ALMACENAMIENTO Y TRATAMIENTO DE DATOS SENSIBLES RELATIVOS A LA SEXUALIDAD DE LOS EMPLEADOS.

1. **¿Cómo se regula la protección de datos personales en Uruguay?**

La Ley N° 18.331 de Protección de Datos Personales y Acción de "Habeas Data" (en adelante, la "Ley") modificada por la Ley N° 19.670 de Rendición de Cuentas y Balance de Ejecución Presupuestal correspondiente al ejercicio 2017 y los Decretos 414/009 y 64/020 regulan la protección de datos personales en Uruguay.

2. **¿Cómo se definen los datos personales en Uruguay?**

La Ley define en su artículo 4 a los datos personales como toda *"información de cualquier tipo referida a personas físicas o jurídicas determinadas o determinables".*

3. **Los datos relativos a la sexualidad de las personas, ¿son datos personales?**

Si. Incluso tienen una protección mayor puesto que son considerados como datos sensibles.

En este sentido, la Ley define a los datos sensibles en su artículo 4 como *"datos personales que revelen origen racial y étnico, preferencias políticas, convicciones religiosas o morales, afiliación sindical o informaciones referentes a la salud o a la vida sexual".*

Por su parte el artículo 18 de la Ley dispone que los datos sensibles únicamente pueden ser incorporados a una base de datos si el titular de dichos datos prestó su consentimiento de forma previa, expresa y por escrito al tratamiento de los mismos. La Ley sólo admite la formación de bases de datos con datos sensibles en ciertos casos puntuales.

4. **¿Cómo pueden las empresas almacenar y tratar datos sensibles relativos a la sexualidad de sus empleados?**

Las empresas tienen dos formas de recopilar este tipo de datos:

a. ***Consentimiento expreso y por escrito de los empleados.***

Obteniendo el consentimiento expreso y por escrito de sus titulares en forma previa al inicio del tratamiento, la empresa podría almacenar y tratar datos sensibles de índole sexual.

Tratándose de datos sensibles, el procesamiento siempre implica un riesgo mayor ya que los derechos de los titulares se pueden ver afectados en mayor medida. En función

de esto, a efectos de llevar este registro de forma legítima, tengan en cuenta los siguientes puntos:

- Al recabar el consentimiento de los empleados, se les debe informar sobre (i) la identificación del responsable del tratamiento y de los datos sensibles a tratarse (en este caso datos relativos a la sexualidad); (ii) la finalidad específica del tratamiento de datos; (iii) el carácter facultativo de las respuestas; (iv) la consecuencia de no proporcionar los datos personales; (v) la posibilidad del titular de ejercer los derechos de acceso, de rectificación, de impugnación, de inclusión, de supresión y de impugnación de valoraciones personales y (iv) el plazo de conservación de los mismos.

- No puede existir un trato discriminatorio hacia los empleados en función de la información recolectada.

- Se debe respetar el principio de finalidad, según el cual los datos únicamente pueden ser procesados para los fines que motivaron su obtención (razones estadísticas, planificación de instancias de concientización e inclusión, etc.). Cualquier uso de esta información para fines secundarios sería ilegítimo.

- Se debe respetar el principio de minimización de datos, según el cual los datos recolectados deben limitarse a los estrictamente necesarios en relación a los fines para los que son tratados.

- Se deben adoptar medidas de seguridad adecuadas que garanticen la protección de los datos recolectados. Además de medidas técnicas en los sistemas de seguridad de la empresa, también son necesarias medidas organizativas, como, por ejemplo, el acceso restringido y que únicamente puedan acceder un número limitado de personas según sea estrictamente necesario.

b. Anonimización o disociación de datos sensibles.

Otra opción para poder procesar datos sensibles de índole sexual es a través de un proceso de anonimización o disociación de los datos que no permita identificar al titular.

La disociación de datos es aquel tratamiento de datos personales en el que la información obtenida no puede vincularse a una persona determinada o determinable. La Unidad Reguladora y de Control de Datos Personales ("URCDP") publicó una Guía sobre Criterios de Disociación de Datos Personales[1] en la que se establece el procedimiento para lograr la anonimización y sus diferentes etapas (preanonimización, anonimización y control).

Se entiende que una anonimización realmente resulta eficaz cuando imposibilita distinguir a una persona en un conjunto de datos, o inferir cualquier tipo de información a partir de ese conjunto.

[1] https://www.gub.uy/unidad-reguladora-control-datos-personales/comunicacion/publicaciones/guia-criterios-disociacion-datos-personales

Como principio, para garantizar que ya no se puede identificar al titular del dato, no basta con eliminar los elementos que pueden servir para identificarlo directamente, sino que se debe tomar las medidas necesarias adicionales, por ejemplo, realizar análisis periódicos del riesgo de reidentificación y cruzamientos de datos, para evitar que se produzca la identificación del titular, la que va a depender del contexto y de los fines del tratamiento que va a ser objeto.

5. **Derecho a la actualización de datos personales.**

Uno de los derechos que consagra la Ley, es el que tienen los titulares de los datos de actualizar aquellos datos que resulten inexactos a la fecha de ejercicio del derecho.

Por ejemplo, de conformidad con el artículo 6 de la Ley Integral para Personas Trans N°19.684, una vez que persona realice la adecuación de nombre o sexo en sus documentos identificatorios, podrá exigir a su empleador que se actualicen sus datos personales de la base de datos inscripta por la empresa. El responsable de la base de datos o del tratamiento deberá realizar la misma en un plazo máximo de 5 días hábiles de recibida la solicitud, sin cargo alguno para el titular.

El incumplimiento de esta obligación por parte del responsable de la base de datos o del tratamiento o el vencimiento del plazo, habilitará al titular del dato a promover la denominada acción de habeas data.