Industria y Comercio
SUPERINTENDENCIA

GUÍA SOBRE EL TRATAMIENTO DE DATOS PERSONALES EN LA PROPIEDAD HORIZONTAL

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO
DELEGATURA PARA LA PROTECCIÓN DE DATOS PERSONALES
2020

El futuro es de todos
Gobierno de Colombia

Industria y Comercio
SUPERINTENDENCIA

GUÍA SOBRE EL TRATAMIENTO DE DATOS PERSONALES
EN LA PROPIEDAD HORIZONTAL

DELEGATURA PARA LA PROTECCIÓN DE DATOS PERSONALES

Industria y Comercio
SUPERINTENDENCIA

ANDRÉS BARRETO GONZÁLEZ
Superintendente de Industria y Comercio

NELSON REMOLINA ANGARITA
Superintendente Delegado para la Protección de Datos Personales

CATERINE GÓMEZ CARDONA
CARLOS ENRIQUE SALAZAR
LUIS ALBERTO MONTEZUMA
AÍDA LUCÍA HURTADO BEJARANO
Autores primera edición

ANGÉLICA ASPRILLA
Jefe de la Oficina de Servicios al Consumidor y Apoyo empresarial OSCAE

ALEJANDRO ARTEAGA
Coordinador de Comunicaciones

DIANA MARIÑO
Corrección de estilo

YENNY PAOLA CASTIBLANCO GARCÍA
Diagramación

ANGÉLICA MARÍA ACUÑA PORRAS
Secretaría General

BOGOTÁ D.C. - COLOMBIA 2020

CONTENIDO

INTRODUCCIÓN

Los edificios o conjuntos de uso residencial, comercial o mixto son personas jurídicas sometidas al régimen de propiedad horizontal[1]. Cuando dichas personas jurídicas recolectan o usan Datos Personales de los visitantes, empleados, residentes o cualquier persona (Titular del dato), están realizando Tratamiento de Datos Personales que debe efectuarse conforme a la Constitución y la Ley. Como tales, son Responsables de Tratamiento y deben cumplir todos los deberes legales. Es factible que para ciertas actividades acudan a terceros como las empresas de seguridad privada, las cuales actúan como Encargados del Tratamiento y también deben acatar los mandatos legales sobre protección de Datos Personales.

Conforme con el artículo 15 superior, las personas tienen el derecho a conocer, actualizar y rectificar toda la información que se haya recogido sobre ellas en bases de datos o archivos de entidades públicas y privadas. Además, señala que "en la recolección, *tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución*". Esta disposición fue desarrollada por la Ley Estatutaria 1581 de 2012, la cual define como *"Tratamiento"* a *"cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión"*.

Según el artículo 50 de la Ley 675 de 2001 "*la representación legal de la persona jurídica y la administración del edificio o conjunto corresponderán a un administrador (…). Los administradores responderán por los perjuicios que por dolo, culpa leve o grave, ocasionen a la persona jurídica, a los propietarios o a terceros. Se presumirá la culpa leve del administrador en los casos de incumplimiento o extralimitación de sus funciones, violación de la ley o del reglamento de propiedad horizontal.*" En lo no previsto en dicha ley respecto de los administradores se aplica la Ley 222 de 1995 la cual requiere que ellos no sólo obren "*de buena fe, con lealtad y con la diligencia de un buen hombre de negocios*", sino que en el ejercicio de sus funciones deben *"velar por el estricto cumplimiento de las disposiciones legales o estatutarias*".

Dado lo anterior, se expide la siguiente guía cuyos objetivos y precisiones señalamos a continuación.

1 Ley 675 de 2001, artículos 4 y 32

OBJETIVOS, PRECISIONES Y COMPLEMENTARIEDAD CON OTRAS GUÍAS Y CARTILLAS DE ESTA ENTIDAD

Esta guía tiene como propósito presentar algunas sugerencias a quienes recolectan o tratan Datos Personales en los edificios o conjuntos de uso residencial, comercial o mixto sometidos al régimen de propiedad horizontal, con miras a orientarlos para que cumplan correctamente la regulación sobre el Tratamiento de los mismos y, de esta manera, respeten los derechos de las personas.

Estas recomendaciones tienen un enfoque preventivo con miras a que los edificios o conjuntos directamente (Responsables del Tratamiento) o, a través de terceros (Encargados del Tratamiento), eviten vulnerar los derechos de cualquier persona (Titular del Dato).

Este documento no es un concepto legal ni constituye asesoría jurídica. Tampoco pretende ser un listado exhaustivo de recomendaciones específicas sobre todos los temas que involucra la protección de Datos Personales en el Régimen de Propiedad Horizontal, pues ello es un asunto interno de cada copropiedad.

Las orientaciones contenidas en este texto solo comprenden algunos de los temas más relevantes sobre la protección de Datos Personales en el Régimen de Propiedad Horizontal. Por consiguiente, el lector debe tener claro que este documento no incluye todos los deberes legales sobre la materia y que la omisión de algunos de ellos en esta guía no lo exime de cumplir todo lo que exige la ley.

Finalmente, esta entidad ha publicado los siguientes documentos que sugerimos consultar porque son complementarios a esta guía:

1. Cuestionario de diagnóstico para el cumplimiento de la Ley 1581 de 2012 en las mipymes;
2. Cartilla de formatos modelos para el cumplimiento de obligaciones establecidas en la Ley 1581 de 2012 y sus decretos reglamentarios;
3. Guía sobre protección de Datos Personales en sistemas de videovigilancia, y
4. Guía para la implementación del Principio de Responsabilidad Demostrada *(accountability)*.

Esta guía contiene recomendaciones con enfoque preventivo para evitar vulnerar los derechos de las personas, no es un concepto legal ni constituye asesoría jurídica

RECOMENDACIONES

Efectúe un diagnóstico de cumplimiento de la Ley 1581 de 2012

Si el edificio o conjunto -*Responsable del Tratamiento*- ha implementado algunas medidas para cumplir la regulación de Datos Personales, recomendamos que realice una evaluación interna de lo hecho para establecer si es correcto o suficiente.

Para dicho efecto, sugerimos que utilice la siguiente cartilla publicada en diciembre de 2018 por la Delegatura para la Protección de Datos de la Superintendencia de Industria y Comercio: *"Cuestionario de diagnóstico para el cumplimiento de la Ley 1581 de 2012 en las mipymes"*[2].

Mediante el uso de los listados de comprobación podrá conocer el nivel de avance de su organización en la implementación de la regulación sobre Datos Personales y el Principio de Responsabilidad Demostrada. Allí se realizan preguntas sobre los siguientes aspectos:

- Principios para el Tratamiento de Datos Personales
- Tratamiento de datos sensibles y de menores de edad
- Derecho de los Titulares de los Datos Personales
- Autorización para el Tratamiento de Datos Personales
- Información mínima a los Titulares
- Suministro de información personal
- Atención de consultas y reclamos de los Titulares
- Política de Tratamiento de Datos Personales
- Aviso de privacidad
- Reporte de violaciones a los códigos de seguridad
- Gestión de Encargados del Tratamiento
- Transferencia y transmisión internacional de Datos Personales
- Responsabilidad Demostrada
- Registro Nacional de Base de Datos

2 El texto lo puede consultar en: https://www.sic.gov.co/sites/default/files/files/Nuestra_Entidad/Publicaciones/Cuestionario_de_diagnostico_para_el_cumplimiento_de_la_Ley_1581_de_2012_en_las_Mipymes.pdf

USE LOS FORMATOS MODELO DE LA SIC PARA EL CUMPLIMIENTO DE LA LEY 1581 DE 2012

Al implementar la ley es importante utilizar algunos documentos para dejar evidencia del cumplimiento de la misma. A título de referencia, usted puede usar los modelos publicados en 2017 por esta entidad en la *"Cartilla de formatos modelos para el cumplimiento de obligaciones establecidas en la Ley 1581 de 2012 y sus decretos reglamentarios"*[3], con miras a que sirvan como referencia y sean ajustados a las particularidades de cada caso.

En la cartilla se da respuesta a algunas inquietudes como: ¿qué es una Autorización para el Tratamiento de Datos Personales?, ¿en qué casos no es necesaria la Autorización? y ¿cómo obtener la Autorización?. Adicionalmente, se hace referencia a la Autorización para el Tratamiento de Datos Personales sensibles, la finalidad de la recolección de Datos Personales, el deber de informar al Titular, los requisitos especiales para el Tratamiento de datos de menores de edad, el manual de políticas y procedimientos internos, la Política de Tratamiento de Datos Personales y los avisos de privacidad.

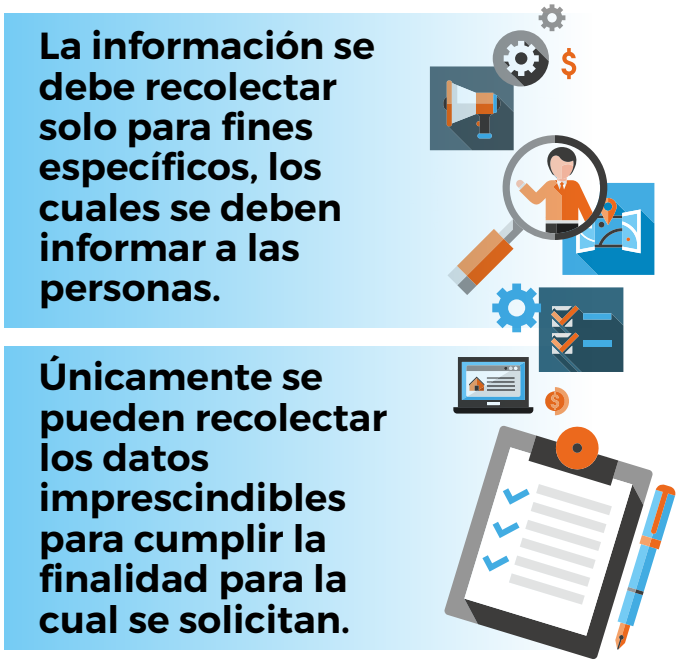
También encontrará un glosario sobre el tema, algunos ejemplos de finalidades para incluir en las autorizaciones y los siguientes documentos:

- Modelo de Autorización para el Tratamiento de Datos Personales
- Modelo de Política de Tratamiento de Información
- Modelo de aviso de privacidad

Dado lo anterior, en esta guía no desarrollaremos de nuevo los temas incluidos en las dos cartillas, las cuales son complementarias al presente texto.

RECOLECTE DATOS DE FORMA LÍCITA Y PARA FINES LEGÍTIMOS, UTILIZANDO MEDIOS QUE DEJEN EVIDENCIA DEL CUMPLIMIENTO DE LA LEY

La recolección, uso, circulación y el Tratamiento de los Datos Personales solo pueden realizarse cuando exista la Autorización previa, expresa e informada del Titular, tal y como lo establece el principio de libertad definido en el literal c) del artículo 4 de la Ley 1581 de 2012[4]. Recuerde que está prohibido *"utilizar medios engañosos o fraudulentos para recolectar y realizar Tratamiento de datos personales"*.

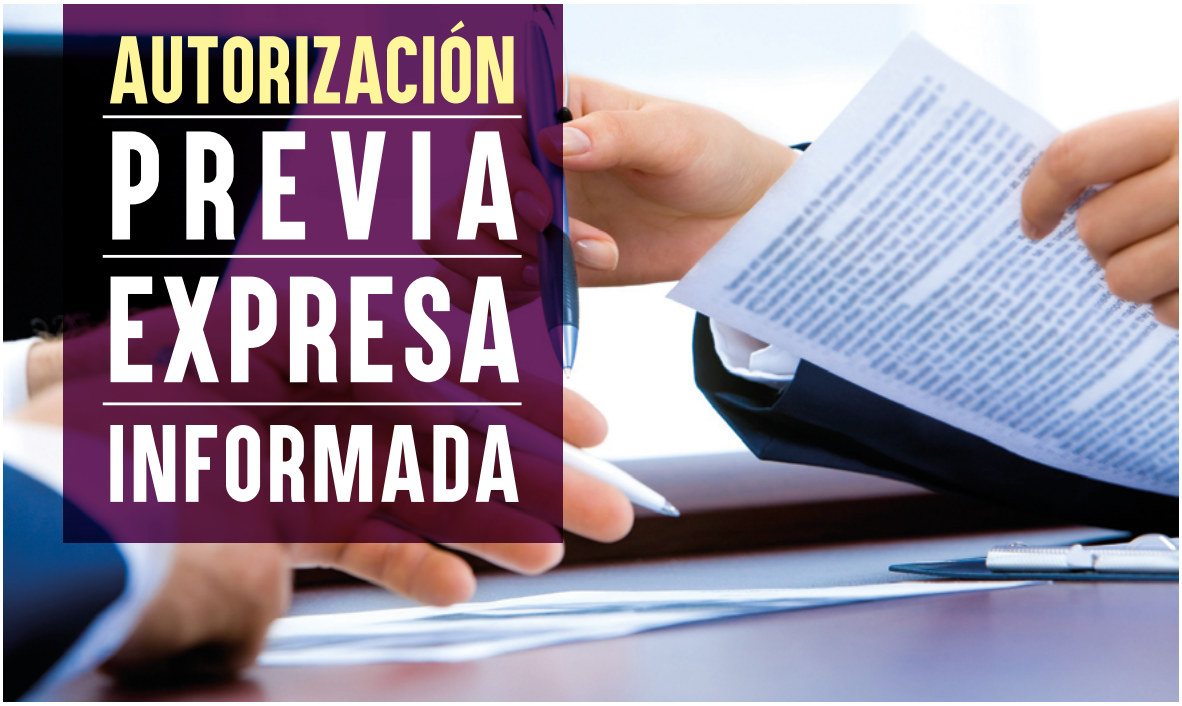


Es imperativo tener presente que la información no se puede recolectar para hacer cualquier cosa, sino solo para finalidades específicas que se deben informar a las personas. Tampoco se puede recolectar cualquier Dato Personal, sino solo aquellos que sean imprescindibles para cumplir la finalidad para la cual son colectados. En este sentido, la regulación ordena que *"la recolección de datos deberá limitarse a aquellos datos personales que son pertinentes y adecuados para la finalidad para la cual son recolectados o requeridos"*[5].

3 El texto lo puede consultar en: https://www.sic.gov.co/sites/default/files/files/Nuestra_Entidad/Publicaciones/Cartilla_formatos_datos_Personales_nov22.pdf

4 „c) Principio de libertad: El Tratamiento sólo puede ejercerse con el consentimiento, previo, expreso e informado del Titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento".

5 Cfr. Artículo 4 del Decreto 1377 de 2013



A su vez, el artículo 9 de la Ley 1581 de 2012 dispone que *"sin perjuicio de las excepciones previstas en la ley*[6]*, en el Tratamiento se requiere la autorización previa e informada del Titular, la cual deberá ser obtenida por cualquier medio que pueda ser objeto de consulta posterior"* y, en este mismo sentido, el artículo 17 de dicha norma consagró como deber de los Responsables del Tratamiento el de *"b) solicitar y conservar, en las condiciones previstas en la presente ley, copia de la respectiva autorización otorgada por el Titular".* El artículo 4 del Decreto 1377 de 2013[7] reitera, entre otras, lo siguiente: *"Salvo en los casos expresamente previstos en la ley, no se podrán recolectar datos personales sin autorización del Titular"* y el artículo 5 del mismo decreto establece que *"El Responsable del Tratamiento deberá adoptar procedimientos para solicitar, a más tardar en el momento de la recolección de sus datos, la autorización del Titular para el Tratamiento de los mismos e informarle los datos personales que serán recolectados así como todas las finalidades específicas del Tratamiento para las cuales se obtiene el consentimiento". (Destacamos)*

El artículo 12 de la Ley 1581 de 2012, por su parte, instituyó que el Responsable del Tratamiento al momento de solicitar la Autorización del Titular

> *"(…) deberá informarle de manera clara y expresa lo siguiente:*
>
> **a.** *El Tratamiento al cual serán sometidos sus datos personales y la finalidad del mismo;*
>
> **b.** *El carácter facultativo de la respuesta a las preguntas que le sean hechas, cuando éstas versen sobre datos sensibles o sobre los datos de las niñas, niños y adolescentes;*
>
> **c.** *Los derechos que le asisten como Titular;*
>
> **d.** *La identificación, dirección física o electrónica y teléfono del Responsable del Tratamiento (…)".*

6 El artículo 10 de la Ley 1581 de 2012 ordena lo siguiente: "ARTÍCULO 10. CASOS EN QUE NO ES NECESARIA LA AUTORIZACIÓN. La autorización del Titular no será necesaria cuando se trate de: a) Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial; b) Datos de naturaleza pública; c) Casos de urgencia médica o sanitaria; d) Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos; e) Datos relacionados con el Registro Civil de las Personas."

7 Incorporado en el Decreto 1074 de 2015.

En este orden de ideas, es pertinente indicar que el artículo 2.2.2.25.2.4 del Decreto 1074 de 2015[8] (Decreto 1377 de 2013, art. 7), estableció los diversos modos de obtener la Autorización para efectos de dar cumplimiento a lo dispuesto en el artículo 9 de la Ley 1581 de 2012, a saber:

> *"Modo de obtener la autorización. Para efectos de dar cumplimiento a lo dispuesto en el artículo 9 de la Ley 1581 de 2012, los Responsables del Tratamiento de datos personales establecerán mecanismos para obtener la autorización de los titulares o de quien se encuentre legitimado de conformidad con lo establecido en el artículo 2.2.2.25.4.1., del presente Decreto, que garanticen su consulta. Estos mecanismos podrán ser predeterminados a través de medios técnicos que faciliten al Titular su manifestación automatizada.*
>
> *Se entenderá que la autorización cumple con estos requisitos cuando se manifieste (i) por escrito, (ii) de forma oral o (iii) mediante conductas inequívocas del titular que permitan concluir de forma razonable que otorgó la autorización. En ningún caso el silencio podrá asimilarse a una conducta inequívoca".*
>
> De lo anterior, se entiende que el Titular ha dado su Autorización para el Tratamiento de sus Datos Personales cuando: (i) sea por escrito; (ii) sea verbal o (iii) mediante conductas inequívocas, es decir, aquellas que no admiten duda o equivocación del titular que permitan concluir de forma razonable que otorgó la Autorización. En otras palabras, la Autorización también se podrá obtener a partir de conductas evidentes, claras e incontrovertibles del Titular que no admitan duda o equivocación sobre su voluntad de dar su consentimiento para que sus datos sean tratados.

En todo caso y al margen del modo cómo se obtenga la Autorización, ésta no sólo debe ser previa, expresa e informada, sino que el Responsable del Tratamiento tiene la carga probatoria de acreditar evidencia de la Autorización y de que informó lo que ordena el artículo 12 de la Ley 1581 de 2012.

TENGA EN CUENTA LAS PAUTAS ESPECIALES PARA RECOLECTAR HUELLAS DACTILARES, DATOS RELATIVOS A LA SALUD, TOMAR FOTOS O EFECTUAR VIDEOGRABACIONES

Las fotos, las videograbaciones, las huellas dactilares y la información relativa al estado de salud de las personas son ejemplos de datos sensibles. Si recolecta, usa o trata este tipo de información debe cumplir con lo que ordena el artículo 6 del decreto 1377 de 2013, a saber:

8 "Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo".

"En el Tratamiento de datos personales sensibles, cuando dicho Tratamiento sea posible conforme a lo establecido en el artículo 6° de la Ley 1581 de 2012, deberán cumplirse las siguientes obligaciones:

1. Informar al titular que por tratarse de datos sensibles no está obligado a autorizar su Tratamiento.

2. Informar al titular de forma explícita y previa, además de los requisitos generales de la autorización para la recolección de cualquier tipo de dato personal, cuáles de los datos que serán objeto de Tratamiento son sensibles y la finalidad del Tratamiento, así como obtener su consentimiento expreso.

Ninguna actividad podrá condicionarse a que el Titular suministre datos personales sensibles."

El Tratamiento de datos sensibles debe estar rodeado de especial cuidado y diligencia en su recolección, uso, seguridad o cualquier otra actividad que se realice con los mismos. En efecto, la Corte Constitucional exige responsabilidad reforzada por parte de los Responsables y Encargados: "*como se trata de casos exceptuados y que, por tanto, pueden generar altos riesgos en términos de vulneración del habeas data, la intimidad e incluso la dignidad de los titulares de los datos, los agentes que realizan en estos casos el tratamiento tienen una responsabilidad reforzada que se traduce en una exigencia mayor en términos de cumplimiento de los principios del artículo 4 y los deberes del título VI*"[9] Por ende, los datos sensibles deben ser objeto de mayores medidas de seguridad, confidencialidad, acceso, circulación y uso restringido.

Los datos sensibles deben ser objeto de mayores medidas de seguridad, confidencialidad, acceso, circulación y uso restringido.

CUMPLA LOS REQUISITOS PARA PODER RECOLECTAR Y TRATAR DATOS PERSONALES DE NIÑAS, NIÑOS Y ADOLESCENTES (NNA)

En el Tratamiento de datos se asegurará el respeto a los derechos prevalentes de los niños, niñas y adolescentes.

El artículo 2 de la Convención de las Naciones Unidas sobre los derechos del niño ordena a los Estados respetar y garantizar los derechos de los niños *"sin distinción alguna, independientemente de la raza, el color, el sexo, el idioma, la religión, la opinión política o de otra índole, el origen nacional, étnico o social, la posición económica, los impedimentos físicos, el nacimiento o cualquier otra condición del niño, de sus padres o de sus representantes legales".*

Los niños, niñas y adolescentes (NNA) gozan de una especial protección y son Titulares de los derechos constitucionales y legales como la Protección de sus Datos Personales. Sus derechos prevalecen sobre los demás tal y como lo ordena el artículo 44 de la Constitución.

9 Cfr. Corte Constitucional, sentencia C-748 de 2011, numeral 2.8.4

El artículo 7 de la Ley 1581 de 2012 ordena que *"en el Tratamiento se asegurará el respeto a los derechos prevalentes de los niños, niñas y adolescentes"*. Por otra parte, el artículo 11 del Decreto 1377 de 2013 establece que la autorización del Tratamiento de datos de menores de edad debe ser otorgada por el representante legal del NNA y precisa que "*el Tratamiento de datos personales de niños, niñas y adolescentes está prohibido, excepto cuando se trate de datos de naturaleza pública, de conformidad con lo establecido en el artículo 7 de la Ley 1581 de 2012 y cuando dicho Tratamiento cumpla con los siguientes parámetros y requisitos:*

1. Que responda y respete el interés superior de los niños, niñas y adolescentes.

2. Que se asegure el respeto de sus derechos fundamentales.

La autorización del Tratamiento de los datos de los NNA debe ser otorgada por su representante legal.

Exija el respeto de la regulación de protección de datos y de su Política de Tratamiento de Datos Personales a los terceros que contrata (Encargados del Tratamiento)

Si el edificio o conjunto -*Responsable del Tratamiento*- *contrata a otra empresa o a un tercero -Encargado del Tratamiento*- para realizar actividades de vigilancia y seguridad u otra actividad, exíjale el cumplimiento de su Política de Tratamiento de Datos Personales y los deberes legales que esto conlleva. Con todo, no solo es obligatorio el desarrollo de sus políticas para el Tratamiento de los Datos Personales, también debe velar porque los Encargados del Tratamiento den cabal cumplimiento a las mismas[10].

Recuerde que esos terceros (empresas de seguridad) obran en nombre suyo y que usted responde frente a los Titulares de los datos y las autoridades por los errores o negligencia de ellos. Además, la ley les impone a estos la obligación de cumplir una serie de deberes[11].

Se recomienda que en los contratos de prestación de servicios pacte con esos terceros las obligaciones especiales y los deberes que

10. Cfr. Artículo 13 del Decreto 1377 de 2013.
11. Los deberes de los Encargados están previstos en el artículo 18 de la Ley 1581 de 2012.

deben cumplir sobre el Tratamiento de Datos Personales. Deje claro qué pueden hacer y qué no. Es fundamental que con las empresas de vigilancia, por ejemplo, se pacten cláusulas contractuales en las que se obliguen a:

- Cumplir las políticas de Tratamiento de información de los conjuntos o edificios
- Garantizar seguridad y confidencialidad de los Datos Personales
- No usar los Datos Personales para fines diferentes a los autorizados
- No apropiarse de los Datos Personales ni quedarse con ellos (copias de planillas, formularios, grabaciones, archivos electrónicos) luego de culminado el contrato de prestación de servicios
- Devolver al conjunto o edificio todos los datos que recolectó durante la prestación de sus servicios.

Adopte medidas para garantizar los principios sobre Tratamiento de Datos Personales en los edificios o conjuntos

Tenga en cuenta que en la recolección, uso y Tratamiento de datos se debe aplicar de manera armónica e integral los siguientes principios:

a. Principio de legalidad en materia de Tratamiento de datos

b. Principio de finalidad

c. Principio de libertad

d. Principio de veracidad o calidad

e. Principio de transparencia

f. Principio de acceso y circulación restringida

g. Principio de seguridad

h. Principio de confidencialidad

El alcance de cada principio está determinado en el artículo 4 de la Ley 1581 de 2012 y sus normas reglamentarias, razón por la cual nos remitimos al mismo para no transcribirlos en este espacio.

RESPETE LOS DERECHOS DE LOS TITULARES DE LOS DATOS E IMPLEMENTE MECANISMOS EFECTIVOS PARA SU EJERCICIO

Los edificios y conjuntos deben garantizar los siguientes derechos[12] de los Titulares de los datos:

a. Conocer, actualizar y rectificar sus Datos Personales frente a los Responsables del Tratamiento o Encargados del Tratamiento.

b. Solicitar prueba de la Autorización otorgada al Responsable del Tratamiento.

c. Ser informado por el Responsable del Tratamiento o el Encargado del Tratamiento, previa solicitud, respecto del uso que les ha dado a sus Datos Personales.

d. Presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a lo dispuesto en la Ley 1581 de 2012 y las demás normas que la modifiquen, adicionen o complementen.

e. Revocar la autorización y/o solicitar la supresión del dato cuando en el Tratamiento no se respeten los principios, derechos y garantías constitucionales y legales.

f. Acceder en forma gratuita a sus Datos Personales que fueron objeto de Tratamiento.

12 Los derechos están previstos en el artículo 8 de la Ley 1581 de 2012.

El alcance de cada derecho está delineado en la Ley 1581 de 2012 y sus decretos reglamentarios, razón por la cual se hace una remisión expresa a dichos textos legales. En todo caso, recuerde que:

- *"los procedimientos de acceso, actualización, supresión y rectificación de datos personales y de revocatoria de la autorización deben darse a conocer o ser fácilmente accesibles a los Titulares de la información e incluirse en la política de tratamiento de la información"*[13].

- *"Los responsables y encargados del tratamiento deben establecer mecanismos sencillos y ágiles que se encuentren permanentemente disponibles a los Titulares con el fin de que estos puedan acceder a los datos personales que estén bajo el control de aquellos y ejercer sus derechos sobre los mismos"*[14].

- *"Todo Responsable y Encargado deberá designar a una persona o área que asuma la función de protección de datos personales, que dará trámite a las solicitudes de los Titulares, para el ejercicio de los derechos a que se refiere la Ley 1581 de 2012 y el presente decreto"* [15].

Ubique avisos de privacidad en sitios fácilmente visibles

Se recomienda que en todas las porterías de los conjuntos o edificios se utilicen avisos de privacidad para informar de manera clara y sencilla todo lo que ordena el artículo 15 del decreto 1377 de 2013.

Utilice avisos para informar a las personas que están siendo videovigiladas

Si utiliza sistemas de videovigilancia ubique avisos en sitios fácilmente visibles a todas las personas para que sepan que están siendo grabadas e infórmeles que su información será tratada para determinados fines y observando la Ley 1581 de 2012.

ESTOS AVISOS:

- Deben ser fácilmente visibles, legibles y comprensibles

- Deben estar ubicados en porterías, ascensores, garajes y todos los demás sitios en donde se utilizarán cámaras o mecanismos de vigilancia

El siguiente puede ser el texto de los avisos para utilizar en las instalaciones de los edificios y conjuntos:

Recuerde que el objetivo de estos avisos es que las personas se enteren rápida y fácilmente que están siendo videovigiladas cuando ingresan a cualquiera de las instalaciones de los edificios y conjuntos.

En todos los demás aspectos, tenga presente lo que se establece en la guía de 2016 "Guía de protección de datos personales en sistemas de videovigilancia"[16] de esta entidad.

Finalmente, tenga presente que la Corte Constitucional, mediante sentencia C-094 de 2020 resolvió lo siguiente: *"Declarar la EXEQUIBILIDAD CONDICIONADA del artículo 237 de la Ley 1801 de 2016, por el cargo analizado, en el entendido de que el manejo y tratamiento de información, datos e imágenes captados y/o almacenados a través de sistemas de*

13 Cfr. el artículo 18 del Decreto 1377 de 2013.
14 Cfr. el artículo 22 del Decreto 1377 de 2013.
15 Cfr. el artículo 23 del Decreto 1377 de 2013.
16 El texto lo puede consultar en: https://www.sic.gov.co/sites/default/files/files/Nuestra_Entidad/Guia_Vigilancia_sept16_2016.pdf

video o medios tecnológicos que estén ubicados o instalados en el espacio público, en lugares abiertos al público, en zonas comunes o en lugares privados abiertos al público o que siendo privados trasciendan a lo público, deberá observar los principios de legalidad, finalidad, libertad, transparencia, acceso y circulación restringida, seguridad y confidencialidad y caducidad, en los términos del numeral 157 de esta providencia."[17]

Garantice la seguridad de los Datos Personales

Debe ser protegida toda la información que se recolecte mediante plantillas, formularios, videovigilancia, huelleros, reconocimiento facial, sistemas biométricos o por cualquier otro medio físico o electrónico.

Sin seguridad no habrá debido Tratamiento de los Datos Personales. Es fundamental adoptar medidas tecnológicas, humanas, administrativas, físicas, contractuales y de cualquier otra índole que eviten:

- Accesos indebidos o no autorizados a la información
- Manipulación de la información
- Destrucción de la información
- Usos indebidos o no autorización de la información
- Circular o suministrar la información a personas no autorizadas

Las medidas de seguridad deben ser apropiadas considerando varios factores como:

(i) los niveles de riesgo del Tratamiento para los derechos y libertades de los Titulares de los datos;

(ii) la naturaleza de los datos;

(iii) las posibles consecuencias que se derivarían de una vulneración para los Titulares y la magnitud del daño que se puede causar a ellos, al Responsable y a la sociedad en general;

(iv) el número de Titulares de los datos y la cantidad de información;

(v) el tamaño de la organización;

(vi) los recursos disponibles,

(vii) el estado de la técnica, y

(viii) el alcance, contexto y finalidades del Tratamiento de la información.

Todas las medidas de seguridad, deben ser objeto de revisión, evaluación y mejora permanente.

Todas las medidas de seguridad, deben ser revisadas, evaluadas y mejoradas permanentemente para que haya un debido Tratamiento de Datos Personales.

17 El texto lo puede consultar en: https://www.corteconstitucional.gov.co/relatoria/2020/C-094-20.htm

Elimine los Datos Personales tan pronto cumplan la finalidad para la cual fueron recolectados

La Corte Constitucional ha señalado que "*los datos deberán ser conservados en una forma que permita la identificación de los interesados durante un periodo no superior al necesario para los fines para los que fueron recogidos. Es decir, el periodo de conservación de los datos personales no debe exceder del necesario para alcanzar la necesidad con que se han registrado*"[18].

Teniendo en cuenta lo anterior, en el artículo 11[19] del decreto 1377 de 2013 se establece que los "*Responsables y Encargados del Tratamiento solo podrán recolectar, almacenar, usar o circular los datos personales durante el tiempo que sea razonable y necesario, de acuerdo con las finalidades que justificaron el tratamiento*". La idea es no almacenar y usar datos indefinidamente. En otros términos, si expiró el tiempo del Tratamiento autorizado por el Titular o ya se cumplió la finalidad del mismo y no existe una norma legal que disponga lo contrario, "*el Responsable y el Encargado deberán proceder a la supresión de los datos personales en su posesión*"[20].

El citado artículo menciona algunos factores que se deben considerar en cada caso concreto para establecer el tiempo de conservación de la información como, entre otros, "*las disposiciones aplicables a la materia de que se trate y a los aspectos administrativos, contables, fiscales, jurídicos e históricos de la información*"[21]. Adicionalmente, dice la norma que los datos "*deberán ser conservados cuando así se requiera para el cumplimiento de una obligación legal o contractual*" [22].

> Los Responsables y Encargados del Tratamiento de datos podrán almacenar la información solo durante el tiempo que sea razonable y necesario para las finalidades con las que se solicitó.

Los edificios y conjuntos pueden tratar los datos por el tiempo necesario siempre y cuando justifiquen dicho término o período razonablemente. Ahora bien, en consonancia con el Principio de Responsabilidad Demostrada, el artículo en comento ordena a los Responsables y Encargados "*documentar los procedimientos para el Tratamiento, conservación y supresión de los datos personales de conformidad con las disposiciones aplicables a la materia de que se trate, así como las instrucciones que al respecto imparta la Superintendencia de Industria y Comercio*".

18 Cfr. Corte Constitucional, sentencia C-748 de 2011, numeral 2.6.5.2.2
19 Denominado "Limitaciones temporales al Tratamiento de los datos personales".
20 Cfr. Artículo 11 del decreto 1377 de 2013.
21 Cfr. Artículo 11 del decreto 1377 de 2013.
22 Cfr. Artículo 11 del decreto 1377 de 2013.

GARANTICE LA CONFIDENCIALIDAD DE LA INFORMACIÓN

Las personas involucradas en el Tratamiento de Datos Personales deben mantener en reserva o secreto los Datos Personales que conocen con ocasión de su trabajo o gestión (personas que viven en un inmueble, datos de contacto, vehículos, visitantes, videograbaciones, trabajadores). No pueden hacer de conocimiento público los datos privados a menos que lo autorice el titular o la ley o exista orden judicial.

En efecto, de conformidad con el literal h) del artículo 4 de la Ley 1581 de 2012 "*todas las personas que intervengan en el tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la presente ley y en los términos de la misma*".

ES IMPORTANTE QUE LOS EDIFICIOS Y CONJUNTOS:

- Capaciten a su equipo humano (empleados, contratistas), al perteneciente a empresas de vigilancia privada o seguridad, a contadores y a todos los que tienen acceso a Datos Personales contenidos en planillas, grabaciones, formularios, etc., para que no suministren ni permitan acceso a esa información a terceros no autorizados por los Titulares de los datos o la ley.

CAPACITE A SU EQUIPO

Para que no suministren información ni permitan acceso a terceros no autorizados

IMPARTA INSTRUCCIONES

Para que no envíen comunicaciones electrónicas masivas que permitan a los destinatarios conocer información de otras personas

PACTE CLÁUSULAS DE CONFIDENCIALIDAD

Pacten cláusulas de confidencialidad en todos los contratos con sus empleados, contratistas, contadores, empresas de vigilancia o seguridad y terceros.

SOBRE EL ENVÍO DE MENSAJES

Capacite a sus empleados para que remitan mensajes únicamente a personas que hayan dado autorización previa, expresa e informada para enviarle comunicaciones a su dirección de correo electrónico.

- Pacten cláusulas de confidencialidad en todos los contratos con sus empleados, contratistas, contadores, empresas de vigilancia o seguridad y terceros.
- No envíen comunicaciones electrónicas masivas que permitan a los destinatarios conocer información de otras personas (direcciones de correo electrónico, cuentas de cobro, etc). Remitan correos electrónicos de forma tal que el destinatario sólo pueda ver su dirección de correo y no tenga acceso a las direcciones de correo de otros destinatarios de la misma comunicación.
- Remitan mensajes únicamente a personas respecto de las cuales se tenga autorización previa, expresa e informada para enviarle

comunicaciones a su dirección de correo electrónico. Para el efecto, antes de enviar el mensaje se debe verificar si se cuenta con dicha autorización, salvo que se trate de direcciones de correo que son datos públicos como, entre otras, direcciones corporativas o relacionadas con la profesión u oficio de una persona.

Implemente estrategias de Responsabilidad Demostrada *(accountability)* frente al Tratamiento de Datos Personales

Los edificios o conjuntos deben establecer la manera cómo probarán que han adoptado medidas útiles para cumplir las reglas sobre el Tratamiento de datos. Es necesario tener presente que, *"los responsables del tratamiento de datos personales deben ser capaces de demostrar, a petición de la Superintendencia de Industria y Comercio, que han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012"*[23] y en el Decreto 1377 de 2013.

Medidas "apropiadas" son aquellas ajustadas a las necesidades del Tratamiento de datos. Y "efectivas" son las que permiten lograr el resultado o efecto que se desea o espera. En otras palabras, no se deben adoptar medidas inoperantes, inservibles, inanes o infructuosas. Solo se deben instaurar aquellas adecuadas, correctas, útiles, oportunas y eficientes con el propósito de cumplir los requerimientos legales para realizar Tratamiento de Datos Personales.

Es preciso resaltar que la regulación sobre Datos Personales impone cargas probatorias en cabeza de los Responsables del Tratamiento como las siguientes:

Conservar prueba de haber informado al Titular, al momento de solicitarle la Autorización, de manera clara y expresa lo que ordena el artículo 12 de la Ley 1581 de 2012 y, cuando el Titular lo solicite, entregarle copia de ello[24].

"Solicitar y conservar, en las condiciones previstas en la presente ley, copia de la respectiva autorización otorgada por el Titular"[25].

"Proveer una descripción de los procedimientos usados para la recolección, almacenamiento, uso, circulación y supresión de información, como también la descripción de las finalidades para las cuales la información es recolectada y una explicación sobre la necesidad de recolectar los datos en cada caso"[26].

23 Cfr. Artículo 26 del Decreto 1377 de 2013.
24 Cfr. Parágrafo del artículo 12 de la Ley 1581 de 2012.
25 Cfr. Literal (b) del artículo 17 de la Ley 1581 de 2012 y artículo 8 del Decreto 1377 de 2013 "Los Responsables deberán conservar prueba de la autorización otorgada por los Titulares de datos personales para el Tratamiento de los mismos".
26 Cfr. Artículo 4 del Decreto 1377 de 2013.

"Documentar los procedimientos para el Tratamiento, conservación y supresión de los datos personales de conformidad con las disposiciones aplicables a la materia de que se trate"[27]**.**

"Desarrollar sus políticas para el tratamiento de los datos personales y velar porque los Encargados del Tratamiento den cabal cumplimiento a las mismas"[28].

"Conservar el modelo del Aviso de Privacidad que utilicen para cumplir con el deber que tienen de dar a conocer a los Titulares la existencia de políticas del tratamiento de la información y la forma de acceder a las mismas, mientras se traten datos personales conforme al mismo y perduren las obligaciones que de este se deriven"[29].

Adoptar "las medidas razonables para asegurar que los datos personales que reposan en las bases de datos sean precisos y suficientes y, cuando así lo solicite el Titular o cuando el Responsable haya podido advertirlo, sean actualizados, rectificados o suprimidos, de tal manera que satisfagan los propósitos del tratamiento"[30].

En suma, los edificios o conjuntos deben establecer medidas útiles, apropiadas y efectivas para cumplir sus obligaciones legales. Adicionalmente, tendrán que evidenciar y demostrar el correcto cumplimiento de sus deberes. Dichas herramientas, deben ser objeto de revisión y evaluación permanente, a fin de determinar su nivel de eficacia en cuanto al cumplimiento y grado de protección de los Datos Personales.

El reto frente al Principio de Responsabilidad Demostrada va mucho más allá de la mera expedición de documentos o redacción de políticas. Se trata de una actividad constante que exige demostrar un cumplimiento real y efectivo en la práctica de sus labores. No basta hacer meras declaraciones simbólicas de buenas intenciones, sino que es obligatorio evidenciar resultados concretos respecto del debido Tratamiento de los Datos Personales.

Es esencial realizar entrenamientos periódicos y especializados al equipo humano de la organización para proveerles la experticia, guía y herramientas que requieren para el correcto desarrollo de las tareas que involucren cualquier Tratamiento de Datos Personales.

Finalmente, esta entidad publicó la *"Guía para la implementación del Principio de Responsabilidad Demostrada (accountability)"*[31] la cual hace parte complementaria de este documento.

27 Cfr. Artículo 11 del Decreto 1377 de 2013.
28 Cfr. Artículo 13 del Decreto 1377 de 2013.
29 Cfr. Artículo 16 del Decreto 1377 de 2013.
30 Cfr. Artículo 22 del Decreto 1377 de 2013.
31 El texto lo puede consultar en: https://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia-Accountability.pdf

Industria y Comercio
SUPERINTENDENCIA

www.sic.gov.co

@sicsuper

Superintendencia de Industria y Comercio de Colombia

Superintendencia de Industria y Comercio

Conmutador: **(571) 5 870 000** - Contact Center: **(571) 5 920 400**
Línea gratuita nacional desde teléfonos fijos: **01 8000 910 165**

El futuro es de todos

Gobierno de Colombia