política del grupo randstad

Política de Protección de datos

randstad

human forward.

Política de Protección de datos

Junio 2021
Función: Departamento de Asesoría Jurídica Global
Número de documento: v3.0 Document classification: C2 Internal Use

1. acerca de esta política

Los Datos Personales son uno de los activos centrales en el negocio de Randstad. Nuestra meta es alcanzar la vida laboral de 500 millones de personas a nivel mundial para el 2030.

Al trabajar en Randstad, esperamos que nuestros empleados entiendan la importancia del manejo y cuidado de datos personales de colegas, talentos, clientes, proveedores y todos las partes interesadas con las que nuestros empleados tomen contacto como parte de su trabajo.

Esta política no pretende evitar el Procesamiento de Datos Personales, sino asegurar un marco uniforme para la protección de datos personales en poder de Randstad, de manera tal que podamos continuar brindando a nuestros talentos y clientes como un socio humano y de confianza en el actual mundo guiado por la tecnología, donde quiera que se encuentren.

La privacidad y protección de una persona física en relación al procesamiento de datos personales es un derecho fundamental en muchas jurisdicciones donde Randstad opera. Por "**Procesamiento**" nos referimos a cualquier actividad que realices en relación a datos personales, como la recolección, registro, organización, componer, almacenar, adaptar o alterar, recuperar, consultar, usar, combinar, restringir, borrar o destruir datos personales.

La mayoría de los países han adoptado leyes para asegurar que todos tengan el derecho a la privacidad y la protección de sus datos personales. Esta legislación establece cómo manejar los datos personales. La violación a esta legislación puede resultar en sanciones, incluyendo fuertes multas impuestas a Randstad o que Randstad sea responsable y deba pagar daños y perjuicios.

En determinados países la legislación local puede imponer normas más estrictas y/o diferentes en relación a los Datos Personales. La legislación local siempre se aplicará y prevalecerá sobre esta política en la medida que exceda las normas de esta política o si impusiese requerimientos más estrictos o brindase más protección. En caso que esta Política brindará más protección que la de la ley local o proveyese garantías, derechos o recursos adicionales a los Titulares de Datos, se aplicará esta Política.

Si fuese necesario, la correspondiente Empresa local del Grupo Randstad debe enmendar esta política para reflejar los mencionados requerimientos locales.

Si hubiese conflicto entre la ley aplicable y esta política, el equipo legal local o el Oficial Local de Datos Personales en relación a la Empresa del Grupo Randstad en cuestión deberá consultar al Oficial Global de Datos Personales para resolver el conflicto y determinar cómo cumplir con esta política y las leyes aplicables.

Las Empresas del Grupo Randstad deben implementar y mantener todo procedimiento local necesario para aplicar esta política, entrenar a todos sus empleados y a cualquiera autorizado al Procesamiento de Datos Personales bajo su control bajo los principios de esta política y designar un Oficial Local de Datos Personales para asesorar y monitorear el cumplimiento de esta política y las leyes aplicables.

Esta política se complementa con guías y modelos (Estándares de Protección de Datos de Randstad) que se elaboran de vez en cuando y es comunicada al Oficial Local de Datos Personales y publicada en la sección DP&IS en la web connect , nuestra intranet.

Esta política es coherente con y se apoya en los Principios Comerciales de Randstad, especialmente los principios 1, 4, 9 y 15:

1. Conocemos y cumplimos con los principios internacionales de derechos humanos, las políticas y procedimientos internos de Randstad y leyes que regulan nuestro negocio.

4. Nos cercioramos de que nuestros registros (incluyendo aquellos que contengan información personal) sean creados, utilizados, archivados y destruidos de acuerdo a la ley.

9. Respetamos el derecho a la privacidad, garantizamos que la información confidencial permanezca confidencial y no abusamos de la información confidencial de otros; y

15. Conservamos y proporcionamos contratos, registros e información financiera completa, justa, puntual, precisa y comprensible.

Esta es la versión 3 de la Política de Protección de Datos Personales del Grupo Randstad. Fue aprobada por la junta ejecutiva del Randstad el 17 de Junio del 2021

Esta política será revisada regularmente para asegurar que cumpla con los requerimientos legales que apliquen y continúe satisfaciendo nuestras necesidades comerciales.

Cualquier duda en concerniente a esta política deberá ser dirigida al Oficial Local de Protección de Datos de la Empresa del Grupo Randstad o el equipo legal local o al Oficial Global de Protección de Datos privacyofficer@randstad.com.

2. lo que esperamos de usted

Es esencial que nuestros empleados (incluyendo oficiales y directores) comprendan cabalmente nuestra política de protección de datos y que sean capaces de identificar situaciones donde puedan surgir cuestiones relacionadas a la protección de datos.

Por eso es importante que leas atentamente lo que se espera de usted.

Randstad apoya que tomes todas las medidas razonables para Procesar Datos Personales en cumplimiento con esta política y las leyes aplicables. Usted puede tener la certeza de que sus propios Datos Personales serán protegidos y de igual modo esperamos que usted respete los estándares de protección de Datos Personalesde otros.

Cuando algo simplemente no se siente correcto para usted acerca de cómo los Datos Personales están siendo tratados, esperamos que contactes a tu gerente y/o tu Data Protection Officer local antes de actuar..

Para los gerentes, esto también significa ser responsable por dar soporte en los esfuerzos de cumplimiento de aquellas personas que reportan a usted, explicando tus principios a tu equipo y asegurando el cumplimiento dentro del área a cargo.

Todos los nuevos empleados recibirán información en relación a esta política en su programa de inducción, y todos los empleados deben completar de manera obligatoria el programa de inducción y programa de actualización, el cual incluirá formación sobre protección de datos personales.

Si sospecha o tiene evidencia de que esta política se ha quebrantado de cualquier manera, esperamos que eleves el tema a tu gerente, con el departamento de legales o con tu Data Protection Officer. Si consideras que el reporte local será poco efectivo o inapropiado deberás utilizar la PC06 - Política para el Reporte de Irregularidades (disponible en la web randstad.com y en randstad.com.ar).

proveedores

Todo esfuerzo debe ser en miras a asegurar que los proveedores (incluyendo agentes, contratados y sus proveedores y subcontratados) que procesen Datos Personales en nombre de Randstad deberán hacerlo en concordancia con esta política. Todas las compañías de Randstad deben utilizar su propio Acuerdo de Procesamiento de Datos que tomará como referencia el Acuerdo de Procesamientos de Datos Global (DPA) para este propósito.

Las compañías del Grupo Randstad pueden auditar estas partes y ante la detección de un hallazgo, Randstad evaluará cómo podrá ser asegurado el cumplimiento, qué riesgos pueden ser mitigados y qué consecuencias podrían darse. Si el incumplimiento persistiera Randstad rescindirá el contrato con el proveedor.

3. principios de protección de datos

Nuestros principios de Protección de Datos requieren que todo Dato Personal sea siempre:

<table>
<tr><td colspan="3">Procesado respetando la privacidad</td></tr>
<tr><td>Procesado en base a

FUNDAMENTOS LEGALES</td><td>Procesado para

PROPÓSITOS ESPECÍFICOS</td><td>Procesado de manera

TRANSPARENTE</td></tr>
<tr><td>ADECUADOS, RELEVANTES Y NECESARIOS</td><td>PRECISOS ACTUALIZADOS</td><td>CONSERVADOS SOLO EL TIEMPO NECESARIO</td></tr>
<tr><td>Procesado en línea con

DERECHOS DE LOS TITULARES DE DATOS</td><td>SEGUROS Y CONFIDENCIALES</td><td>Transferido a terceros

Solo si está permitido por esta política y con el propósito comercial por el cual fue recolectado.</td></tr>
</table>

3.1 Responsabilidad, privacidad por diseño y uso de sistemas aprobados, proveedores y procesos

En Randstad, procesamos los datos personales de manera responsable con la privacidad. Esto significa que no solo tenemos la responsabilidad de cumplir con las leyes aplicables, sino que debemos poder demostrar que cumplimos con las mismas.

Para poder hacerlo los dueños del negocio y en última instancia el directorio de Randstad deben:

- ❖ Asegurar que los sistemas, proveedores y procesos a utilizar dentro de su función o línea de negocio fueron evaluados como riesgos de protección de datos. Sistemas, proveedores y procesos que son marcados como un riesgo para la protección de datos durante su evaluación en One Trust no podrán ser utilizados para el procesamiento de datos hasta que ese riesgo haya sido mitigado ("privacidad por diseño"), y
- ❖ Mantener al día los registros de las actividades procesadoras de datos ("data mapping").

Nadie está autorizado a utilizar sistemas, proveedores y procesos para almacenar o tratar (de cualquier modo) Datos Personales, que no hayan sido aprobados.

En caso de duda, cualquiera que trate Datos Personales deberá consultar con su Gerente y/o Data Protection Officer local para confirmar si las evaluaciones necesarias fueron realizadas y se obtuvo la aprobación del sistema, proveedor y procesos a utilizar.

3.2 Base legal

Para que los Datos Personales sean procesados de acuerdo a la ley, se deben reunir ciertas condiciones. Una de ellas es que los Datos Personales únicamente pueden ser procesados si hay un fundamento legal para hacerlo.

Cuando sea permitido por la ley aplicable, se debe otorgar preferencia a los siguientes fundamentos legales:

- ○ **Necesidad (pre-)contractual** Los Datos Personales son procesados cuando es necesario redactar y firmar un acuerdo con el titular de los Datos. Este es un caso en el que el procesamiento de los Datos Personales es necesario para la ejecución de los servicios de HR aceptados por nuestros talentos (incluyendo servicios de reclutamiento y selección, mediación, staffing, payroll, desarrollo del personal, orientación de carrera, coaching, planificación, y administración de personal y salarios);

- ○ Un **interés legítimo** de Randstad (o de una tercero a quien se le revelan los Datos Personales), siempre que esos intereses no se contrapongan con los intereses o derechos fundamentales de los Titulares de Datos cuyos Datos Personales están siendo procesados;

- ○ El Procesamiento se realiza en cumplimiento de una **obligación legal** a la cual la Empresa del Grupo Randstad está sujeta (ej.: obligaciones de la seguridad social o impositivas);

- ○ El Sujeto de Datos ha sido informado y haya dado su **consentimiento** de manera documentada (únicamente cuando Randstad no pueda basarse en ninguno de los supuestos anteriores).

Cuando se recolectan Datos Personales Sensibles, se requiere una mayor protección y deberá ser procesado únicamente cuando haya una obligación legal y con el consentimiento expreso del Titular de Datos

3.3 Procesamiento limitado por una finalidad

Los Datos Personales solamente pueden ser procesados para los fines específicos informados al Titular de Datos cuando éstos fueron recolectados por primera vez o por cualquier otro fin específicamente permitido por la ley vigente.

Esto significa que no se deben recolectar Datos Personales por una finalidad y luego utilizarlos para otra.

Para Randstad, las finalidades pueden, entre otras, estar relacionadas con la provisión de servicios, que incluye reclutamiento y selección, mediación, personal temporario, Tercerización del Proceso de Reclutamiento (Recruitment Process Outsourcing - RPO), Programas de Gestión de Servicios (Managed

Services Programs - MSP), payroll; desarrollo personal, orientación de carrera, coaching y administración de salarios y personal

Sin embargo puede que el procesamiento de Datos Personales por una nueva finalidad esté justificado bajo las leyes aplicables ex. La nueva finalidad guarda relación con el fin original, Randstad tiene una clara obligación establecida por ley o el consentimiento es obtenido.

Si se vuelve necesario procesar datos personales para un nuevo fin, debes evaluar los riesgos potenciales por protección de datos personales ('privacidad por diseño'). Puede ser necesario informar al Titular de los Datos Personales de la nueva finalidad para brindarle la posibilidad que se oponga.

3.4 Procesamiento transparente

Somos transparentes con los Titulares de Datos respecto a que sus Datos Personales están siendo procesados. Cuando recolectamos Datos Personales tomamos las medidas necesarias para informar a los Titulares de Datos en una manera fácil, clara y accesible (en la mayoría de los casos mediante el Aviso de Privacidad), **quién** es el Controlador de Datos (que compañía del Grupo Randstad es responsable del procesamiento), **para qué** fines se Procesan los datos, **cómo** serán Procesados, las identidades de las **personas a la cual** se le pueden revelar los datos (tales como clientes y/u otras Empresas del Grupo Randstad), a **dónde** serán transferidos o desde donde serán accesibles y cuáles son sus **derechos** en relación a su información según la ley vigente.

3.5 Adecuados, relevantes y limitados a lo que sea necesario en relación a los propósitos

Los Datos Personales sólo deben recolectarse y procesarse en la medida que un fin específico lo requiera y que sea claro para el Titular de los Datos Personales. Cualquier dato que no sea necesario para ese propósito no deberá ser recolectado.

El Procesamiento de Datos Personales debe estar restringido a los Datos que sean razonablemente adecuados y relevantes para el propósito en cuestión.

Si necesitas conservar cierta información sólo sobre determinados individuos, solo deberás almacenar la información de esos individuos, la información probablemente sea excesiva e irrelevante en relación a otras personas.

No debemos conservar Datos Personales bajo la premisa que podrían llegar a ser útiles en algún futuro.

3.6 Precisos, actualizados y solo cuando son necesarios

Los Datos Personales deben ser precisos y mantenerse al día. Se deben tomar medidas para verificar la exactitud de cualquier Dato Personal , en el punto de obtención y en intervalos regulares posteriormente.

Los Datos Personales son imprecisos si son incorrectos o engañosos respecto a cualquier hecho.

Todas las Compañías del Grupo Randstad deben ser cuidadosas al recibir cualquier comunicación de un Titular de Datos cuestionando la veracidad de los Datos Personales. Cuando se tome conocimiento de que los Datos Personales son incorrectos o engañosos, Randstad debe tomar acciones razonables para corregir o eliminarla tan pronto sea posible.

3.7 Conservados no más tiempo del necesario

Mientras exista una obligación legal que lo establezca (como por ejemplo leyes laborales o impositivas) Randstad tiene un deber legal de retenerla de acuerdo a la Política de retención de datos.

Los Datos Personales que no estén sujetos a períodos específicos de retención de acuerdo a la ley vigente deberán ser conservados mientras sean necesarios para cumplir el fin para el cual los Datos Personales son procesados.

Los Datos Personales deben ser eliminados de forma segura o anonimizados cuando el periodo de retención concluya. Esto puede significar que cierta información debe ser eliminada mientras que otra puede ser conservada.

3.8 Procesados conforme a los derechos de los Titulares de Datos

Los Titulares de Datos Personales conservan ciertos derechos sobre sus Datos Personales y se deberán implementar todas las medidas que permitan ejercer esos derechos que de acuerdo a la ley aplicable pueden incluir:

- Derecho de acceso
- Derecho de rectificación
- Derecho de eliminación
- Derecho a objetar el Procesamiento
- Derecho a no ser sujeto de decisiones automatizadas, incluyendo tipos de perfiles.

Cada compañía del Grupo Randstad debe implementar procedimientos para manejar de manera adecuada y oportuna los requerimientos de los Titulares de Datos para el ejercicio de sus derechos.

3.9 Seguridad de los Datos Personales y obligación de reportar incidentes

Cuando estás tratando Datos Personales debes proteger la confidencialidad, integridad y disponibilidad de los Datos Personales y estar atento al cumplimiento de los requerimientos de la seguridad de la información como está establecido en su empresa del Grupo Randstad sobre la base de la política de seguridad de la información.

Toda actividad sospechosa o real sobre incidentes de seguridad deben ser inmediatamente notificados al Data Protection Officer Local y al Information Security Officer.

Randstad debe implementar medidas técnicas y organizacionales apropiadas para asegurar el nivel de seguridad en concordancia con el nivel de riesgo que resulte del procesamiento (ej. destrucción accidental o malintencionada, pérdida, alteración, revelación no autorizada, o acceso a Datos Personales).

Randstad debe:

- implementar procedimientos Standard en gestión de incidentes (actualizados regularmente);
- Implementar un canal para asegurar los reportes de incidentes de seguridad de manera oportuna y efectiva;

- reportar incidentes vía el sistema "case management system" (CMS) a Global (de acuerdo a los parámetros definidos en el procedimiento de gestión de incidentes);
- Entrenar a todo el personal en cómo identificar y reportar (internamente) incidentes de seguridad (incluyendo al Directorio);
- Entrenar al equipo de gestión de incidentes y Directorio en el procedimiento de gestión de incidentes;
- Cuando sea requerido por la legislación vigente, notificar a la Autoridad de Protección de Datos Personales el hallazgo de la infracción dentro de los plazos aplicables;
- Cuando sea requerido por la ley, notificar a los Titulares de Datos afectados.

3.10 Transferencias de Datos Personales

Los Datos Personales se pueden transferir solamente a otra entidad dentro del Grupo Randstad o con clientes y proveedores, si esa transferencia cumple con los principios de protección de datos y los lineamientos establecidos en esta política y/o en legislación complementaria sobre Protección de Datos personales.

Compartiendo Datos Personales entre compañías del Grupo Randstad y control conjunto

Para la operación y gestión eficiente de nuestro negocio, las compañías del Grupo Randstad pueden definir conjuntamente los propósitos y medios para el Procesamiento de Datos Personales (controladores conjuntos) o compartir los Datos Personales entre ellos.

Transferencia Entre Grupo

Para permitir compartir los Datos Personales entre las compañías del Grupo Randstad, se aplicará el acuerdo de Protección de datos Intra-Group, salvo que las compañías del Grupo Randstad involucradas tengan un acuerdo específico que rija para esa transferencia de Datos Personales.

Control Conjunto

Cuando dos o más compañías del Grupo Randstad conjuntamente determinen los fines y medios del procesamiento y donde la GDPR aplique al procesamiento, estas compañías del Grupo Randstad serán conjuntamente Controladores. En esos escenarios, deberán:

- Acordar un documento para el registro de las actividades procesadoras ('data mapping'):
  - Una descripción de la actividad procesadora controlada conjuntamente;
  - La identificación de las compañías del Grupo Randstad que son conjuntamente Controladores;
  - Los roles y responsabilidades acordados en relación al procesamiento de Datos Personales;
- Informar a los Titulares de Datos involucrados (3.4 procesamiento transparente) y tener un resumen sobre el acuerdo a disposición de estos.

Digital Factory, IT, HR, Legal & Compliance, por ejemplo, son funciones donde puede surgir el control conjunto cuando varias compañías del Grupo Randstad determinan los fines del procesamiento. Por ejemplo: un caso de mala conducta financiera es reportado a través del Procedimiento de reporte de malas conductas por un empleado corporativo a Randstad. El caso puede tener consecuencias para Randstad N.V. así como para la OpCo. Randstad N.V. y la OpCo investigarán conjuntamente el caso. El procesamiento de Datos Personales en conexión con esta investigación es una actividad de procesamiento controlada conjuntamente.

Sin embargo, el mero hecho de que dos o más compañías del Grupo Randstad estén involucradas en el procesamiento de Datos Personales no significa por sí mismo que sean controladores conjuntos (ni siquiera cuando el procesamiento se relaciona con Digital Factory, IT, HR, Legal & Compliance or Enterprise Clients).

La autoridad de Datos Personales en los Países Bajos es la principal autoridad supervisora en relación a actividades de procesamiento controladas conjuntamente en las que Randstad N.V. está involucrada.

Compartiendo Datos Personales con terceros

Localización de los Datos y transferencias internacionales de Datos Personales

Al implementar esta política y en particular cuando se transfiera Datos Personales a otro país, las compañías del Grupo Randstad deberán tomar en consideración cualquier requerimiento legal local que establezca condiciones específicas, incluyendo la localización de los Datos y la transferencia de Datos Personales.

Proveedores

Randstad debe como práctica habitual utilizar sus Acuerdos estándar para el procesamiento de Datos tomando como referencia los Términos y Condiciones del Grupo Randstad y el Acuerdo para el procesamiento de Datos del Grupo Randstad (DPA).

Si los servicios contratados involucran la revelación de Datos Personales, acceso o por cualquier modo procesados por el proveedor aplicará lo siguiente:

- Solo los proveedores que ofrezcan garantías suficientes de implementar medidas técnicas y organizacionales apropiadas (luego de completar la evaluación correspondiente en OneTrust) podrá ser seleccionado.
- Los Acuerdos de protección de Datos deben ser firmados previo a revelar, acceder o recolectar cualquier Dato Personal, o procesado de cualquier otro modo. Se requerirá lo siguiente:
  - Los Términos y Condiciones estándar de Randstad, incluyendo el Código Global de proveedores.
  - Requerimientos de seguridad de la Información de los proveedores de Randstad.
  - el Acuerdo para el procesamiento de Datos de Randstad (salvo que el Proveedor actúe como controlador de Datos en cuyo caso no será requerido. Nota: para proveedores de mediano o alto riesgo el Acuerdo estándar puede no ser suficiente e incluirá obligaciones adicionales al proveedor para mitigar los riesgos identificados en la evaluación en OneTrust);

- ➢ Cuando sea aplicable, los acuerdos de transferencia de datos (ej. Cuando se contrate un proveedor de EEUU mientras que la OpCo se encuentre en los EEA, o sea contratado globalmente).

Clientes y otras terceras partes

La transferencia de Datos Personales con terceras partes puede ser permitida si es necesario para la ejecución de un contrato con el Titular de Datos Personales (ej. términos y condiciones firmados por el candidato, fondos de pensión y compañías de seguro), para cumplir con las leyes de protección de datos (ej. La transferencia de Datos Personales al Ministerio de Trabajo y AFIP), si el Titular de Datos ha dado su consentimiento informado y documentado (ej. Compartir Datos Personales de candidatos a clientes), para proteger derechos (por ejemplo en juicio), o en situaciones de emergencia donde la transferencia es necesaria para proteger los intereses vitales del Titular de los Datos (ej. Por seguridad o por motivos de salud e higiene). En otros casos, el departamento legal o el Data Protection Officer de Randstad deberá ser consultado antes de transferir Datos Personales a un tercero.

4. Roles y Responsabilidades

Directorio Local

Es la responsabilidad del Directorio de Randstad: (1) conducir el negocio cumpliendo con la legislación aplicable y esta política; (2) brindar apoyo a todos los departamentos para cumplir sus obligaciones cumpliendo con la legislación aplicable y esta política; y (3) confirmar que Randstad da cumplimiento a la legislación aplicable y esta política.

Gerentes de líneas de negocios

Los gerentes de líneas de negocios y el Directorio de Randstad son responsables por:

- ❖ Asegurar que sistemas, proveedores y procesos a utilizar dentro de sus funciones o líneas de negocio fueron evaluados por riesgos relacionados a la protección de Datos Personales. sistemas, proveedores y procesos que fueron marcados como un riesgo durante la evaluación de riesgo (OneTrust) no podrán ser utilizados para el procesamiento de Datos Personales hasta que esos riesgos sean mitigados ("privacidad por diseño"), y
- ❖ Mantener actualizados los registros de las actividades de procesamiento ("data mapping").

Local Data Protection Officer

Responsabilidades clave del Data Protection Officer Local incluyen:

- ❖ Supervisar y confirmar el cumplimiento de la Empresa del Grupo Randstad con esta política y la ley vigente de Protección de Datos. Aconsejar y asistir al directorio y gerentes de líneas de negocio sobre el cumplimiento de la legislación sobre de Protección de Datos, esta política y las estrategias de negocios en esta área.

- ❖ Resolver conflictos entre la ley vigente y esta política consultando con el Data Protection Officer del Grupo.

- Reportar al Directorio sobre el estado de cumplimiento con esta política y la legislación de Protección de Datos. Reportar al Data Protection Officer Global sobre el estado de cumplimiento con esta política y la legislación local de Protección de Datos. Esto incluye reportar sobre un posible o efectivo incumplimiento y proveer consejo en como remediarlo. Ser el principal punto de contacto para la Autoridad de Protección de Datos en el país y para las personas que deseen hacer uso de sus derechos contra Randstad (ej. Involucrados en una filtración de datos).

Data Protection Officer Global

Responsabilidades clave del Data Protection Officer Global incluyen:

- Aconsejar a la Junta Ejecutiva y gerentes de líneas de negocio de Randstad sobre temas de Protección de Datos.
- Recomendar modificaciones a esta política para garantizar que cumpla con los requisitos legales vigentes y las necesidades de Randstad.
- Coordinar la comunidad de Protección de Datos de Randstad.
- Colaborar con la Gerencia de Riesgo, Legales, IT y otros departamentos en asuntos de Protección de Datos.
- Supervisar que Randstad Holding y las compañías del Grupo Randstad cumplan con la legislación sobre protección de Datos Personales y esta política, reportando al Directorio de Randstad N.V. sobre el estado de cumplimiento de Randstad N.V. con la legislación sobre protección de Datos Personales y esta política.
- Brindar apoyo al Data Protection Officer local supervisando el cumplimiento de las Empresas del Grupo Randstad con esta política.
- En colaboración con el Data Protection Officer Local, promover un enfoque coherente a los temas de Protección de datos en todas las empresas del Grupo Randstad.
- Brindar apoyo y guía a las Empresas del Grupo Randstad implementando esta política y los procedimientos y programas de cumplimiento relacionados.
- Resolver cualquier conflicto o desacuerdo en relación a los requerimientos de esta política u otros asuntos que se relacionen con la protección de datos

Risk & Auditoria (R&A)

Responsabilidades clave de Risk & Auditoría (R&A) en relación a esta política incluyen:

- Asesorar de manera independiente y obtener tranquilidad sobre el cumplimiento y adhesión de la legislación aplicable, así como las políticas internas y procedimientos de Randstad Global y las compañías locales del Grupo Randstad dentro del plan anual de R&A.
- En base al riesgo crítico, validar el monitoreo de las actividades realizadas por por el Directorio en relación a esta política.
- En cuanto a los riesgos y controles relacionados a esta política, R&A también brindará apoyo en las siguientes actividades:
  - Facilitar y cuestionar el diseño y los parámetros de riesgo y control de la estructura (ej. el riesgo de los procesos de Directorio y el Marco de control clave "KCF").
  - Proveer metodología y guía en oportunidades y gestión de riesgo.
  - Facilitar las evaluaciones de controles internos (KCF) & declaraciones.

apendice I

definiciones de términos clave

Controlador de Datos se refiere a la entidad que decide por qué y cómo son Procesados los Datos Personales. Tiene la responsabilidad de establecer prácticas y políticas alineadas con las leyes y normas de Protección de Datos. Randstad y sus Empresas del Grupo son el Controlador de Datos de la mayor parte de los Datos Personales utilizados en nuestro negocio.

Procesador de Datos se refiere a una entidad legal separada del Controlador de Datos que procesa Datos Personales en su nombre. Los empleados de los Controladores de Datos se encuentran excluidos de esta definición, pero podría incluir a proveedores y clientes u otras terceras partes que tratan Datos Personales en nuestro nombre. En algunas situaciones, una Empresa del Grupo Randstad puede actuar en el rol de Procesador de Datos, por ejemplo, para algún MSP o servicios de payroll, ya sea en nombre de un cliente, proveedor y otra Empresa del Grupo Randstad.

Titulares de Datos se refiera a cualquier persona que puede ser identificada, directa o indirectamente, por medio de un identificador de quien recolectamos información en conexión con nuestro negocio y las operaciones tal como (entre otras) el talento de Randstad (candidatos personal temporario y tercerizado), personal interno, (posibles) clientes y otras partes interesadas (incluyendo proveedores, asesores, auditores, websites y visitantes de las sucursales).

Datos Personales es cualquier dato que directa o indirectamente se refiera a un individuo (ej. nombre, email, teléfono, nacimiento, género, identificaciones únicas, raza, religión, salud, afiliación gremial, calificaciones, opinión, experiencia) y que se pueden obtener en cualquier formato (ej. papel, digital, foto, video, sonido).

Procesos y Gerentes de línea de negocios refiere a toda iniciativa de Randstad que los gerentes de línea de negocios han desplegado una nueva o existente iniciativa junto a Randstad para un proceso o producto.

Procesamiento (o Procesar) tiene el significado otorgado en en la sección “acerca de esta política”.

Datos Personales Sensibles incluyen la información sobre el origen étnico o racial de una persona, sus opiniones políticas, religiosas o creencias similares, adhesión a sindicatos, condición física o mental, vida sexual, o sobre un delito que haya cometido o se le atribuya, lo resuelto en esos juicios o la sentencia emanada por los jueces. Los Datos Personales Sensibles solamente se pueden Procesar bajo condiciones estrictas y requerirán del consentimiento expreso de la persona en cuestión. Otra información, como el CUIL o datos bancarios o de tarjeta de crédito, pueden ser igualmente confidenciales aun si no estuviesen clasificados como "sensibles". En algunos países, las imágenes de fotos o videos pueden calificarse como Datos Personales sensibles porque revelan el origen racial o étnico de una persona y/o creencias religiosas o similares.

Acuerdos estándar significa los modelos y guías específicos que dan soporte y complementan esta política y son redactados, actualizados regularmente y comunicados por el Data Protection Officer Local y publicados en la intranet y la web “connect” de DP&IS.