RÉGIMEN DIFERENCIADO PARA PYMES EN LA LEY 21.719

ANÁLISIS TÉCNICO Y PROPUESTAS DE INTERPRETACIÓN

Contribución de la Asociación de Profesionales en Protección de Datos (AGPD Chile)

Santiago de Chile · 9 de octubre de 2025

Agenda

1. Contexto
2. Alcance del concepto de PYME (Art. 14 septies)
3. Principios de Seguridad y Transparencia (Art. 14 septies)
4. Régimen de Encargados de Tratamiento
5. Cierre

Contexto: Art. 14 septies

Régimen diferenciado de cumplimiento.

Los **estándares o condiciones mínimas** que se impongan al responsable de datos para el cumplimiento de los **deberes de información y de seguridad** establecidos en los artículos 14 ter y 14 quinquies, respectivamente, serán determinados considerando el **tipo de dato** del que se trata, si el responsable es una **persona natural o jurídica**, el **tamaño** de la entidad o empresa de acuerdo a las categorías establecidas en el artículo segundo de la ley N° 20.416, que fija normas especiales para las empresas de menor tamaño, la **actividad** que desarrolla y el **volumen**, **naturaleza** y las **finalidades** de los datos personales que trata.

Novedad normativa.

Objetivo: proporcionalidad sin perder garantías.

“No se trata de flexibilizar derechos, sino de adaptar el cumplimiento a la realidad de las PYMEs”

Alcance del concepto de PYME

Remisión Ley 20.416

Criterio Financiero:

- Microempresa: hasta 2.400 UF
- Pequeña empresa: entre 2.400 y 25.000 UF
- Mediana empresa: entre 25.000 y 100.000 UF

Consolidación de ingresos

- Grupos económicos,
- Relaciones de control directo o indirecto.

Problemática interpretativa

Ignora naturaleza y riesgo del tratamiento

- Startups
- Organizaciones sin fines de lucro
- Fragmentación empresarial
- Disociación entre ingresos y capacidad operativa de la empresa.

Propuestas de interpretación

Criterio funcional y basado en riesgo, no solo financiero.

- Consolidación de ingresos a nivel de grupo económico
- Incorporar criterios operativos (Número de trabajadores, tecnologías, etc.)
- Evaluación de riesgos como condición de entrada

Recomendaciones para la Agencia

- **Guía interpretativa**
- Lista de **“banderas rojas”** (AEPD - ICO).
- **Consolidar los ingresos**
- A**utodiagnóstico**
- Fomentar el uso de **Códigos de Conducta**

Principio de Seguridad

Art. 3 letra f) de la Ley 21.719

“En el tratamiento de los datos personales, el responsable debe garantizar estándares adecuados de seguridad, protegiéndolos contra el tratamiento no autorizado o ilícito, y contra su pérdida, filtración, daño accidental o destrucción. Las medidas de seguridad deben ser apropiadas y acordes con el tratamiento que se vaya a efectuar y con la naturaleza de los datos.”

Elementos del principio de seguridad

Obligación Legal

Pesa sobre el responsable la obligación legal de **garantizar** estándares **adecuados** de seguridad

Protección de Datos Personales

Los estándares deben propender a proteger los personales de la organización

Prevención de incidentes

Se deben adoptar medidas que permitan **evitar incidentes de seguridad** (por ejemplo: tratamiento no autorizado o ilícito, o la pérdida, filtración, daño accidental o destrucción de los datos personales

Medidas idóneas al Tratamiento

Las medidas deben ser adoptadas de forma apropiada y acorde con el tratamiento que se vaya a efectuar

Medidas idóneas a la naturaleza del dato

Las medidas deben ser adoptadas de forma apropiada y acorde con la naturaleza de los datos personales

Aplicación diferenciada a PYMES

Texto Legal	*"los estándares o condiciones mínimas que se impongan al responsable de datos para el cumplimiento de los deberes de información y de seguridad establecidos (…) serán determinados considerando el tipo de dato del que se trata,* ***si el responsable es una persona natural o jurídica, el tamaño de la entidad o empresa de acuerdo a las categorías establecidas en el artículo segundo de la ley N° 20.416, que fija normas especiales para las empresas de menor tamaño, la actividad que desarrolla y el volumen, naturaleza y las finalidades de los datos personales que trata*****".**
¿Quién determina el estándar diferenciado?	los **"estándares o condiciones mínimas de cumplimiento"** y las medidas diferenciadas a que alude el artículo 14 septies de la LPD **serán determinados por la Agencia mediante instrucción general**
¿Cómo lo va a determinar la Agencia?	La Agencia deberá determinar cuales podrían ser tales estándares o condiciones mínimas de cumplimiento para las PYME's, considerando al menos: **i.si es persona natural o jurídica;** **ii.tamaño de la entidad** **iii.actividad desarrollada; y** **iv.características de los datos personales** (volumen, naturaleza, y finalidades) Al respecto consideramos relevante analizar la experiencia comparada europea, en la determinación de cómo debiera aplicarse el principio de seguridad para PYMEs / SMEs.

Experiencia de la National Cyber Security Center del Reino Unido (NCSC)

Enfoque del NCSC de UK

Fuente: *Cyber Security Small Business Guide, NCSC.*

- La NCSC promueve un conjunto de medidas de **bajo coste y alto impacto** que son el estándar mínimo de seguridad proporcional:

1. **Copias de Seguridad (Data Backup)**: Realización regular y almacenamiento seguro (cifrado y ubicación física separada del lugar de trabajo principal).
2. **Seguridad de Acceso**: Uso de contraseñas robustas y, fundamentalmente, la implementación de la autenticación multifactor (MFA) en todas las cuentas y dispositivos que almacenen información personal.
3. **Principio de Mínimo Privilegio:** Limitar el acceso a la información personal solo a aquellos empleados que lo necesiten estrictamente para su función.
4. **Disposición y Software:** Eliminación segura de equipos de TI y registros antiguos, además de mantener el software antivirus y antimalware actualizado.

- El énfasis de estas directrices en medidas como la MFA y las copias de seguridad separadas revela una preferencia por soluciones organizacionales que mitiguen el riesgo humano.

- Estas medidas, que requieren disciplina y formación más que una gran inversión en infraestructura, **ofrecen la mayor mitigación de riesgo por el menor costo, lo que se considera la aplicación práctica y efectiva del principio de proporcionalidad para entidades de menor tamaño.**

- Lo anterior tiene especial relevancia, considerando que de acuerdo al *Data BreachInvestigationsReport (DBIR) de Verizon de 2023, "[e]l 74% de todas las brechas incluyen el elemento humano, con personas involucradas ya sea por Error, Uso indebido de privilegios, Uso de credenciales robadas o Ingeniería social."*

Experiencia de El Garante (Autoridad de Datos de Italia)

Enfoque de El Garante (Italia)

Fuente: *Directrices Prácticas Y Medidas De Simplificación Para Las Pyme. El Garante.*

- **El Garante** propone un cumplimiento simplificado para las PYMEs, mediante 2 herramientas:

- Checklist simplificado, el cual contiene los siguientes 4 aspectos en la sección de medidas de seguridad:

  - ¿Tomó las medidas de seguridad adecuadas para proteger los datos personales?
  - ¿Tomó las medidas de seguridad mínimas necesarias para proteger los datos personales?
  - Si procesa datos sensibles y/o judiciales, ¿redactó, si estaba obligado a hacerlo, la declaración de política de seguridad y cumple con los requisitos establecidos en ella?
  - ¿Se revisan periódicamente las medidas de seguridad establecidas en la declaración de política de seguridad, en cualquier caso antes del 31 de marzo de cada año?

- Cumplimiento de las medidas de seguridad mínimas del Art. 33, 34 y 35 de la legislación de protección de datos Italiana, entre las cuales se encuentran:

  - Autenticación Informática
  - Sistemas de Autorización
  - Conservación y Custodia
  - Copia de Respaldo y Recuperación
  - Mantenimiento y Actualización

Experiencia de la European Union Agency For Network and Information Security (ENISA)

Enfoque de ENISA

Fuente: Guidelines for SMEs on the security of personal data Processing, ENISA.2016.

- **ENISA** propone un marco de acción para la gestión de riesgos simplificado para las PYME's, a través de una guía práctica y escalonada, para que tales entidades puedan cumplir con sus obligaciones de seguridad de datos de una manera proporcionada a los riesgos que afrontan y a los recursos de los que disponen, de la siguiente forma

- **Pasos para evaluación de riesgos**

  - **Paso 1:** Definición de la operación de tratamiento y su contexto. La PYME debe comprender claramente qué datos personales trata, con qué finalidad, por qué medios, dónde se lleva a cabo el tratamiento, quiénes son los interesados y quiénes los destinatarios de los datos.

  - **Paso 2:** Comprensión y evaluación del impacto. Se debe evaluar el impacto potencial que un incidente de seguridad podría tener sobre los derechos y libertades de las personas. El texto propone cuatro niveles de impacto: bajo, medio, alto y muy alto.

  - **Paso 3:** Definición de posibles amenazas y evaluación de su probabilidad. Este paso consiste en identificar las amenazas para la seguridad de los datos y valorar la probabilidad de que ocurran.

  - **Paso 4:** Evaluación del riesgo. Finalmente, se combina la evaluación del impacto y la probabilidad de la amenaza para determinar el nivel de riesgo global, que puede ser bajo, medio o alto.

Experiencia de la European Union Agency For Network and Information Security (ENISA)

Enfoque de ENISA

Fuente: Guidelines for SMEs on the security of personal data Processing, ENISA.2016.

- **ENISA** propone un marco de acción para la gestión de riesgos simplificado para las PYME's, a través de una guía práctica y escalonada, para que tales entidades puedan cumplir con sus obligaciones de seguridad de datos de una manera proporcionada a los riesgos que afrontan y a los recursos de los que disponen, de la siguiente forma

- **Pasos para evaluación de riesgos**

  - **Paso 1:** Definición de la operación de tratamiento y su contexto. La PYME debe comprender claramente qué datos personales trata, con qué finalidad, por qué medios, dónde se lleva a cabo el tratamiento, quiénes son los interesados y quiénes los destinatarios de los datos.

  - **Paso 2:** Comprensión y evaluación del impacto. Se debe evaluar el impacto potencial que un incidente de seguridad podría tener sobre los derechos y libertades de las personas. El texto propone cuatro niveles de impacto: bajo, medio, alto y muy alto.

  - **Paso 3:** Definición de posibles amenazas y evaluación de su probabilidad. Este paso consiste en identificar las amenazas para la seguridad de los datos y valorar la probabilidad de que ocurran.

  - **Paso 4:** Evaluación del riesgo. Finalmente, se combina la evaluación del impacto y la probabilidad de la amenaza para determinar el nivel de riesgo global, que puede ser bajo, medio o alto.

Principio de Seguridad

Recomendaciones para la Agencia

Recogiendo los puntos mencionados anteriormente, podría recomendarse a la futura APDP que se enfoque en los siguientes puntos al establecer condiciones mínimas de cumplimiento del principio de seguridad para PYMEs:

- Crear herramientas o marcos de cumplimiento simplificado: una idea práctica en este ámbito podría ser desarrollar una herramienta digital que guíe a las PYMEs a través de pasos básicos, explicados detalladamente, o preparar checklists que permitan a las PYMEs tener herramientas de cumplimiento simplificado, en lenguaje sencillo.

- Publicar guías sobre el deber de seguridad: Preparar y difundir guúas claras que traduzcan las obligaciones de seguridad de la Ley 21.719 en pasos concretos para la realidad de entidades chilenas, enfatizando las medidas técnicas y organizativas de bajo costo (por ej. como MFA, backup y políticas de control de acceso).

- Definir criterios de atenuación de sanciones: Revisar la factibilidad de establecer multas en base a criterios de atenuación basados en la capacidad financiera (UF) y considerando además la proactividad y colaboración de la entidad en la etapa post-brecha.

Principio de Transparencia

La transparencia y la información como garantía instrumental

La obligación de transparencia e información integra el núcleo esencial del derecho a la protección de datos y garantiza el ejercicio efectivo de los derechos del titular.

Diferenciación de estándares para responsables que califican dentro del artículo 14 septies

- ¿Cuáles serían los mínimos de cumplimiento exigibles a responsables de menor tamaño, que tratan datos de bajo o escaso riesgo, sin que ello genere una vulneración del derecho a la protección de datos?
- ¿Es posible rebajar el listado que se contiene en el artículo 14 ter?
- ¿Es posible en base al artículo 3 letra g) reemplazar la publicación de políticas por la publicación de las prácticas de tratamiento de datos personales?

Principio de Transparencia

Propuesta

Una medida razonable sería exigir del responsable, como mínimo la puesta a disposición del público en su sitio web o medio equivalente, lo siguiente:

- La **individualización** del responsable de datos y su representante legal y datos de contacto.
- El derecho que le asiste al titular para solicitar ante el responsable, **acceso**, **rectificación**, **supresión**, **oposición** y **portabilidad** de sus datos personales, de conformidad a la ley.
- **Prácticas de Tratamientos:** Tipos de datos que trata; descripción genérica del universo de personas que comprenden sus bases de datos; destinatarios a los que se prevé comunicar o ceder los datos; finalidades de los tratamientos que realiza; base de legitimidad del tratamiento, tratamientos que se basan en la satisfacción de intereses legítimos y medidas de seguridad.
- El derecho que le asiste al titular de **recurrir ante la Agencia**, en caso de que el responsable rechace o no responda oportunamente las solicitudes que le formule.
- El periodo durante el cual se **conservarán** los datos personales.

Principio de Transparencia

Consideraciones estratégicas

- La futura consideración de Chile como país con **nivel adecuado** de protección de datos a efectos de transferencias internacionales.
- Una delimitación adecuada y clara del estándar diferenciado para evitar la generación de **controversias administrativas y judiciales** en torno a la interpretación y aplicación del artículo 34 bis, letra a), que tipifica el incumplimiento del deber de información del artículo 14 ter.

Recomendaciones para la Agencia

- Establecer un **estándar mínimo uniforme y claro** de las prácticas de tratamiento de datos personales.
- Delimitar expresamente los **tratamientos excluidos** del régimen de diferenciación y elaborar **matrices** que permitan que permitan a los responsables identificar si su actividad califica para aplicar estándares diferenciados.
- Implementar **herramientas** de cumplimiento simplificadas para PYMES (mediante planillas Excel y/o softwares gratuitos).

Régimen de Encargado de Tratamiento

Art.15 bis. inc. 4° de la Ley 21.719 - Cesión de datos personales

“El tercero mandatario o encargado deberá cumplir con lo dispuesto en los artículos 14 bis (*Deber de secreto o confidencialidad*) y 14 quinquies (*Deber de adoptar medidas de seguridad*). La diferenciación de estándares de cumplimiento establecida en el inciso primero del artículo 14 septies también será aplicable al tercero mandatario o encargado (...)”

Problema Interpretativo

- ¿Se aplica al tamaño del responsable, del encargado, o de ambos?
- ¿Qué ocurre si una PYME contrata a una gran empresa tecnológica como encargado? ¿Puede el encargado aplicar un estándar diferenciado?

Régimen de Encargado de Tratamiento

Propuesta de interpretación

La diferenciación debe considerar ambas perspectivas:

- Artículo 28(1) GDPR obliga al responsable a seleccionar solo encargados que ofrezcan "***garantías suficientes para aplicar medidas técnicas y organizativas apropiadas***".

- Artículo 32 GDPR dispone que tanto responsables como encargados deben aplicar medidas de seguridad proporcionales al riesgo, considerando el **"estado de la técnica"**, los "**costes de implementación**" y la "**naturaleza**" del tratamiento.

- EDPB Guidelines 07/202013: Los encargados, aunque limitados por las instrucciones del responsable, cuentan con cierto margen de **discrecionalidad** sobre el modo de servir mejor a los intereses del responsable, de manera que permitan al encargado elegir los medios técnicos y organizativos **más adecuados** (medios esenciales y no esenciales)

Régimen de Encargado de Tratamiento

Recomendaciones para la Agencia

- **Instrucción General interpretativa** que aclare que la diferenciación de estándares debe considerar: (a) El **perfil del encargado** (tamaño, sector, capacidad técnica). (b) El **tipo de tratamiento** instruido por el responsable y su **nivel de riesgo**. (c) Las **condiciones del responsable** del tratamiento.

- **Lineamientos específicos** para encargados en función de **escalas organizacionales** y **sectores críticos** (Ej. servicios tecnológicos, salud, educación)

- **Prohibición expresa** para encargados de gran escala acojerse a estándares mínimos si su propia estructura y el tratamiento que realizan conllevan riesgos elevados para los titulares.

- **Modelos tipo de cláusulas contractuales** que reflejen estos criterios de proporcionalidad y corresponsabilidad entre responsables y encargados.

Cierre

1. El régimen diferenciado **no es una exención**, sino una forma de garantizar el cumplimiento efectivo.

2. Requiere **equilibrio** entre protección de derechos y viabilidad operativa de las PYMEs.

3. Las PYMEs representan el **98,6 %** del total de empresas en Chile Fuente: *Ministerio de Economia, Consejo de Empresas de Menor Tamaño*. Plan de Desarrollo Estratégico (2023)

Gracias

Email
directorio@agpdchile.cl

Linkedin