Modelo de prevención de infracciones de la ley de protección de datos

Chile queda a la vanguardia en materia de protección de datos en la región y ello implicará un esfuerzo relevante por parte de las organizaciones que deberán adecuar sus normativas internas a la brevedad.

Este incidente que hoy es recordado especialmente porque puso en evidencia –nuevamente– nuestra legislación anacrónica en esta materia, será considerado parte de nuestro precario pasado.

En efecto, el viernes 13 de diciembre pasado se publicó la Ley Nº 21.719, que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales, normativa largamente esperada por la comunidad de especialistas en datos y la prevención de riesgos legales.

En lo que interesa propiamente al cumplimiento o compliance, la norma regula el **modelo de prevención de infracciones** en materia de datos personales que me dispongo a resumir en lo que sigue:

Se trata de un modelo voluntario, como sucede con la generalidad de los modelos de prevención, y que debe contener, a lo menos, los siguientes elementos que señala la norma:

Esta regulación interna, además, deberá incorporarse expresamente como obligación en los contratos de trabajo o de prestación de servicios de todos los trabajadores y prestadores de servicios de las entidades que actúen como responsables de datos o los terceros que efectúen el tratamiento, incluidos los máximos ejecutivos de la misma o, bien, como una obligación del reglamento interno de orden higiene y seguridad.

Como se puede apreciar, los elementos que considera el legislador para entender que estamos en presencia de un modelo preventivo son muy similares a los de un sistema preventivo general de compliance (como el penal, por ejemplo, que contempla el artículo 4º de la actual Ley 20.393).

En relación con la **función de compliance**, será ejercida, como vimos, por el delegado de protección de datos personales (DPD/DPO) que deberá ser designado por la máxima autoridad directiva o administrativa del responsable de datos. La norma agrega que se considerará como la máxima autoridad directiva o administrativa al directorio, un socio administrador o a la máxima autoridad de la empresa o servicio, según corresponda.

Respecto de la **autonomía de la función**, se señala expresamente que el delegado de protección de datos deberá contar con autonomía respecto de la administración, en las materias relacionadas con la ley, disponiendo de una excepción respecto de las micro, pequeñas y medianas empresas, en que el dueño o sus máximas autoridades podrán asumir personalmente las tareas de delegado de protección de datos.

Sabemos que la autonomía de la función hace referencia a la capacidad del órgano de compliance de actuar por iniciativa propia, sin necesidad de estar recibiendo órdenes o mandatos específicos.

La **independencia de la función** también se considera en la norma, al disponer que el delegado de protección de datos podrá desempeñar otras funciones y cometidos, procurando mantener la independencia en su función. Y agrega que el responsable garantizará que dichas funciones y cometidos no den lugar a conflictos de intereses.

En temas de independencia es importante señalar que lo relevante acá es contar con un encargado que ejerza la función con neutralidad frente a las variables o incentivos económicos.

Dispone, asimismo, una norma que frecuentemente no está escrita pero existe en las grandes empresas, esto es, que las sociedades o entidades que pertenezcan a un mismo grupo empresarial, empresas relacionadas o sujetas a un mismo controlador en los términos previstos en la Ley de Mercado de Valores, podrán designar un único delegado de protección de datos, siempre que todas ellas operen bajo los mismos estándares y políticas en materia de tratamiento de datos personales, y el delegado sea accesible para todas las entidades y establecimientos.

Es interesante advertir que la norma se hace cargo del importante tema de la **estatura de la función de compliance** y agrega al respecto que la designación debe recaer en una persona que reúna los requisitos de idoneidad, capacidad y conocimientos específicos para el ejercicio de sus funciones. Probablemente esto obligará a las entidades a tener disponible una descripción del cargo que aborde con propiedad este requisito.

Por otra parte, se aborda también el **secreto de la función**, obligando al delegado de protección de datos a mantener estricto secreto o confidencialidad de los datos personales que conociere en ejercicio de su cargo. Incluso, los funcionarios públicos que desempeñen estas funciones e infrinjan este deber de secreto o confidencialidad, serán sancionados conforme al tipo penal de revelación de secretos (artículos 246 a 247 bis del Código Penal).

Además, se señala que el responsable de datos deberá disponer que el delegado cuente con los medios y facultades suficientes para el desempeño de sus funciones, debiendo otorgarle los recursos materiales necesarios para realizar adecuadamente sus labores, en consideración al tamaño y capacidad económica de la entidad.

Y en relación con las facultades, la norma señala, a modo ejemplar, cuáles pueden ser esas facultades esperadas: informar y asesorar respecto de las disposiciones legales y reglamentarias relativas al derecho a la protección de los datos personales y a la regulación de su tratamiento; promoción de la política; supervisión del cumplimiento; difusión y formación; gestión de riesgos; planificación trabajo anual, reportes, resolución de consultas y cooperación con la agencia, entre otras

En materia de **certificación del modelo**, se señala que la Agencia de Protección de Datos será la entidad encargada de certificar que el modelo de prevención de infracciones cumple con los elementos que contiene la ley y el Reglamento que la propia Agencia deberá dictar.

Es probable, en todo caso, que el sistema termine funcionando de la manera en que lo hacen actualmente los planes de cumplimiento de protección a los derechos de los consumidores, en que una entidad certificadora autorizada por el Sernac emite un informe que sirve de insumo para la decisión final de aprobación por la parte del regulador.

La ley agrega que la Agencia incorporará al Registro Nacional de Sanciones y Cumplimiento a las entidades que posean una certificación vigente y que estos certificados tendrán una vigencia de tres años y podrán ser dejados sin efecto en los casos que se señalan en el propio cuerpo legal: revocación, disolución de la persona jurídica, resolución judicial, cese de actividades, entre otras.

Pero ¿qué pasa con los garrotes y las zanahorias? En el caso de filtración de datos del Servel que citaba al comienzo, la multa máxima que arriesgaba la entidad podía ser de un par de millones de pesos. Ahora las multas pueden llegar a las 20 mil unidades tributarias mensuales, esto es, USD 1,5 millones aproximadamente, que puede recargarse hasta en un 50% si no se adoptan medidas oportunas. Y en caso de reincidencia, la multa podría ascender a un monto de tres veces el valor asignado a la infracción. Es un buen garrote.

Las zanahorias, por su parte, pueden encontrarse en el esquema de circunstancias atenuantes: la cooperación, la reparación, la irreprochable conducta anterior en la materia, la autodenuncia ante la Agencia y en lo que interesa acá: "**El haber cumplido diligentemente sus deberes de dirección y supervisión"** para la protección de los datos personales sujetos a tratamiento, lo que se verificará con la **certificación** de la que hablábamos más arriba.

Como puede apreciarse, Chile queda a la vanguardia en materia de protección de datos en la región y ello implicará un esfuerzo relevante por parte de las organizaciones que deberán adecuar sus normativas internas a la brevedad.

Fuente: https://www.elmostrador.cl/

LINK DE LA NOTICIA

1. Designación de un delegado de protección de datos personales, que se conoce frecuentemente por las siglas DPD o DPO.
2. Definición de sus medios y facultades.
3. Identificación del tipo de información que la entidad trata, su ámbito territorial, categoría, clase o tipos de datos o bases de datos que administra, y la caracterización de los titulares de datos.
4. Identificación de procesos de negocio que son riesgosos para la comisión de las infracciones leves, graves y gravísimas señaladas en los artículos 34 bis, 34 ter y 34 quater.
5. Protocolos, reglas y procedimientos que permitan control.
6. Mecanismos de reporte interno y externo (a la Autoridad de Protección de Datos) para cumplir con el deber de reporte de vulneraciones a las medidas de seguridad.
7. Sanciones y procedimiento denuncias.

Hace un tiempo, el Servicio Electoral de Chile (Servel) publicó en internet y posibilitó la descarga de una base de datos personales de 15 millones de electores habilitados para votar y que contenían no solo los nombres de los electores, sino además número de RUT asociado, militancia política, edad, sexo e, incluso, la pertenencia a pueblos originarios.