POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES

DANONE

Versión	Versión 1
Historial	Entrada en vigor en abril de 2016
Procedimiento de aprobación	Aprobada por el Comité de Compliance y ética empresarial en abril de 2016
Público destinatario	Todos los empleados de Danone
Titular	Director general de Compliance
Nivel de confidencialidad	Uso interno
Número de páginas	19
Idiomas	Inglés (referencia legal), árabe, indonesio, malayo, búlgaro, chino, checo, danés, holandés, farsi, finés, francés, alemán, griego, hindi, húngaro, italiano, japonés, camboyano, coreano, letón, lituano, noruego, polaco, portugués, rumano, ruso, eslovaco, español, sueco, tailandés, turco, ucranio, vietnamita (idiomas de referencia)

ÍNDICE

01 INTRODUCCIÓN

1.1 Objetivo y alcance de la Política de Protección de Datos Personales ('Política')

Esta Política se aplica a Grupo Danone en todo el mundo, incluyendo a todas las subsidiarias y afiliadas con propiedad mayoritaria o bajo control efectivo (es decir, las subsidiarias consolidadas) y todos los empleados de las mismas. Con el objeto de asegurar la eficiencia y consistencia del Programa de Compliance, esta Política reemplaza todas las políticas existentes de Protección de Datos Personales de Danone. Pueden redactarse políticas adicionales para satisfacer alguna necesidad local o específica para algún negocio, pero solamente en la medida en que sea necesario, y sujeto a la aprobación del Comité de Compliance y Ética Empresarial ('CCB').

Los terceros a quienes, Danone subcontrate para todas o parte de las actividades de Procesamiento de Datos Personales ("Procesamiento") deben también cumplir con esta Política.

Esta Política de Protección de Datos Personales establece detalladamente las reglas y responsabilidades que deben seguir los empleados de Danone cuando administren Datos Personales ("Datos Personales"[1]). Se dirige en particular, a quien sea responsable del Procesamiento de Datos Personales de los empleados y consumidores de Danone: están disponibles los templates de Protección de Datos Personales para proporcionar una mayor guía a los empleados.

En la era digital en que vivimos, los Datos Personales son esenciales para los negocios y, si se administran apropiadamente, abren nuevas fuentes de crecimiento. Sin embargo, una administración responsable de Datos Personales es vital para la sustentabilidad del negocio y Danone no realiza ningún comportamiento que pudiera dañar nuestros negocios o las comunidades en las cuales operamos. Reconocemos por completo el derecho fundamental que tienen los individuos a su privacidad y su derecho al resguardo de Datos Personales. La protección del derecho a la privacidad de los empleados y otros individuos es el objetivo primordial de esta Política de Protección de Datos Personales y un elemento clave del compromiso de Danone con el cumplimiento de normas globales de protección de Datos Personales.

Esta Política no cubre los requerimientos relacionados con confidencialidad, integridad y disponibilidad de datos en general, ni el uso personal incidental de los Recursos de Comunicación Electrónica de Danone ("Recursos de Comunicación Electrónica"): éstos siguen siendo regulados dentro de los Lineamientos relacionados con Seguridad de la Información y Sistemas Comunicación, otras políticas corporativas o locales, y leyes aplicables.
La ley local de privacidad puede variar; cuando exista una diferencia entre el requerimiento legal y esta Política, siempre debe aplicarse la norma más estricta.

[1] Este formato (comillas) denota que los términos se pueden encontrar en el Glosario

1.2 Riesgos asociados con violaciones a la legislación sobre Protección de Datos Personales

El incumplimiento de la ley de Protección de Datos puede generar penas civiles y penales y/o prisión (para individuos). Además, las violaciones a las leyes de Protección de Datos pueden causar un daño significativo a la reputación de Danone. El incumplimiento de esta Política (u otras Políticas de Compliance) no será tolerado por Danone y puede causar una acción disciplinaria. Dicha acción disciplinaria variará de acuerdo con la severidad del incumplimiento pero puede incluir la cancelación de bonos de empleado, aplazamiento de promoción, suspensión sin paga, terminación de la relación laboral o denuncia a las autoridades.

1.3 Roles y Responsabilidades de Compliance

Todos los Danoners son responsables de adherirse al Código de Ética de Negocios y las Políticas de Compliance, incluyendo la Política de Protección de Datos Personales. Esto implica que las políticas internas, por lo tanto, no deben contravenir las reglas establecidas en esta Política.

Los **Gerentes Generales ("GM")**, en relación con sus respectivas CBUs; los **GMIs** también en relación con sus respectivas CBS,

- son responsables de la implementación y ejecución de los procesos establecidos en esta Política y su cumplimiento.

Los **miembros del COMEX**, en relación con las WBUs, WBS, RBUs y RBS en sus respectivas áreas de responsabilidad,

- asumen la función y responsabilidad asignada a los GMs para sus CBUs.

Los **Ejecutivos de Cumplimiento del Clúster**[2] **("CO Clúster")**,

- asesoran y apoyan a los GM's en todas las funciones en el Clúster respectivo con la aplicación de esta Política y contratan asesores externos cuando sea necesario;
- monitorean los regímenes de leyes de Protección de Datos en el Clúster y mantienen informado al área de Compliance sobre cualquier desarrollo importante;
- informan inmediatamente a Compliance si cualquier CBU en el Clúster se ve sujeta a la investigación de una autoridad de privacidad.

El Equipo de Cumplimiento WBS ("Cumplimiento WBS")

- proporciona lineamientos relacionados con cuestiones generales sobre la aplicación de esta Política;
- asesora en respuesta a cuestiones que no pueden resolverse en su totalidad por parte del CO Clúster en relación con todas las unidades de negocios;

[2] O, cuando sean designados de acuerdo con las reglas establecidas en la Política Marco de Cumplimiento (sección 6.1), Ejecutivos de Cumplimiento en los niveles de las WBUs, WBS, RBUs, RBS y CBUs.

- puede, después de la decisión del Chief Compliance Officer ('CCO'), decidir que aconsejará en casos o guiará investigaciones que tengan un impacto sustancial sobre el riesgo de Compliance de la compañía.

02

PRINCIPIO DE PROCESAMIENTO DE DATOS PERSONALES

En Danone, el Procesamiento de Datos Personales se permite solo cuando es justo y legal, con cumplimiento de los principios enlistados en las páginas siguientes, y administrado mediante apropiadas medidas técnicas y organizativas, lo que nos permite demostrar que respetamos toda ley aplicable.
Para ayudar a asegurarnos de esto, el CO Clúster tendrá que revisar toda nueva actividad relacionada con Datos Personales (por ejemplo, una nueva categoría de Datos Personales procesados, una nueva plataforma de Procesamiento o un nuevo propósito de Procesamiento).

2.1 Propósito específico y legítimo

Procesamos Datos Personales solo para propósitos específicos y explícitos. Por lo tanto, en el momento de la recolección de Datos Personales, o antes, determinamos el propósito del Procesamiento y lo comunicamos a los propietarios de los Datos Personales ("Titulares de Datos") y después de su acopio, procesamos los Datos Personales solo de manera compatible con este propósito.

Por ejemplo, si la información de contacto de un consumidor se ha obtenido con el propósito del procesamiento de una queja, no puede agregarse a la lista de distribución de nuestro boletín a menos de que se haya informado al consumidor sobre este propósito adicional y haya consentido este fin.

Adicionalmente, nuestro propósito debe de ser legítimo. Por lo tanto, cuando lo determinamos, verificamos si son legítimos y legales bajo las leyes aplicables, preguntándonos si lo que intentamos hacer es justo y legal: generalmente, este es el caso cuando nuestro interés y el del Titular de los Datos están alineados. Claramente, no es legítimo un propósito que implicaría una violación a la privacidad de los Titulares de los Datos.

Por ejemplo, la televisión de circuito cerrado es, bajo las leyes de Protección de Datos de muchos países, una actividad legítima, cuando tiene el objeto de asegurar la seguridad de los empleados, pero se convierte en ilícita cuando se usa para ponerlos bajo vigilancia constante y permanente.

2.2 Proporcionalidad y calidad de Datos

Solo recolectamos los Datos Personales que necesitamos para nuestros propósitos y no solicitamos o conservamos detalles irrelevantes. No debemos conservar Datos Personales por la posibilidad remota de que pudieran ser útiles en el futuro.

Los Datos Personales que conservamos deben también ser precisos y mantenerse actualizados. Debemos rectificar o eliminar información imprecisa o incompleta, tan pronto como sepamos sobre tal imprecisión y/o falta de información.

Por ejemplo, si necesitamos hacer preguntas específicas sobre la salud de los candidatos para puestos particulares, estas preguntas no deben ser parte de nuestros cuestionarios estándar, ya que en la mayoría de los casos no lo necesitamos.

De manera similar, si el propósito que comunicamos para el Procesamiento es enviar un boletín con ofertas especiales a los consumidores, solo debe obtenerse la información de contacto, sin ninguna información innecesaria, tal como detalles de cuentas bancarias.

2.3 Retención limitada

Conservamos los Datos Personales de forma que permita la identificación del Titular de los Datos solo por el periodo de tiempo necesario para los propósitos del Procesamiento, alineado con la información proporcionada al Titular de los Datos. No conservamos Datos Personales por una duración ilimitada de tiempo, a menos de que sea expresamente requerido por la ley.

Es una buena práctica revisar regularmente los Datos Personales que conservamos y eliminar todo lo que ya no necesitemos, siempre tomando en cuenta las reglas aplicables a cualquier tipo de Datos Personales. Sin embargo, los Datos Personales no deben conservarse indefinidamente 'por si acaso', o si existe solo una pequeña posibilidad de que lleguen a usarse.

Por ejemplo, Danone debe revisar los Datos Personales que mantiene sobre sus empleados cuando dejan la compañía. Necesitamos retener suficientes datos para poder proporcionar referencias o información sobre los arreglos de su pensión, pero debemos eliminar los detalles de sus contactos de emergencia o domicilios previos.

2.4 Información del Titular de Datos

Cuando acopiamos Datos Personales, o como máximo cuando se procesan por primera vez, debemos proporcionar información suficiente y adecuada a los Titulares de los Datos, como mínimo:

- los propósitos del Procesamiento;
- la identidad y los detalles de contacto del Controlador de los Datos Personales ("Controlador de los Datos"); los principales Procesadores de Datos Personales ("Procesador de Datos"), y sus representantes;

- sobre cualquier transferencia de los Datos Personales fuera del país donde se proporcionaron; especificando, si se les otorga el mismo nivel de protección, y cómo;
- cuánto tiempo se conservarán los Datos Personales;
- sus derechos (ver párrafo 2.8) y los medios para que los ejerciten;
- la naturaleza obligatoria o voluntaria de la revelación de los Datos Personales.

Debemos informar a los Titulares de los Datos usando un lenguaje claro y llano, a su vez conciso, transparente, inteligible y en formas de fácil acceso, tales como declaraciones de privacidad, ya sean digitales o impresas, una política de privacidad en un sitio web, un e-mail dando acuse de recibo de una solicitud o queja, un boletín por e-mail o reglas internas concernientes al procesamiento de los Datos Personales de empleados.

La Directiva anexa, sobre acceso a Recursos de Comunicación Electrónica, proporciona a los Danoners una lista de las motivaciones que pueda tener Danone para acceder a su Recurso de Comunicación Electrónica.

2.5 Consentimiento del Titular de Datos

En relación con la ley local en vigor, siempre debe obtenerse un consentimiento sin ambigüedades otorgado por los Titulares de los Datos para el Procesamiento de Datos Personales.

Consideramos que los Titulares de los Datos han consentido al Procesamiento de Datos Personales cuando han proporcionado los Datos Personales voluntariamente, han recibido la información apropiada y habiendo tenido la opción de objetar al Procesamiento Datos, no ejercieron tal derecho.

Generalmente, el consentimiento no es necesario cuando los Datos Personales se procesan para realizar un contrato en el que los Titulares de los Datos son una de las parte, para cumplir con una obligación legal, para proteger los intereses vitales de los Titulares de los Datos o de otra persona o con un propósito relacionado con algún interés legítimo de la empresa o de terceros, cuando los intereses, derechos y libertades de los Titulares de los Datos no superen dicho interés.

Siempre tenemos que distinguir claramente entre nuestra solicitud de consentimiento y otras piezas de información, presentarla de manera apropiada para la edad y capacidad de los Titulares de los Datos y las circunstancias particulares del caso. Adicionalmente, debemos revisar si los consentimientos que hemos recogido continúan siendo los apropiados mientras evoluciona nuestra relación con los Titulares de los Datos.

En cualquier caso, nunca debemos hacer que el cumplimiento de un contrato sea condicional al procesamiento de Datos Personales que no sean necesarios para su cumplimiento.
Por favor, consulte la Directiva de acceso a los Recursos de Comunicación Electrónica para conocer la lista de motivaciones que pueda tener Danone para acceder a su Recurso de Comunicación Electrónica sin el consentimiento del Usuario (“Usuario”).

2.6 Información de los Titulares de Datos

En Danone, la confidencialidad y seguridad de los Datos Personales que se nos confían es esencial. Por lo tanto:

- siempre mantenemos los Datos Personales de manera confidencial y si necesitamos revelarlos a terceros, sin importar la relación, siempre cubrimos con un contrato todos los aspectos relevantes de tal revelación;
- implementamos las medidas apropiadas, tanto técnicas como organizativas, para proteger los Datos Personales contra destrucción accidental o dolosa, o pérdida o alteración accidental, o revelación o acceso no autorizados;
- pedimos a todo el que esté autorizado para acceder a los Recursos de Comunicación Electrónica (incluyendo a los miembros del Equipo de Tecnología de la Información y/o administradores de sistema de Danone, durante el desempeño de sus obligaciones):
    - que no usen el otorgamiento de acceso para obtener registros diferentes a aquellos para los cuales se autorizó el acceso,
    - que limiten el acceso a un nivel mínimo de contenido y la menor acción posible, limitando el número de personas involucradas a solamente aquellas que se requieran para iniciar y llevar a cabo el acceso,
    - que no busquen, usen, o revelen el contenido de los Recursos de Comunicación Electrónica, excepto cuando estén autorizados por Danone,
    - que inmediatamente se pongan en contacto con el Gerente Corporativo de Seguridad de Sistemas de Información y el Ejecutivo en Jefe de Cumplimiento siempre que encuentren cualquier material que de manera razonable pueda considerarse de naturaleza criminal (por ejemplo pornografía infantil, asociación delictuosa, etc.), o que de cualquier otra manera contravengan cualquier ley, reglamento, regla o política vigente y aplicable.

Por favor, consulte la Directiva de Acceso a los Recursos de Comunicación Electrónica para conocer el procedimiento que debe respetarse al acceder al Recurso de Comunicación Electrónica de Danone.

2.7 Salvaguarda de Datos Sensibles

Como regla general, no procesamos Datos Sensibles ("Datos Sensibles"), a menos de que:

- Los Titulares de los Datos hayan dado su consentimiento explícito para el Procesamiento o;
- El procesamiento sea necesario para el logro de las obligaciones y derechos de Danone en las áreas de empleo, seguridad social y la ley de protección social, o para proteger los intereses vitales de los Titulares de los Datos, o si están relacionados con datos abiertamente publicados por los Titulares de los Datos, o si es necesario para el establecimiento, ejercicio o defensa de una reclamación legal.

Como los Datos Sensibles pueden usarse de manera discriminatoria, necesitan tratarse con mayor cuidado que otros Datos Personales.

2.8 Derechos del Titular de Datos

Siempre ofrecemos a los Titulares de los Datos los medios efectivos para:

- oponerse al Procesamiento de Datos Personales por razones legítimas ('derecho de oposición'):
    - los Titulares de los Datos siempre tienen el derecho de oponerse al Procesamiento de sus Datos Personales con el propósito único de mercadotecnia: en consecuencia, siempre debemos proporcionar el medio de 'optar por la salida', tal como un vínculo 'eliminar suscripción' en boletines enviados por e-mail.
- saber qué Datos Personales tenemos en relación con él o ella ('derecho de acceso');
- si se descubre que los Datos Personales que tenemos en relación con él o ella no son exactos o actualizados, requerir su rectificación ('derecho de rectificación);
- si se descubre que los Datos Personales que tenemos en relación con él o ella ya no son relevantes en relación con los propósitos de su Procesamiento original, o si él o ella han retirado su consentimiento u objetado al Procesamiento, solicitar que se eliminen ('derecho de cancelación');
    - como ejemplo, un consumidor puede oponerse al procesamiento de su lugar de nacimiento para los propósitos del procesamiento de una queja,
    - cuando un Titular de los Datos pide ejercer el 'derecho de cancelación', es vital recordar que este derecho no es absoluto, y que dependiendo de la naturaleza de la solicitud, tendremos que eliminar todos o parte de los Datos Personales que tenemos. Por lo tanto, debemos asistir a los Titulares de los Datos al decidir qué datos son verdaderamente necesarios en qué Procesamiento, y no eliminarlo todo, a menos de que explícitamente exprese el deseo de eliminar todos los Datos Personales. Con este fin, siempre debemos dar a los Titulares de Datos, en particular a los consumidores, varias opciones para una eliminación personalizada, es decir, eliminar la dirección de e-mail, eliminar el domicilio postal, eliminar la información familiar, etc.,
    - en algunas situaciones, una solicitud de eliminación no es legítima. Si, por ejemplo, un empleado solicita la eliminación de su número de seguro social de la base de datos de Danone, no podemos satisfacer tal solicitud ya que esta información es necesaria para la implementación del convenio de trabajo. De la misma forma, cuando los consumidores se registran en uno de nuestros sitios web para ser parte de una iniciativa promocional y solicitan la eliminación de sus datos de contacto, pero al mismo tiempo confirman que quieren participar, entonces aceptar esta solicitud de eliminación colocaría a Danone en violación del

contrato promocional. En estos dos casos, los datos son relevantes y necesarios para el cumplimiento del contrato que los Titulares de los Datos han celebrado con Danone.

- Restringir el Procesamiento de los Datos Personales por el tiempo necesario para actualizarlos, como una alternativa a su eliminación, si se necesita para el establecimiento, ejercicio o defensa de una reclamación legal, o por el tiempo necesario para verificar la legitimidad de una objeción a la solicitud de Procesamiento ('derecho a restricción del Procesamiento').

Si los Titulares de Datos requieren de nuestra acción para que ejerzan sus derechos, proporcionamos la información y asistencia lo más pronto posible.

2.9 Procesamiento de Datos Personales

Cuando procesamos Datos Personales como Controladores de Datos, somos directamente responsables en relación con todas las leyes, regulaciones y políticas internas aplicables, ya sea que procesemos los Datos Personales directamente o mediante terceros.

Se considerará que una CBU es Controlador de Datos, por ejemplo, si establece una actividad de investigación de mercado con Datos Personales de los consumidores, administra un call center de servicio al cliente (aún si un proveedor procesa las solicitudes pero a nuestro nombre), o firma un contrato de empleo que mencione los Datos Personales del empleado.

Cuando otro Controlador de Datos nos nombra como Procesador de Datos, debemos asegurarnos de cumplir con las instrucciones del Controlador de Datos.

Se considerará que una CBU es el Procesador de Datos si conserva Datos Personales de los consumidores en una base de datos central para la administración de relaciones con consumidores, lleva a cabo análisis de mercado, o envía comunicaciones de mercadotecnia a nombre de otras CBUs.

Sin importar nuestro papel en el Procesamiento de Datos Personales, debemos cumplir con todos los requerimientos de las autoridades locales de Protección de datos.

Por ejemplo, en algunos países, cada actividad de Procesamiento de Datos Personales debe notificarse a la autoridad competente en protección de datos, mediante un formato específico (en línea o impreso). En otros países, se requiere que haya consejos de trabajo para aprobar un Procesamiento específico de Datos Personales, y los Datos Sensibles no pueden recolectarse o procesarse sin la previa autorización de la autoridad de Protección de Datos.

2.10 Uso de Procesadores de Datos

Cuando realizamos todo o parte del Procesamiento de Datos Personales a través de terceros Procesadores Datos, seguimos siendo responsables de todos los actos que realicen a nuestro nombre: esta responsabilidad no puede evitarse.

Como consecuencia:

- respetamos el Código de Conducta con Socios Comerciales de Danone y los procedimientos de selección de terceros, cuando seleccionamos a terceros como Procesadores Datos;
- los obligamos ante nosotros mediante un contrato que establece el objetivo y duración del Procesamiento, su naturaleza y propósito, el tipo de Datos Personales y de Titulares de Datos, y estipulamos instrucciones claras, incluyendo aquellas relacionadas con una eventual transferencia de datos fuera del país en el cual se recolectaron;
- exigimos evidencia de que existen medidas apropiadas de seguridad y confidencialidad que hayan implementado o pretendan implementar antes de empezar con el Procesamiento de Datos Personales.

Si la contratación externa del Procesamiento de Datos Personales implica la transferencia de Datos Personales fuera del país donde fueron obtenidos y no se reconoce oficialmente que el país receptor cuenta con un nivel adecuado de protección de datos, debemos implementar medidas de protección apropiadas.

Si un tercero nos nomina para ser su Procesador de Datos y recibimos Datos Personales a través de este intermediario, debemos verificar que se nos ha dado la información correcta, y que se ha obtenido el consentimiento apropiado de los Titilares de los Datos (particularmente sobre su revelación a nosotros).

03

PROCEDIMIENTO PARA REALIZAR UNA DENUNCIA/QUEJA

Procedimiento para la realización de una denuncia/queja («denuncia de irregularidades»)

La denuncia o queja sobre una irregularidad consiste en que un empleado de Danone o un tercero relacionado a Danone, informe a Danone de la sospecha de presuntas irregularidades. Para Danone, el alcance de una denuncia de irregularidades engloba la conducta requerida por Danone según lo establecido en nuestro Código de conducta empresarial, en la presente Política de Integridad y en nuestras políticas de Compliance. También abarca otros tipos de conducta ilícita, malversación de fondos y cualquier actividad que suponga o pueda suponer un peligro para el medio ambiente o para cualquier persona que trabaje para nuestra empresa.

Política de Danone sobre la denuncia de irregularidades

En Danone queremos conocer inmediatamente cualquier infracción o posible infracción de nuestros principios empresariales, cualquier conducta ilícita, malversación de fondos y actividad que suponga o pueda suponer un peligro para el medio ambiente o para cualquier persona que trabaje para nuestra empresa.

Siempre animamos a los empleados de Danone a que expongan cualquier tipo de preocupación directamente a una persona de referencia en la empresa (como a su N+1, N+2 o al responsable de RR. HH., de finanzas o de Compliance).

Sin embargo, si los empleados de Danone prefieren informar confidencialmente acerca de una preocupación, queja o denuncia a través del cualquier otro canal, también tenemos a su disposición una herramienta de información llamada Danone Ethics Line, a la que puede accederse a través de la página web www.danoneethicsline.com. Esta herramienta se puede utilizar de forma anónima, si es necesario.

No se deben tomar represalias contra las personas que notifiquen de buena fe una preocupación genuina.

Investigaciones

Todas las preocupaciones, quejas o denuncias planteadas se investigarán internamente de manera apropiada. La organización de la investigación estará gestionada por el Comité de Danone Ethics Line. Se puede informar de los resultados a la CCB (con exclusión de los miembros implicados), que

se encargarán de decidir qué medidas se deben adoptar. La información detallada sobre las investigaciones viene contenida en la Política de investigaciones internas.

ANEXO 1 – REGLAS ESPECÍFICAS A PAÍSES

Estamos conscientes de la imposibilidad de adoptar un enfoque 'universal' en la Protección de Datos Personales.

En la medida en que cualquier ley local entre en conflicto con la aplicación de esta Política, se le considerará como modificada únicamente a que esté limitado a lo que se requiera para posibilitar que se cumpla solamente en dicha jurisdicción local.

Para mayor información, por favor póngase en contacto con su CO Clúster.

Abajo, enlistamos algunas reglas nacionales específicas que pueden tener un impacto sobre el Procesamiento de Datos Personales: pueden ser solamente validos en el país bajo el cual se enlistan.

Definición de Datos Personales

Se puede encontrar una definición general de Datos Personales en el Anexo 2. En la **UE**, los Datos Personales son cualquier información relacionada con una persona física identificada o identificable, que incluye identificadores como el nombre, número de identificación, datos de localización, identificador en línea, o uno o más factores específicos a la identidad física, psicológica, genética, mental, económica, cultural o social de los Titulares de los Datos.

En **Argentina**, Datos Personales es cualquier información relacionada o atribuida o atribuible a individuos o entidades legales.

Definición de Datos Sensibles

Se puede encontrar una definición general de Datos Sensibles en el Anexo 2. En la **UE**, los Datos Sensible son los Datos Personales que revelan el origen racial o étnico, las opiniones políticas, las creencias religiosas, morales o filosóficas, membresía en sindicatos, o los datos genéticos, datos biométricos, o datos relacionados con la salud, las preferencias y vida sexuales.

En **China**, los Datos Sensibles se definen como información personal cuya filtración o alteración pueden tener el resultado de un impacto adverso para los Titulares de los Datos. Los ejemplos pueden incluir el número de identificación personal, número de teléfono celular, raza, punto de vista político, creencia religiosa, genética o huellas dactilares.

En la **India**, los Datos Sensibles se definen también como "información personal", que consiste en la información relacionada con cualquier punto de los siguientes: contraseñas; información financiera tal como los detalles de cuenta bancaria o de tarjeta de crédito u otros instrumentos de

pago; cualquier detalle relacionado con lo anterior o revelado a una entidad corporativa para proporcionar un servicio.

En **Japón**, puede considerarse el domicilio legal como un Dato Sensible.

En los **EUA** los datos de crédito, información personal obtenida en línea de niños menores a 13 años, e información que puede usarse para llevar a cabo un robo de identidad o fraude pueden ser considerados como Datos Sensibles.

Consentimiento

Se puede requerir un consentimiento explícito en algunos países. Específicamente:

- En **Taiwán** y en **Singapur**, es obligatorio obtener un consentimiento explícito para la recolección, procesamiento, uso y almacenamiento de los Datos Personales de los Titulares de los Datos: "Consiento la recolección, procesamiento, uso y almacenaje de mis Datos Personales para los propósitos descritos más arriba";

- En **Italia, Australia, Hong Kong, Nueva Zelanda** es obligatorio obtener un consentimiento explícito para la recolección, procesamiento, uso y almacenamiento de los Datos Personales de los Titulares de los Datos si es con propósitos de comercialización directa: "Consiento la recolección, procesamiento, uso y almacenaje de mis Datos Personales para los propósitos de comercialización directa descritos más arriba";

- En **Italia** y **Japón** es obligatorio obtener un consentimiento explícito para la recolección, procesamiento, uso y almacenamiento de los Datos Personales de los Titulares de los Datos si es con propósitos de crear un perfil: "Consiento la recolección, procesamiento, uso y almacenaje de mis Datos Personales para los propósitos de crear un perfil";

- En **China, Malasia, Tailandia, Hong Kong, Japón** es obligatorio obtener un consentimiento explícito para la transferencia de los Datos Personales de los Titulares de los Datos a afiliadas, proveedores de servicios y socios comerciales: "Consiento a la transferencia de mis Datos Personales a afiliadas, proveedores de servicios y socios comerciales de [insertar el nombre de la CBU que obtiene los datos] fuera de [insertar el nombre de país de acopio]";

- La legislación anti-spam de **Canadá** regula la distribución de mensajes electrónicos. En ciertas circunstancias, es obligatorio obtener un consentimiento explícito de los Titulares de los Datos para enviarles mensajes electrónicos, así como mensajes electrónicos con propósitos de comercialización: "La legislación anti-spam de Canadá regula la distribución de mensajes electrónicos. En relación con lo anterior, [insertar el nombre de la CBU que obtiene los datos] y [insertar el nombre de cualquier otra entidad que envíe e-mails a clientes] puede enviar a usted e-mails relacionados con sus compras así como con propósitos de comercialización (incluyendo invitaciones a ventas o eventos privados, boletines y publicaciones, avisos, novedades o información que pueda ser de interés para usted). Usted puede retirar su consentimiento a recibir tales comunicaciones electrónicas en cualquier momento, eliminando su suscripción a nuestro e-mail como se describe en el

propio e-mail o poniéndose en contacto con nosotros en las direcciones electrónicas o postales mencionadas más arriba" "Consiento en recibir mensajes electrónicos de [insertar el nombre de la entidad legal que recolecta los datos] y [insertar el nombre de cualquier otra entidad que envíe e-mails a clientes]" "Consiento en recibir mensajes electrónicos con propósitos de comercialización de [insertar el nombre de la entidad legal que recolecta los datos] y [insertar el nombre de cualquier otra entidad que envíe e-mails con propósitos de comercialización a clientes]".

Transferencia

En la **UE**, cuando se transfieren los Datos Personales a un país que no asegure un nivel adecuado de protección, se requiere que el Controlador de Datos obtenga medidas de protección apropiadas, tales como 'reglas corporativas obligatorias', cláusulas estándar de protección de datos adoptadas por la Comisión, cláusulas estándar de protección de datos adoptadas por una autoridad de supervisión, y aprobadas por la Comisión, cláusulas contractuales entre el controlador o procesador y el controlador, procesador o el receptor de los datos en el tercer país.

ANEXO 2 – GLOSARIO

Referencia en el texto	Definición completa
Controlador de Datos	Aquel que, solo o junto con otros, determina los propósitos y medios del Procesamiento de Datos Personales.
Procesador de Datos	Aquel que procesa los Datos Personales a nombre del Controlador de Datos.
Titulares de los Datos	La persona física (ya sea un consumidor, empleado, cliente o empleado de un proveedor, y cualquier tercero) a la cual pertenecen los Datos Personales.
Recursos de Comunicación Electrónica	Dispositivos electrónicos, software y medios de comunicación electrónica, que incluyen, sin limitación, a las computadoras personales y estaciones de trabajo, computadoras laptop, teléfonos y teléfonos inteligentes, impresoras, módems, máquinas de fax, correo electrónico, mensajería instantánea y sistemas de correo de voz, que sean propiedad de, arrendados por, o de cualquier manera administrados por Danone.
Datos Personales	Información que permite identificar, por sí misma o en combinación con otras piezas de información, a una persona física.
Procesamiento	Cualquier operación o conjunto de operaciones que se realiza a los Datos Personales, ya sea por medios automáticos o no automáticos, tal como el acopio, registro, retención, organización, almacenaje, adaptación o alteración, actualización, extracción, consulta, uso, revelación mediante transmisión, diseminación o de cualquier otra forma que la haga disponible, alineación o combinación, bloqueo, eliminación o destrucción.
Datos Sensibles	Datos Personales que si se usan indebidamente pueden causar un serio daño o vergüenza a una persona física (por ejemplo opiniones políticas, creencias religiosas, membresía en un sindicato, datos concernientes a la salud o vida sexual). Por favor, consulte el Anexo 1 para más detalles.
Usuarios	Empleados, directores, consultores y proveedores a quienes Danone haya otorgado Recursos de Comunicación Electrónica para asistirlos en el desempeño de sus obligaciones o entrega de resultados laborales.

Anexo a la Política de Protección de Datos Personales de Grupo Danone

DIRECTIVA DE ACCESO A RECURSOS DE COMUNICACIÓN ELECTRÓNICA ('DIRECTIVA')

Se considera que el contenido de los Recursos de Comunicación Electrónica de Danone y todo lo que transita en nuestras redes está bajo la responsabilidad de Danone. En cualquier momento podemos acceder a todo eso por medio de sujetos delegados internos o externos, con respeto a las leyes nacionales vigentes y las políticas de Danone, con o sin consentimiento de, o aviso previo a, el Usuario.

Las razones para el acceso incluyen la necesidad de:

- determinar el cumplimiento de la Políticas de Compliance y otras políticas de Danone;
- extraer información en respuesta a una orden judicial o responder a una solicitud de autoridades o agencias públicas, o para el propósito de establecer, ejercer o defender una reclamación legal;
- conducir una investigación interna sobre alguna presunta infracción, tal como, sin limitación, acoso, discriminación, robo de secreto comercial, violación a la seguridad o confidencialidad de información;
- asegurar el desempeño y seguridad de nuestro sistema de Recursos de Comunicación Electrónica o llevar a cabo su mantenimiento;
- asegurar las operaciones rutinarias de negocios y continuidad del negocio, y
- cualquier otro propósito de negocios que requiera acceso a nuestros Recursos de Comunicación Electrónica.

Antes de acceder a los Recursos de Comunicación Electrónica, debe obtenerse el consentimiento de los Usuarios, siempre que sea posible. Para determinar si existe alguna razón para no hacerlo, siempre debe buscarse la asesoría del CO Clúster, y se debe respetar la Directiva. Si en una emergencia no se puede respetar esta Directiva, las acciones deben limitarse a la búsqueda mínima de contenidos y la mínima acción necesaria para resolver la emergencia, y debe subsecuentemente buscarse la autorización apropiada sin retraso alguno.

Investigaciones de la Autoridad

Danone puede estar obligada bajo la ley aplicable a acceder a los Recursos de Comunicación Electrónica y revelar el contenido relacionado a autoridades públicas que tienen el derecho legal a obtenerlo sin el consentimiento del, o información previa al, Usuario. De manera similar, Danone

puede revelar el contenido de sus Recursos de Comunicación Electrónica para cumplir una orden expedida por un tribunal, un citatorio, una orden judicial o a un órgano con la jurisdicción apropiada, en cualquier otra circunstancia donde la ley requiera tal revelación.
Cuando se enfrenten a tales situaciones, los empleados de Danone tendrán que informar al CO Clúster relacionado, quien está a cargo de:

- junto con el Jefe del Departamento Legal del Clúster, o en ausencia de éste último, con el apoyo de un asesor legal, valorar las bases de la solicitud, y el respeto a cualquier ley aplicable de privacidad y de protección de datos, y a cualquier regla específica que pueda limitar el acceso, revelación o transferencia;

- aprobar o rehusar el acceso, informando al mismo tiempo al Director Regional de IS, al Chief Compliance Officer, al Gerente de Seguridad Corporativa de Sistemas de Información y al Director de Regulación de IS del Grupo.

Cuando se apruebe, el acceso se llevará a cabo a nivel de la CBU, en cumplimiento con los Lineamientos para Inspecciones Gubernamentales No Anunciadas de Danone, la Política de Investigación Interna, los Lineamientos de Investigación Interna y la Política *Dawn Raid*.

Siempre que el acceso cubra algún contenido de los Recursos de Comunicaciones Electrónicas que no esté disponible de inmediato para el personal de la CBU, el CO Clúster hará la solicitud por escrito al Ejecutivo en Jefe de Cumplimiento. Cuando sea autorizado, se comunicará el acceso al Ejecutivo en Jefe de Seguridad e Inteligencia Competitiva, al Director Regional de IS, al Gerente de Seguridad Corporativa de Sistemas de Información y al Director de Regulación de IS del Grupo, para evaluación y ejecución técnica, dentro de un marco temporal acordado con la autoridad interesada.

Si no se ha nominado ni al CO Clúster ni al Jefe del Departamento Legal del Clúster, tiene que involucrarse al WBS de Compliance.

Investigaciones internas

Todo acceso a los Recursos de Comunicaciones Electrónicas que sea necesario en el desempeño de una investigación interna se realizará en cumplimiento de la Política Marco de Compliance, la Política de Investigación Interna, los Lineamientos de Investigación Interna y la Política *Dawn Raid*.

Operaciones de Negocios (Ausencias Temporales y Definitivas de Empleados)

Como regla general, se estimula a las CBUs para que usen técnicas o procedimientos que minimicen la necesidad de acceder a los Recursos de Comunicación Electrónica de un empleado ausente, tales como los mensajes "de ausente", cuentas de grupo de trabajo, auto-reenvío con filtrado, o listas de correo. Sin embargo, las CBUs también deben implementar procedimientos para administrar ausencias temporales o definitivas. Estos procedimientos deben cubrir:

- las condiciones que regulan el acceso, reutilización o eliminación de los Recursos de Comunicaciones Electrónicas por parte de la CBU, y su contenido después de la partida;

- las instrucciones relacionadas con la disposición de registros de comunicaciones electrónicas personales, por ejemplo, si deben ser eliminados o transmitidos a otras cuentas personales de e-mail u otros medios personales;
- las instrucciones sobre si debe instalarse un mensaje de ausencia, que indique la fecha de la separación e información alternativa de contacto en la CBU;
- fecha en la cual se dará por terminada la cuenta y ya no será accesible al empleado que se ha retirado.

Los empleados deben estar informados sobre estos procedimientos desde su contratación y, si es necesario, deben dar su consentimiento a las condiciones arriba mencionadas.

Si se requiere el acceso a los Recursos de Comunicaciones Electrónicas de un empleado ausente o separado para continuar con las operaciones de Danone, y no se obtuvo el permiso apropiado antes de la ausencia o separación, solamente el CO Clúster puede autorizar dicho acceso. La solicitud de acceso debe ser hecha por el gerente de línea del empleado, por escrito, y toda la información relevante debe incluirse en la solicitud, tal como el motivo de la solicitud, el perímetro propuesto del acceso (el acceso basado en palabras clave o el acceso basado en remitentes/destinatarios definidos, son opciones que se recomiendan enfáticamente), la lista de las personas involucradas en el acceso y el manejo de la extracción y su periodo de retención.

El CO Clúster, junto con el Jefe del Departamento Legal del Clúster Head, o en ausencia de éste último, con el apoyo de un asesor legal, valorará las bases razonables de la solicitud, y el respeto a cualquier ley aplicable de privacidad y de protección de datos, y a cualquier regla específica que pueda limitar el acceso, y lo aprobará o rehusará.

El acceso será autorizado solamente para razones relevantes de negocios, y cuando se requiera para cumplir con necesidades operativas críticas, que dependan del tiempo.

Si se autoriza, se comunicará el acceso al Gerente de Seguridad Corporativa de Sistemas de Información y al Director de Regulación de IS, para su valoración técnica. Al mismo tiempo, se le informará al Ejecutivo en Jefe de Cumplimiento Ejecutivo en Jefe de Seguridad e Inteligencia Competitiva. Después de la valoración, el Gerente de Seguridad Corporativa de Sistemas de Información, dentro de un término máximo de 48 horas, se le comunicará al solicitante que se le otorgará el derecho de llevar a cabo el acceso, y cuándo.

Si no se ha nominado ni al CO Clúster ni al Jefe del Departamento Legal del Clúster, tiene que involucrarse al WBS de Compliance.