NOTEBOOK DATA

Marzo 2022 N°1

ZEGARRA AGUILAR
abogados

Teléfono: (51-54) 417 369
Calle Mariscal Benavides No 407 Selva Alegre, Arequipa
Arequipa – Perú

Encargada de Edición:

Sharom Salas Medina Área de Protección de Datos Personales.

TABLA DE CONTENIDO

¿Se pueden instalar cámaras en los colegios? La videovigilancia en los entornos escolares: Tratamiento Legal
Adolfo Zegarra Aguilar 2

Cumplimiento legal de protección de datos personales dentro de las relaciones laborales
Sharom Salas Medina 5

Datos personales: Preguntas más frecuentes 9

Ley de protección de datos personales en el sector salud
Renso Fernan Zegarra 11

Importancia de la implementación de los sistemas de protección de datos personales
Renato Lozada Herrera 14

Datos sobre la materia en los últimos años 16

ZEGARRA AGUILAR
abogados

El contenido de este documento es meramente informativo y no puede reemplazar a las consultas legales

Presentación

En nuestro país existe una regulación sobre Protección de Datos Personales, aunque todavía algunos estén al margen, esta comprende, básicamente, la Ley N° 29733 – Ley de Protección de Datos Personales, el Decreto Supremo N° 003-2013-JUS – Reglamento de la Ley de Datos Personales y la Directiva de Seguridad de la Información. El incumplimiento de las disposiciones establecidas en dichas normas puede acarrear multas entre 0.5 y 100 UIT.

En el panorama internacional, mucho antes que en el territorio nacional, la protección de datos personales resulta imperante, una prueba de ello es el Reglamento General de Protección de Datos de la Unión Europea (Reglamento UE 2016/679), cuyas sanciones por la inobservancia de sus disposiciones son mucho más elevadas que las antes mencionadas.

En este contexto, el Área de Protección de Datos Personales de nuestra firma ha decidido compartir con ustedes, a través de esta publicación, la información más relevante sobre este tema de actualidad con la finalidad de proporcionar elementos suficientes para un adecuado tratamiento de esta data y prevenir la comisión de infracciones que generen contingencias en la gestión de su actividad económica.

Debemos hacer presente que la experiencia adquirida durante los últimos años en materia de Protección de Datos Personales, tanto en la consultoría del día a día, así como en los procesos de implementación del sistema de cumplimiento en esta materia y nuestra participación en procedimientos administrativos, nos permiten alcanzar les este instrumento que esperamos sea de utilidad

WORLD COMPLIANCE ASSOCIATION
ORGANIZACIÓN ASOCIADA

REGRESO A CLASES PRESENCIALES

¿SE PUEDEN INSTALAR CÁMARAS EN LOS COLEGIOS?

LA VIDEOVIGILANCIA EN LOS ENTORNOS ESCOLARES: TRATAMIENTO LEGAL

"...la imagen está considerada como dato personal, razón por la cual, se encuentra dentro del ámbito de protección del marco legal. Es por ello importante tener en consideración que, cualquiera sea la forma, a través de la cual se pretenda hacer uso de la imagen de una persona, es imperativo obtener previamente el consentimiento formal...".

Con la Ley N° 29733 y su Reglamento, aprobado por el Decreto Supremo N° 003-2013-JUS, en el Perú se regula la protección de datos personales. A partir de las normas

Adolfo Zegarra Aguilar
azegarra@zegarralaw.com

ZEGARRA AGUILAR
abogados

antes indicadas la información que identifica o hace identificable a las personas naturales está sujeta a ciertas condiciones que, para su recopilación y ulterior tratamiento, requieren principalmente del consentimiento libre, previo, expreso e informado del titular de los datos. De lo contrario se estaría contraviniendo las disposiciones legales.

Precisamente, en este contexto la imagen está considerada como dato personal, razón por la cual, se encuentra dentro del ámbito de protección del marco legal. Es por ello importante tener en consideración que, cualquiera sea la forma, a través de la cual se pretenda hacer uso de la imagen de una persona, es imperativo obtener previamente el consentimiento formal y expreso de su titular, salvo las excepciones de ley .

En este orden de ideas, debemos manifestar que la videovigilancia, tan común en nuestros días, es una manera recopilar imágenes. En efecto, la necesidad de preservar la seguridad hace que el empleo de medios tecnológicos, como cámaras en accesos físicos, zonas concurridas y otros lugares, sea algo permanente y cada vez con mayor frecuencia en diversos ámbitos, entre estos, los entornos escolares. Situación que ha sido considerada por el contexto legal, debido a su impacto en la vulneración de la privacidad.

Al respecto, la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales aprobó la Directiva N° 001-2020-JUSDGTAIPD, que regula el tratamiento de datos personales captados a través de sistemas de videovigilancia, con fines de seguridad, control laboral y otros, dedicando un acápite especial a los entornos escolares.

Entre las principales disposiciones de la Directiva se debe considerar las siguientes:

- Comunicar a la comunidad educativa la existencia de cámaras y otros dispositivos análogos en un lugar visible, internamente o en espacios abiertos. Para tal fin se colocarán distintivos o carteles. Se puede abarcar espacios públicos o comunes, tales como accesos, patios de recreo, pasillos, comedores, siempre con miras a la protección y defensa del interés superior del niño y del adolescente.

- La zona de videovigilancia deberá ser la mínima imprescindible.

- No deben instalarse cámaras de videovigilancia en zonas privadas o en lugares que afecten la imagen o intimidad en forma desproporcionada. Aunque sí está permitido grabar en las aulas y otros

[2] (i) Datos personales recopilados por entidades públicas en cumplimiento de sus funciones. (ii) Los que se encuentran contenidos en fuentes de acceso al público. (iii) Se hace tratamiento de datos relativos a la solvencia patrimonial o de crédito. (iv) Los necesarios para la preparación, celebración y ejecución de un contrato. (v) Se hace tratamiento de datos personales de salud en circunstancias de emergencia, para prevenir, diagnosticar y tratar al titular (...). (vi) Tratamiento de datos de las entidades sin fines de lucro, cuya finalidad sea política, religiosa o sindical (...). (vii) Se hubiera aplicado un procedimiento de anonimización o disociación. (viii) Para salvaguardar intereses propios del titular. (ix) Para prevenir el lavado de activos, financiamiento del terrorismo u otros delitos, por mandato legal. (X) Información que se brinda a la UIF. (xi) El tratamiento de datos que se realiza en virtud del derecho fundamental a la libertad de información.

lugares en los que se desarrolla la personalidad de los niños y adolescentes, con fines de seguridad, solo en circunstancias excepcionales y justificadas por la presencia de un riesgo objetivo para la seguridad y los derechos fundamentales de los menores.

ZEGARRA AGUILAR
abogados

- El acceso a las imágenes de videovigilancia en los entornos escolares solo debe estar permitido al Director de la institución o a la persona autorizada para tal fin. No es información de libre acceso.

- Se establece que la conservación de las imágenes podrá darse por un plazo máximo de 30 días desde su captación, pudiendo solo guardar las imágenes que muestren algún hecho trascendente que deba ser revelado a los padres de familia o tutores, o por la comisión de actos delictivos, poniendo los hechos en conocimiento de la Policía Nacional o el Ministerio Público.

- Finalmente, todos los demás aspectos están regidos por la Ley y el Reglamento, no debiendo dejarse de lado que, tratándose de menores de edad los datos vinculados a estos tienen el carácter de sensibles.

DATOS PERSONALES EN EL SECTOR LABORAL

CUMPLIMIENTO LEGAL DE PROTECCIÓN DE DATOS PERSONALES DENTRO DE LAS RELACIONES LABORALES

"Dentro de las organizaciones aún no existe una conciencia suficiente sobre la seguridad de los datos ni sobre la manera de garantizar su confidencialidad y el manejo apropiado para evitar su alteración, pérdida, tratamiento o acceso no autorizado."

Todas las esferas de nuestra cotidianidad han sido tomadas por las nuevas tecnologías y en consecuencia han ampliado el acceso a la información, generando nuevos riesgos relacionados principalmente al uso masivo y descontrolado de los datos personales. Esto a su vez ha llevado al surgimiento de marcos normativos para hacerle frente a esos riesgos, pudiendo desprenderse

Sharom Salas Medina
ssalas@zegarralaw.com

ZEGARRA AGUILAR
abogados

nuevas obligaciones y responsabilidades legales para quienes intervienen en el tratamiento de datos personales.

En el entorno laboral dichas tecnologías incluyen procesos tan diversos como la gestión de personal, las comunicaciones internas y externas, las formas de monitoreo y control del trabajo, entre otras. Es una realidad que los empleadores captan, procesan y almacenan una gran cantidad de datos e información sobre sus trabajadores, y es aún más real que estos procesos deben asegurarse de cumplir con lo dispuesto en las normativas sobre protección de datos.

En el Perú se cuenta con la Ley N° 29733 y su Reglamento, aprobado por Decreto Supremo N°003-2013, a través de los cuales se define los conceptos básicos que se deben tener en cuenta en esta materia. La pandemia hizo patente que puedan surgir situaciones inesperadas que lleven a examinar con más cuidado y reevaluar las tensiones entre el derecho a la protección de datos personales como son los de la salud de los trabajadores y el interés legítimo de presentar y garantizar la salud de los mismos en este difícil contexto.

En el ámbito laboral, en cualquier caso, siempre es importante ser consciente de las responsabilidades legales que implica el manejo de datos personales y de los riesgos particulares asociados a su tratamiento. Esto ocurre en gran parte porque no existen desarrollos normativos específicos para las relaciones laborales en esta materia. A nivel internacional, sin embargo, sí existen algunos lineamientos que pueden servir de referente y de esta forma dar algunas luces sobre el asunto que planteamos. El documento titulado Protection of Workers Personal Data, una publicación de la OIT, es el que contiene una suerte de código de privacidad de los trabajadores, en ella se resaltan los principios relacionados con la debida administración de los datos personales en ámbitos laborales. Del mismo modo, un referente interesante es la Guía sobre la Protección de Datos Personales en la Relaciones Laborales, publicada recientemente por la Autoridad Española de Protección de Datos, este documento ofrece un panorama comprensivo de las múltiples facetas de la gestión de personal y la relación laboral en las que surge la necesidad de la protección de datos personales.

Dentro de las organizaciones aún no existe una conciencia suficiente sobre la seguridad de los datos ni sobre la manera de garantizar su confidencialidad y el manejo apropiado para evitar su alteración, pérdida, tratamiento o acceso no autorizado. Las brechas e incidentes de seguridad en el contexto del trabajo remoto se hacen cada vez más frecuentes en nuestro medio; por ejemplo, en un trabajador que por las funciones a su cargo tiene acceso y manejo de datos protegidos o información sensible sobre muchas personas en la organización, las normas sobre protección de datos obligan al empleador a adoptar medidas de seguridad y confidencialidad para prevenir que sus empleados le den mal uso a la información que manejan. Si un trabajador filtra la información, el empleador podría tener que responder ante las multas y eventuales daños y procedimientos administrativos que se generen en caso no haya implementado las medidas adecuadas, por ello, las empresas deben examinar sus prácticas de privacidad, implementar políticas específicas y capacitar a su personal para generar conciencia sobre las buenas prácticas y sobre la protección de los datos personales, a fin de evitar sanciones y demandas judiciales por daños ocasionados ante manejos inapropiados de la información personal.

Por otro lado, en el ámbito de la protección de datos de trabajadores dentro del contexto de una pandemia mundial, se debe guardar confidencialidad sobre esos datos personales. Solo podrán ser revelados de la obligación de confidencialidad, a través de un consentimiento previo, informado, expreso e inequívoco del titular de los datos personales, resolución judicial consentida o ejecutoriada o cuando medien razones fundadas relativas a la defensa nacional, seguridad pública o sanidad pública, sin perjuicio de guardar el secreto profesional.

La Dirección General de Protección de Datos Personales ha emitido la Directiva de Seguridad de la Información Administrada por los Bancos de Datos Personales aprobada por Resolución Directoral No. 019-2013-JUS/DGPDP, Directiva de Seguridad, la cual establece estándares de seguridad según las características particulares de cada banco de datos.

Sin embargo, en el contexto actual la Autoridad de Protección de Datos Personales ha recordado que compartir información sobre la salud de una persona (COVID-19, factores de riesgo, entre otros), sin su consentimiento es una infracción a la LPDP. Esto es muy importante de observar.

ZEGARRA AGUILAR
abogados

DATOS PERSONALES: PREGUNTAS MÁS FRECUENTES

- **¡Qué son los Datos Personales?**

  Son toda aquella información o dato que permite identificar a una persona natural o la hace identificable, como por ejemplo el nombre, el documento nacional de identidad, firma, domicilio, imagen, voz, entre otros.

- **¿Qué son los Datos Sensibles?**

  Los datos personales adquieren calidad de sensibles cuando la información está estrechamente vinculada con la intimidad de la persona, como por ejemplo datos biométricos, origen racial y etnico, ingresos económicos, información relacionada con la salud, entre otros.

- **¿Como proteger los Datos Personales en el Perú?**

  Dentro de nuestro sistema legal, existen dos vías que asegurarían el respeto del derecho de protección de datos a sus titulares.

  Judicialmente, a través del proceso de habeas data, el titular de los datos puede conocer, actualizar, incluir, suprimir o rectificar la información referida a su persona que se encuentre almacenada o registrada en forma manual, mecánica o informática, en archivos, bancos de datos o registros de entidades públicas o privadas que brinden servicios o acceso a terceros. Asimismo, puede suprimir o impedir que se suministren datos de carácter sensible que afecten su intimidad.

  Y administrativamente, a través de una solicitud dirigida al titular del banco de datos o al encargado del tratamiento, siendo así que el titular del dato puede requerir el acceso, rectificación, corrección u oposición a cualquier tratamiento.

- **¿En qué consiste el tratamiento de Datos Personales?**

  Resulta ser cualquier operación o proceso, automatizado o manual, que se realiza sobre los datos personales, tales como recopilación, grabación, registro, almacenamiento, conservación, uso, consulta, transferencia, modificación, supresión, bloqueo, entre otros.

- **¿Qué es el consentimiento para el tratamiento de Datos Personales?**

  Es la autorización que debe brindar el titular para que sus datos puedan ser recopilados y tratados según la finalidad informada. La autorización puede brindarse de forma verbal o escrita; no obstante, para el tratamiento de datos sensibles es indispensable el consentimiento escrito, el cual siempre debe ser previo, informado, expreso e inequívoco.

DATOS PERSONALES: PREGUNTAS MÁS FRECUENTES

¿Cuándo no se requiere consentimiento?

La ley 29733 establece aquellas excepciones a la obligación de contar con consentimiento siendo algunas de ellas cuando los datos personales son recopilados por entidades públicas para el cumplimiento de sus funciones, cuando se encuentran contenidos en fuentes accesibles al público, cuando se trata de datos referidos a la solvencia patrimonial o de crédito por parte de las entidades financieras, cuando los datos sean tratados para prevenir el lavado de activos, financiamiento del terrorismo, entre otros.

- **¿Qué son los bancos de Datos Personales?**

Los bancos de datos personales son el conjunto organizado de datos de carácter personal, que se pueden encontrar en distintos soportes tales como físicos, magnéticos, digitales, ópticos, entre otros; pudiendo tener titularidad pública o privada, y pueden estar organizados de forma automática o manual.

- **¿Quién es el titular y el encargado del tratamiento de Datos Personales?**

En un primer momento, el titular del banco de datos personales es aquella persona natural, persona jurídica privada o entidad pública que establece la finalidad para la recopilación y almacenamiento de los datos personales, así como el tratamiento y las medidas de seguridad que le serán aplicables; mientras que el encargado del tratamiento de datos personales es aquella persona natural o jurídica, pública o privada, que realiza el tratamiento de los datos en nombre y por cuenta del titular del banco de datos.

- **¿Qué es la Autoridad Nacional de Protección de Datos Personales?**

La Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales es el órgano que ejerce la Autoridad Nacional de Protección de Datos Personales, la cual depende del Despacho Viceministerial de Justicia del Ministerio de Justicia y Derechos Humanos y tiene como principal función garantizar el derecho fundamental de protección de datos personales.

- **¿En qué consiste la facultad sancionadora de la Autoridad?**

Consiste en la facultad para iniciar, de oficio o a petición de parte, un procedimiento administrativo sancionador contra el titular del banco de datos, de administración pública o privada, que incurra en cualquiera de las infracciones tipificadas en el Reglamento de la Ley de Protección de Datos Personales, decantando en posibles sanciones materializadas en multas determinadas por unidades impositivas tributarias.

SALUD & DATOS PERSONALES

LEY DE PROTECCIÓN DE DATOS PERSONALES EN EL SECTOR SALUD

"...emerge una obligación para los establecimientos de salud a tratarlos, de contar con un consentimiento escrito, libre, voluntario, consciente e informado, en el cual, conste de manera indubitable la autorización del paciente para que sus datos sean utilizados y trasladados a otras personas, ya sean naturales o jurídicas"

La Ley de Protección de Datos Personales-Ley 29733 y su Reglamento, aprobado por Decreto Supremo Nro. 003-2013, exigen obligaciones a todas las personas en general, incluidas a las que prestan servicios relacionados a la salud, ya sean públicas o privadas; parámetros y cuidados para que los datos de las personas naturales sean tratados (utilizados, compartidos, gestionados, entre otros) de manera idónea.

Renso Fernan Zegarra
rfernanzegarra@zegarralaw.com

ZEGARRA AGUILAR
abogados

Es en este sentido, que el MINSA desde octubre de 2020 a través de la Directiva Administrativa N° 294-MINSA/2020/OGTI, aprobada por la Resolución Municipal N° 688-2020/MINSA, marca pautas para un tratamiento de datos personales idóneos, de acuerdo a las exigencias de la Ley y su Reglamento.

Este dispositivo administrativo, resulta aplicable a todos los establecimientos de salud del sector público y privado del Sistema Nacional de Salud.

De otro lado, define que los Datos Personales en Salud (DPS) son todos aquellos referidos a la situación de salud o enfermedad de una persona o la identifica y la hace identificable individualmente, tales DPS, se generan en todo acto médico, de salud o cualquier atención recibida dentro o fuera de un establecimiento de Salud. Asimismo, los DPS son considerados datos de carácter sensible, reconocidos incluso constitucionalmente, por el derecho fundamental a la intimidad, que en caso sean vulnerados, se les inicie a los establecimientos de salud un procedimiento administrativo sancionador con multas de hasta 100 UITs.

Es por ello que, los directores, gerentes, jefes, médicos jefes, o quienes hagan sus veces en los establecimientos de salud o servicios médicos de apoyo, tienen que disponer las medidas correspondientes para garantizar la protección de los DPS en los procesos de atención que se realizan.

Entonces, al ser datos de carácter sensible, emerge una obligación para los establecimientos de salud a tratarlos, de contar con un consentimiento escrito, libre, voluntario, consciente e informado, en el cual, conste de manera indubitable la autorización del paciente para que sus datos sean utilizados y trasladados a otras personas, ya sean naturales o jurídicas.

Cabe añadir que, se puede prescindir el consentimiento de los pacientes en supuestos puntuales como son: (i) Cuando sean necesarios en circunstancia de riesgo; (ii) Para la prevención, diagnóstico y tratamiento médico o quirúrgico del titular de dichos DPS, siempre que dicho tratamiento sea realizado en los establecimientos de salud o por profesionales de salud, respetando el secreto profesional, con lo que, queda siempre una obligación de reserva para el profesional que recibe esta información.

ZEGARRA AGUILAR
abogados

Cabe aclarar que, los DPS no son los que se utilizan para fines estadísticos, sino que, estos pasan por un proceso de anonimato para que al final se conviertan en Información en Salud (IS) que servirá para que el Ministerio de Salud cuente con material para elaborar los datos estadísticos correspondientes, para aplicar las políticas de Estado necesarias, como por ejemplo, el número de contagiados por la Covid-19.

Para finalizar, los datos personales merecen tutela y protección, en mérito que son parte incluso dentro de nuestra intimidad, asimismo, los Datos Personales en Salud, son de carácter sensible, por lo que, para que los establecimientos los utilicen, deberán de tener un consentimiento otorgado por el titular, caso contrario se vulnerarán derechos de naturaleza constitucional, pudiendo desencadenar en un procedimiento sancionador acompañado de multas de hasta 100 UITs.

PROTECCIÓN DE DATOS PERSONALES EN LAS EMPRESAS

IMPORTANCIA DE LA IMPLEMENTACIÓN DE LOS SISTEMAS DE PROTECCIÓN DE DATOS PERSONALES

"De esta manera, las diferentes áreas de las empresas podrán determinar si los sistemas de información, las tecnologías, las políticas, las iniciativas y los proyectos de la organización protegen adecuadamente los datos personales de los intervinientes en cada uno de sus procesos".

El servicio de "Implementación del Sistema de Protección de Datos Personales" está destinado al análisis del cumplimiento de los estándares de la normativa nacional vigente en materia de privacidad de datos a partir de tres documentos normativos de trascendental importancia: i) la Ley N° 29733 – Ley de Protección de Datos Personales; ii) el Decreto Supremo N° 003- 2013-JUS – Reglamento de la Ley de Datos Personales; y iii) la Directiva de Seguridad de la Información, aprobada por la Autoridad Nacional de Datos Personales.

Renato Lozada Herrera
rlozada@zegarralaw.com

ZEGARRA AGUILAR
abogados

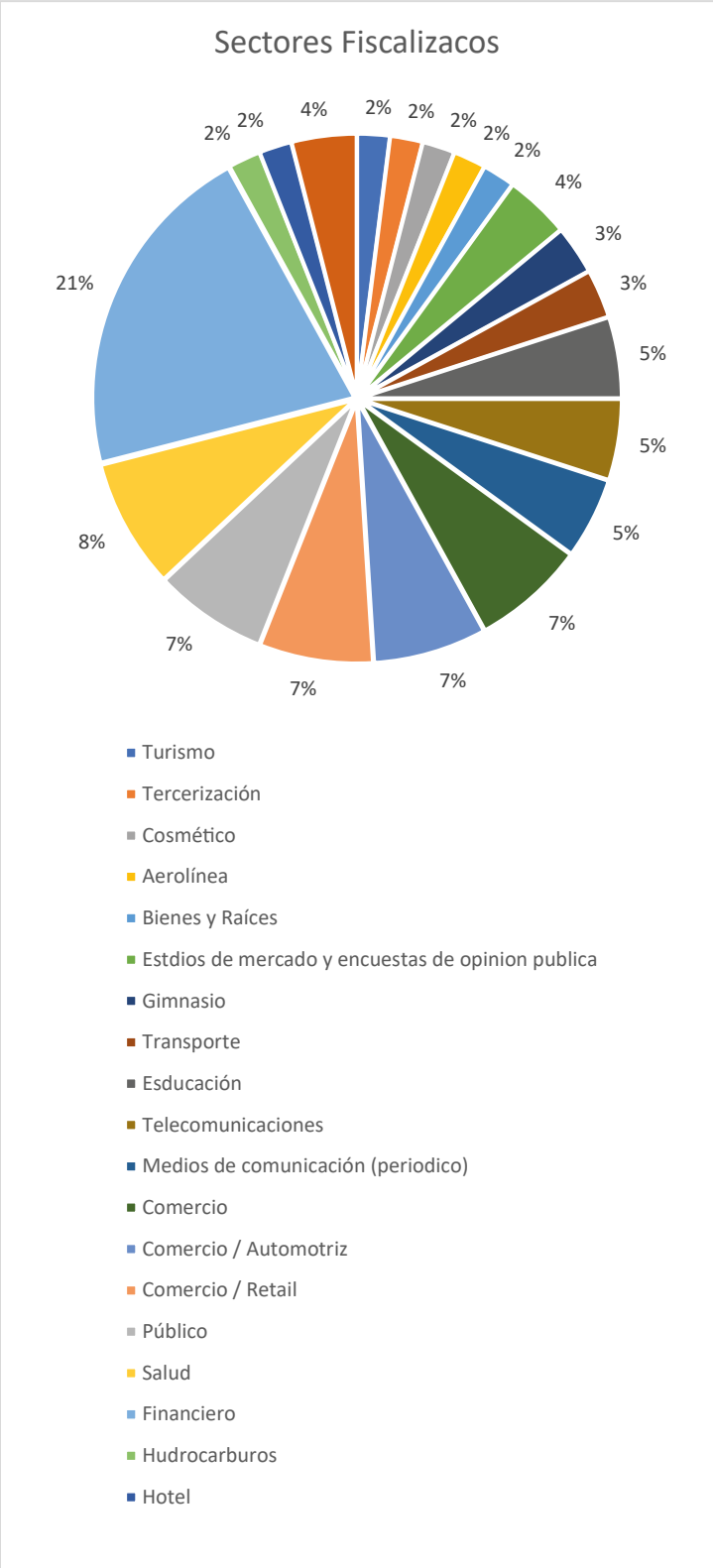
Según el art. 2.4 de la Ley N° 29733, califican como datos personales, toda aquella información sobre una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados; por lo tanto, a efectos del presente artículo al referirnos a los datos personales, haremos énfasis en la definición antes citada.

A partir de la adecuada implementación de la normativa antes citada, cada empresa podrá medir en el marco de sus actividades los impactos y riesgos propios del tratamiento de los datos personales de sus clientes, trabajadores, visitantes, proveedores, entre otros. De esta manera, las diferentes áreas de las empresas podrán determinar si los sistemas de información, las tecnologías, las políticas, las iniciativas y los proyectos de la organización protegen adecuadamente los datos personales de los intervinientes en cada uno de sus procesos.

Bajo tales consideraciones, las principales obligaciones que se desprenden de la legislación nacional exhortan a las empresas a contar con: i) capacitaciones constantes que permitan a los responsable del manejo de cualquier dato personal, comprender los alcances de sus responsabilidades; ii) administrar e identificar adecuadamente una matriz de riesgos que determine de forma integral aquellas falencias y las potenciales sanciones que de dicho incumplimiento se desprende; iii) incluir cláusulas de protección de datos personales, en sus contratos comerciales, laborales y cualquier otro documento de carácter legal mediante el cual se dé consentimiento o tenga como finalidad el tratamiento de datos personales; iv) gestionar ante la Autoridad de Protección de datos personales, institución adscrita al Ministerio de Justicia y Derechos Humanos, la inscripción de todas aquellos bancos de datos que cada empresa maneje en el ejercicio de sus labores.

De esta manera, aquellas empresas que implementen adecuadamente el un Sistema de Protección de Datos Personales, cumplir cabalmente con el respeto de los derechos de todas las personas que intervengan sus relaciones cotidianas, así como evitar la imposición de sanciones que repercutan directamente en los objetivos de cada institución.

DATOS SOBRE LA MATERIA EN LOS ÚLTIMOS AÑOS



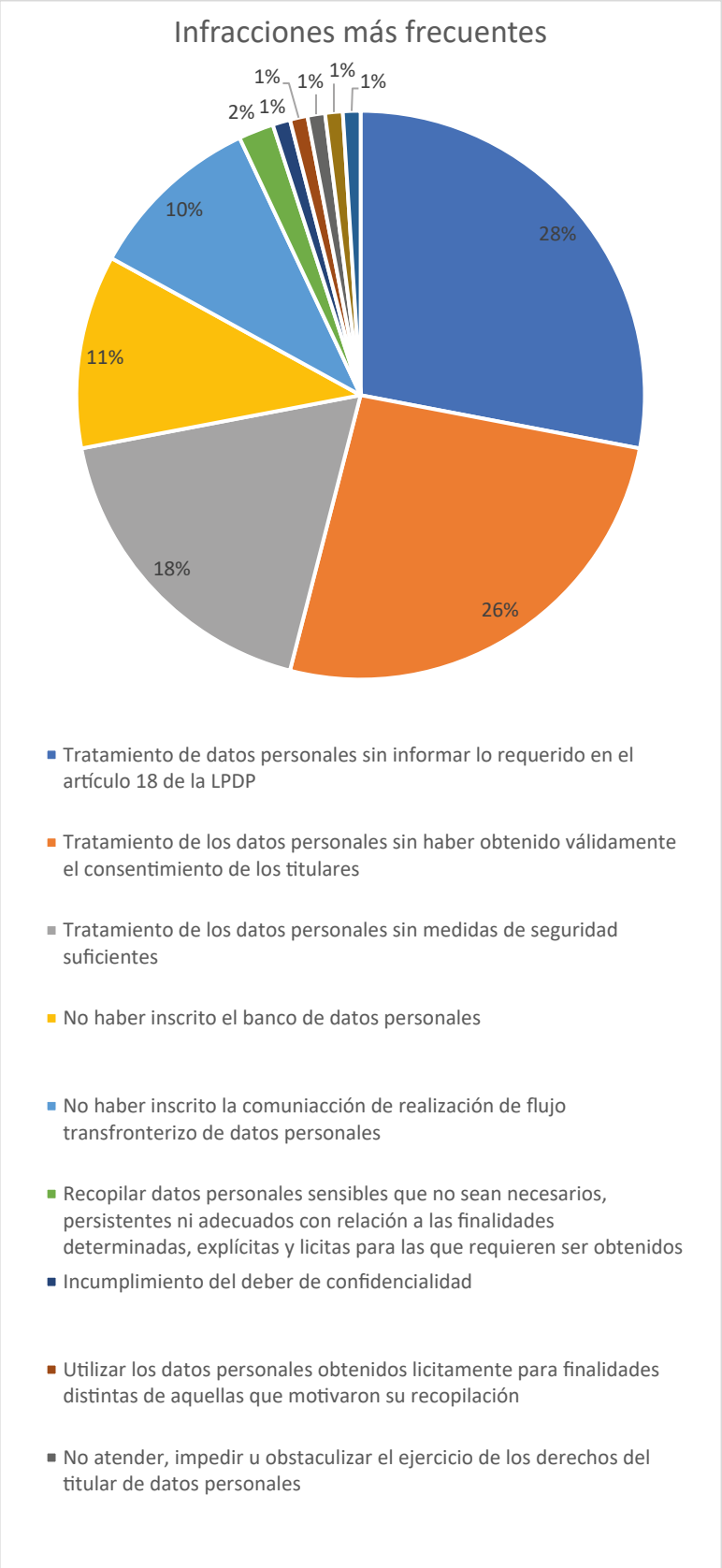
zegarra & schipper
abogados consultores

Recientemente Zegarra & Schipper (ZYS Abogados), firma entendida en la materia, publicó las conclusiones de una investigación que realizó sobre la Actividad de Fiscalización y Ejercicio de la Potestad Sancionadora de la ANPDP, la Autoridad Nacional de Protección de Datos Personales, en el periodo 2021. Al respecto encontramos datos importantes que nos gustaría compartir en la presente publicación.

En el periodo del año 2021, la actividad fiscalizadora y sancionadora de la Autoridad Nacional de Protección de Datos Personales, fue considerable. Se lograron identificar ciento setenta y dos (172) visitas de fiscalización, entre visitas presenciales y remotas ; y trescientas treinta y cinco (335) fiscalizaciones a entidades. De las referidas acciones, se derivó el inicio de ciento treinta y dos (132) procedimientos administrativos sancionadores.

- Dentro de estos procedimientos de fiscalización y sanción son determinadas entidades las cuales son materia de fiscalización de forma más incisiva y recurrente, pudiendo ser entidades financieras, entidades de

Fuente: Estudio Zegarra & Schipper Abogados.



salud, entidades de comercio, entidades de giro automotriz hasta entidades del sector público. Esta información se aprecia en el siguiente gráfico, donde se detallan todos los sectores fiscalizados y que fueron sancionados durante el periodo señalado:

- Por lo tanto, hay que tener en cuenta que el sector con mayor porcentaje de fiscalización y sanción fue el sector financiero con un 21%, seguido del sector salud con un 8%. Estos datos sacan a relucir la importancia que le da la Autoridad a la protección de datos personales en las relaciones de carácter financiero y la recurrente falencia en sus obligaciones sobre la materia por parte de las entidades que se desempeñan en la mencionada área empresarial.

- Así también, son múltiples las posibles infracciones a cometerse en el ámbito de la protección de datos personales, siendo las más recurrentes las siguientes:

- El incumplimiento de la obligación referida al Tratamiento de Datos sin Medidas de Seguridad ha sido una de las infracciones más frecuentes que han dado inicio a procedimientos administrativos sancionadores. Durante el periodo señalado, la multa mínima impuesta por la DPDP por esta infracción fue de 0.5 UIT; y, la máxima, de

Fuente: Estudio Zegarra & Schipper Abogados.

2.82 UIT. El promedio de las multas impuestas a las entidades fiscalizadas por incumplir la obligación de cumplir con las medidas de seguridad en el tratamiento de datos personales es 2 UIT aproximadamente.

- Como se desprende del gráfico previo, podemos ver que las infracciones con mayor porcentaje de frecuencia de comisión se refieren al Tratamiento de datos personales sin informar lo requerido en el Artículo 18 de la Ley sobre la materia, refiriéndose directamente a la obligación de informar al titular de los datos personales sobre la transferencia de datos a una person, sea natural o jurídica, distinta a él.

- Contar con el consentimiento de los titulares de los datos constituye una de las obligaciones más observadas al momento de realizar fiscalizaciones, puesto que es el primer paso que debe considerar toda entidad para proceder a tratar este tipo de información. Sin un consentimiento libre, expreso e informado nos encontraríamos cometiendo la segunda más frecuente infracción, dado a que el límite para el tratamiento de datos personales es la autorización del titular del dato; es decir, la recopilación y transferencia de datos sin consentimiento es ilegal.

ZEGARRA AGUILAR

abogados

legal@zegarralaw.com

www.zegarralaw.com