

Chile's Personal Data Law 21.719: a practical SME guide

What changes on December 1, 2026, what your customers can demand, and the first steps to comply without overspending. Operational guidance, not legal advice.

VE Solutions · Fractional technology & AI leadership

If you store data about customers, employees, or suppliers — a WhatsApp list, a member spreadsheet, records, emails, cameras — Chile's new personal data law applies to you. It is not just for banks or large companies: it covers any business that processes people's data.

This guide covers the essentials in business-owner language: what changes, what can be demanded of you, and where to start. It does not replace a lawyer; it prepares you to talk to one without starting from zero, and to avoid buying 'magic compliance' you do not need.

1. What changes, and from when

Law 21.719 modernizes data protection in Chile and comes into full force on December 1, 2026. It creates a dedicated authority — the Personal Data Protection Agency — with real inspection and sanctioning powers.

Fines are tiered by severity and, in the most serious cases, can reach amounts that put an entire SME at risk. The point is not to memorize figures: for the first time, non-compliance has a real, enforceable cost.

- Full force: December 1, 2026.
- A new enforcement agency with tiered sanctions (minor, serious, and very serious).
- Applies to companies of any size that process personal data.
- Health data and other sensitive data carry the highest standard.

2. The rights your customers can demand

Anyone whose data you hold can hold you to account: what you have about them, what you use it for, that you correct it, delete it, stop using it for marketing, or hand it over in a portable format. And you have deadlines to respond.

For an SME, the practical risk is not the hostile customer: it is having NO process at all to respond. If a request landed in your inbox today, who sees it, what do they answer, and where is it recorded?

- Access: what data you hold and why.
- Rectification: fixing what is wrong.
- Deletion: erasing when it applies.
- Objection and marketing opt-out: stop using their data to sell to them.
- Portability: handing over their data in a standard format.

3. Consent: the pre-ticked box no longer works

Valid consent must be free, specific, informed, and unambiguous. In practice: no pre-ticked boxes, no 'by purchasing you accept advertising' hidden in the terms, and marketing consent goes SEPARATE from everything else.

Just as important: you must be able to PROVE consent. A simple record — who, when, for what, how — is worth more than any nice statement on your website.

- Marketing always gets its own checkbox, unticked by default.
- Keep evidence: date, accepted text, and channel.
- Opting out must be as easy as opting in.

4. Your first 7 steps (in order)

You do not need to start with a giant project. You need to start in order. These seven steps cover what a basic inspection would look at first, and almost all can be done with what you already have.

1. Inventory: what data you hold, whose, where it lives, and who can access it.
2. Lawful basis: for each use — contract, consent, or another legal ground?
3. A visible, plain-language privacy policy describing what you actually do.
4. Consent up to date: forms with separate checkboxes and a record.
5. Contracts with whoever processes data on your behalf (software, agencies, accountants).
6. Minimum security: real passwords, per-person access, a tested backup.
7. A channel and an owner for rights requests, with a deadline.

5. Where technology helps (and where it does not)

The right technology lowers the cost of compliance: forms that record consent on their own, automatic backups, role-based access. And when you use AI, local deployment makes the difference: a model running on your own infrastructure processes your data without it ever leaving your business.

What does NOT exist is 'software that makes you compliant' just by buying it. Compliance is process plus evidence; tooling only makes it cheaper and harder to forget.

- Automate the record-keeping (consent, requests, backups), not the judgment.
- With sensitive data, prefer local processing or vendors with a clear contract.
- Distrust anyone selling 'total compliance' without looking at your operation.

Three concrete cases

RETAIL

The butcher shop's WhatsApp list

A broadcast list with 400 customers is a personal database. It needs separate, recorded marketing consent, a simple way off the list, and an owner if someone asks for their number to be deleted. None of this needs expensive software: it needs order and evidence.

HEALTHCARE

The veterinary clinic with records and reminders

Health data — in clinics, dental practices, and care centers too — is sensitive: a higher standard, more care about who accesses it and which vendor processes it. If an AI agent confirms appointments, it must identify itself as AI, record consent, and hand over to a person. Local processing is gold here.

SERVICES

The gym with members, payments, and cameras

Member data, payment methods, and security cameras coexist in the same business. Each has a different legal basis: the membership contract, billing obligations, premises security. Mapping them takes an afternoon and orders every decision that follows.

The 10-point checklist

Print this page. If you tick fewer than 7, you have work to do before December 2026.

- ☐ I know what personal data I hold and where it lives.
- ☐ Every use has an identified legal basis.
- ☐ My privacy policy describes what I actually do.
- ☐ Marketing consent is a separate, unticked checkbox.
- ☐ I can prove when and how each contact consented.
- ☐ I have a contract with every vendor that touches my data.
- ☐ Access is per person and revoked when someone leaves.
- ☐ I have an automatic backup and have tested restoring it.
- ☐ There is a channel and an owner for rights requests.
- ☐ If I use AI with customer data, I know where it is processed and who sees it.

What if I need help?

This guide is operational guidance, not legal advice: to interpret the law for your case, consult a lawyer. Where we do help is the technical and process side: an express compliance diagnostic from \$390.000 + VAT, full adaptation depending on your case, and technology that records compliance on its own — including AI models that run on your own infrastructure, where your data never leaves.

Let's talk through your case at vsol.cl · contacto@vsol.cl