimice el costo de la retención de los registros.

Esta adenda lo asistirá: (a) en la comprensión de las diferentes categorías de datos personales retenidos por K-C y (b) con una explicación de las pautas de retención para las diferentes categorías de datos personales.

Todo el personal que tenga responsabilidad sobre las categorías de datos personales abordadas en esta adenda deberá garantizar que los datos personales se eliminen dentro de los plazos especificados a continuación. Las únicas excepciones son los casos en los que se aplique una de las "Excepciones a esta adenda" (Sección 2) o si el equipo del Departamento Legal de K-C le indica que respete un período de retención diferente debido a alguna obligación legal conflictiva a la cual K-C esté sujeto.

Consulte el Apéndice A de la Política global de privacidad de los datos de K-C para acceder a un Glosario de los términos definidos en esta adenda.

2. EXCEPCIONES A ESTA POLÍTICA

Litigios

Se podrá solicitar jurídicamente que K-C retenga datos personales durante períodos más prolongados cuando los datos personales se relacionen con litigios previos o actuales u otros procedimientos judiciales. La frecuentemente denominada "Conservación de documentos debido a litigio" es una obligación legal que anula cualquier período de retención que, de otro modo, se aplicaría a los datos personales.

Si tiene conocimiento de cualquier otro litigo previo o actual relacionado con los datos personales, o en caso de una "Conservación de documentos debido a litigio", deberá suspender de inmediato la eliminación de los datos personales. El incumplimiento de una Conservación de documentos debido a litigio podría exponer a K-C a graves consecuencias legales. Los archivos y documentos relacionados con litigios actuales o pendientes deberán conservarse hasta que toda disputa se resuelva por completo y que no exista posibilidad de apelación.

Análisis estadístico de los datos personales

Los datos personales podrán almacenarse por períodos más prolongados en los casos en que solamente se procesen con fines estadísticos o de investigación y si se hubieran implementado las salvaguardas técnicas y organizacionales, por ejemplo, si se utilizan seudónimos para los datos personales y el procesamiento no se utiliza para tomar una decisión que afecte a una persona en particular. Si se aplicara el análisis estadístico a los datos personales y se implementaran salvaguardas apropiadas como el uso de seudónimos, entonces los períodos de retención declarados indicados a continuación no se aplicarían a esos datos personales y podrían guardarse durante un período más prolongado si existiera la necesidad continua de hacerlo. Sin embargo, la retención aún estaría sujeta a consideraciones importantes para K-C como la retención de registros actualizados, la optimización del uso del espacio y la minimización del costo de la retención de datos.

Los datos personales que se anonimicen no están sujetos a la Política de global de privacidad de los datos de K-C y, por lo tanto, los períodos de retención indicados en esta adenda no se aplicarán a estos. No obstante, la norma jurídica para que los datos se consideren "anónimos" es exigente; por eso, antes de confiar en la naturaleza anónima de la información, comuníquese con el líder de privacidad pertinente, cuyos detalles de contacto se pueden encontrar aquí en la página de SharePoint del Programa global de privacidad de datos.

3. RETENCIÓN DE DATOS PERSONALES

En virtud de la legislación sobre protección de datos, K-C tiene la obligación legal de no retener datos personales por un período mayor al necesario para el fin o los fines para el cual o los cuales se obtuvieron. Esta obligación legal se refleja en el Principio de protección de datos de K-C llamado "Limitación de almacenamiento".

4. PERÍODOS DE RETENCIÓN PARA LAS CATEGORÍAS DE DATOS PERSONALES

La retención de datos personales no incluidos en las categorías identificadas deberá determinarse, principalmente, por la aplicación del principio general de Limitación de almacenamiento, es decir que K-C solo deberá guardar datos personales durante el período que se consideren necesarios para los fines que se recopilaron o para un propósito adicional permitido. Si no está seguro acerca de cómo aplicar este principio y tiene dudas sobre cuál es el período de retención de datos apropiado para cierta categoría de datos personales, comuníquese con el líder de privacidad de los datos pertinente, cuyos detalles de contacto pueden encontrarse aquí en la [página de SharePoint del Programa global de privacidad de los datos].

Podrá encontrar información detallada sobre los períodos de retención que K-C aplica a las categorías de datos personales en el Programa de retención de registros empresariales (Enterprise Record Retention Schedule, ERRS) disponible en http://www.gric.kcc.com/Home.aspx.

INFORMACIÓN ADICIONAL

Encontrará información adicional sobre esta adenda y la Política global de privacidad de datos de K-C aquí: [página de SharePoint del Programa global de privacidad de datos].

Las preguntas sobre esta adenda pueden enviarse a KC HelpLine: [KCHelpLine@kcc.com].