TANARO

NEW PERSONAL DATA LAW

Let's protect people's data



What every team needs to know

Starts October 15, 2027

Chilean Law No. 21,719 · Training by Tanaro

What will we cover?

1	**The basics**	What the law is, when it applies and who it protects
2	**The rules**	When and how data can be used
3	**The rights**	What customers and employees can ask for
4	**Day-to-day work**	Cameras, deliveries, social media and daily tasks
5	**Tasks and risks**	What companies must do and what happens if they fail

Why a new law?

Chile had a law from 1999. The internet, apps and smartphones changed everything.

BEFORE

Law 19,628 (1999)

- No dedicated regulator
- Very low fines
- Few rights
- Few security rules

NOW

Law 21,719

- A new Agency enforces it
- Very high fines
- More rights for people
- Data must be protected and leaks reported

When does it apply?

The law already exists. Everyone was given time to prepare.



Dec 13, 2024

Law is published

The preparation period begins.

Dec 1, 2026

Original date

Postponed by law.

Oct 15, 2027

Law takes effect

Extension published in the Official Gazette (Nov 2026).

The extension is now law: it applies from October 15, 2027. Prepare anyway.

Who is protected and who must comply?



PROTECTS all individuals

- Customers
- Employees and job applicants
- Suppliers who are individuals
- **Regardless of nationality**



APPLIES to anyone using data

- Large and small companies
- Retail, services, health, education…
- Their suppliers (apps, systems)
- **And every employee must keep it confidential**

Key terms

Five simple words to understand the law.



Data subject

The person the data belongs to. E.g., the customer.



Controller

Whoever decides what to do with the data. E.g., the company.



Processor

Whoever uses the data on behalf of another. E.g., the payroll system.



Processing

Anything done with data: collecting, recording, storing, sending, deleting.



Agency

The new authority that supervises and imposes fines.

What is personal data?

Any information that shows who a person is.

- **Name**
- **ID number or passport**
- **Phone**
- **Email**
- **Photo or video**
- **Address**
- **Payment details**
- **Licence plate**

If the information can identify the person → it is personal data.

TANARO

Sensitive data: extra care

Highly private data. Only used with consent or where the law allows.



Health

Illnesses, test results, medical leave



Fingerprint or face

Fingerprint or facial-recognition time clocks



Religion and origin

Beliefs, ethnic or racial origin



Private life

Sex life, union membership, political views

Workplace example

A co-worker hands in a medical certificate.

Only the person processing it sees it. Never discuss their illness.

Children under 14: their parents' consent is needed to use their data.

TANARO

Where is data in your company?

Retail

Customers, receipts, deliveries, loyalty cards

Restaurants and hotels

Bookings, guests, delivery

Health and wellness

Records, test results, appointments

Offices and services

Customer databases, contracts, emails

Construction and industry

Workers, contractors, site access

Education

Students, parents, grades

Extra care by industry

Some companies handle more delicate data and must protect it even more.



Health and wellness

Health data is sensitive. Only those who need it for care may see it.



Education and children

Data of children under 14 requires parents' consent.



Credit and collections

Debt and payment data have special rules. If leaked, each person must be told.



HR and recruitment

Employee and applicant data: only for work purposes, with limited access.

The 5 golden rules

How to protect data, every day.

1

Ask only for what you need

For a quote, name and contact are enough.

2

Use it only for that

The customer's phone is not for anything else.

3

Keep it safe

Password-protected, locked away, out of sight.

4

Delete it when done

Don't keep data forever.

5

Be transparent

People must know what you do with their data.

When can we use data?

We always need a valid reason. These are the main ones:



The person said yes

Clear, freely given consent. It can be withdrawn at any time.

E.g., agrees to receive promotions.



There is a contract

The data is needed for the service.

E.g., address for delivery.



The law requires it

A law requires having the data.

E.g., employee details for their contract.



Legitimate interest

A fair reason that does not harm the person.

E.g., cameras for security.

How to ask for consent properly

The person's "yes" must be clear. It cannot be assumed.



DO

- The customer ticks the "Yes, I want promotions" box themselves
- Explain what their data will be used for
- They can say no and still be served
- They can withdraw consent easily and for free



DON'T

- The box is pre-ticked
- "Silence means yes"
- "No sale without accepting promotions"
- Use the consent for something else

Each person's rights

Customers and employees can ask us to:



Access

"What data do you have?"



Correct

"My phone number is wrong."



Delete

"Delete my data."



Object

"Don't use my data for that."



Port

"Give me my data in a file."



Restrict

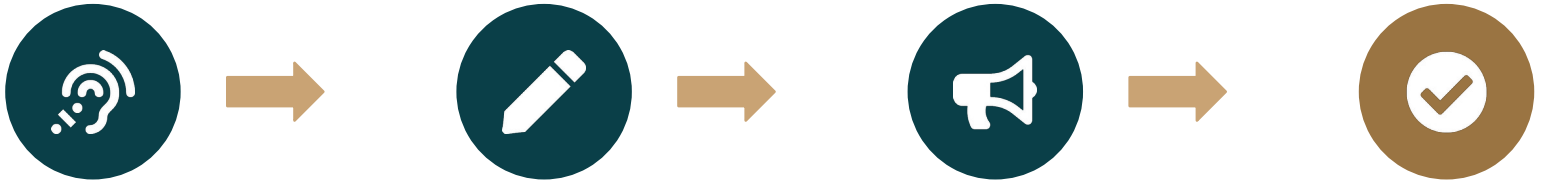
"Stop using it for now."

The company must reply in writing within 30 days.

TANARO

If a customer asks you about their data…

You don't have to solve it yourself. Follow these steps:



1. Listen respectfully

Never refuse or argue.

2. Write it down

Name, contact and request.

3. Report it today

Tell the data protection officer the same day.

4. The company replies

In writing, within 30 days.

Each company needs a designated contact for these cases, known to all staff.

Security cameras

A person's image is personal data.



Recommendations for the company

Visible sign

Let people know there are cameras.

For security only

Not to monitor employees minute by minute.

Never in restrooms

Or changing rooms: they are private spaces.

Few people watch them

Only authorised staff.

Delete over time

Don't keep recordings forever.

Don't share videos

Not on WhatsApp or social media.

Employees: your data is protected

- ID card or passport
- Contract
- Salary bank account
- Address
- Medical leave
- Time-clock fingerprint

The company must:

- Use your data only for work: pay, social security, taxes
- Let only those who need it see it
- Take extra care of your health data
- Tell you if it uses your fingerprint or face
- **You can ask to see and correct your data**

Deliveries, social media and promotions



Deliveries

- Use the address and phone only to deliver
- Don't save them on your personal phone
- Don't contact the customer afterwards



Social media

- Ask before posting photos with customers
- The same for photos of co-workers
- Never post documents containing data



Promotions

- Only to those who said "yes"
- Always with an easy way to opt out
- If someone opts out, remove them quickly

Day to day: do's and don'ts

DO

- Lock your work computer and phone
- Lock away papers containing data
- Tear up or shred papers you no longer need
- Use data only for your work
- Report anything odd or anything lost

DON'T

- Take photos of customers or documents
- Share customer phone numbers on WhatsApp
- Post customer videos on social media
- Lend your password to anyone
- Discuss customers' or co-workers' health

Right or wrong?

Group discussion: raise your hand if you think it's right.

1. A co-worker asks for a customer's number to ask her out. You give it.
2. A customer asks to stop receiving promotions. You note it and tell the data officer.
3. You film an angry customer on your phone and post it on TikTok.
4. You leave your computer unlocked with the customer list and go to lunch.
5. You ask the customer only for the data needed for their invoice.
6. The HR manager keeps medical certificates in a locked cabinet.

Answers

1. WRONG

The number was only for serving her. Using it for anything else is not allowed.

2. RIGHT

It's their right. Remove them from the list quickly.

3. WRONG

People are shown without consent. Tell the data officer and post nothing.

4. WRONG

Anyone could see the data. Always lock it.

5. RIGHT

It's needed for the sale. Use it only for that.

6. RIGHT

It's health data: it needs extra care.

Tasks for the company

For owners, management and supervisors, before 15 October 2027:

1. **Make an inventory**
   What data we hold, where it is and why.
2. **Publish a privacy notice**
   On the website and at customer service.
3. **Ask for clear consent**
   For promotions: the customer ticks "yes".
4. **Protect the data**
   Passwords, limited access, backups.
5. **Review suppliers**
   Sales, payroll, cloud and delivery systems.
6. **Disclose fingerprint or camera use**
   Which system, why and for how long.
7. **Set up a request channel**
   And reply within 30 days.
8. **Train the team**
   And have a data breach plan.

Suppliers that use our data

If another company handles data for us, there must be a contract.

- **Sales and checkout**
- **Cloud and email**
- **Accounting and payroll**
- **Cameras**
- **Marketing**

The contract must state:

- What data it uses and whose
- What for and for how long
- That it cannot use it for anything else or pass it on

- That it must keep it confidential and secure
- That it must tell us about any breach
- That it must delete or return it at the end

4-step action plan

A guide for owners and supervisors.



1. Review

Now

- Inventory of the data we hold
- Where it is and who sees it
- Which suppliers use it



2. Organise

Next

- Privacy notice
- Consent forms
- Supplier contracts



3. Protect

Before Oct 2027

- Passwords and access
- Cameras and paperwork
- Data breach plan



4. Maintain

From Oct 2027

- Train the team
- Handle requests
- Review every year

If something goes wrong

Examples: a laptop is stolen, a folder is lost, email is hacked.



Employee

Tell the data officer immediately. Don't hide it: reporting quickly helps everyone.

Deliberately hiding a breach is a very serious offence.

Company

- Notify the Data Protection Agency without delay if people are at risk.
- Also notify those affected if health, children's, payment or debt data is involved.
- Record what happened and what was done to fix it.

What if the law is not followed?

A new body, the Personal Data Protection Agency, supervises and imposes fines.

MINOR

up to

5,000 UTM

≈ CLP 359 million

E.g., not replying on time

SERIOUS

up to

10,000 UTM

≈ CLP 717 million

E.g., using data without consent

VERY SERIOUS

up to

20,000 UTM

≈ CLP 1,434 million

E.g., hiding a breach

Amounts in Chilean pesos based on the September 2026 UTM (CLP 71,721). Smaller companies: in the first year the Agency may issue only a written warning.

My daily checklist

Before ending your shift, check:

- [ ] I locked my work computer and phone
- [ ] I put away papers and folders with data
- [ ] I left no customer data in sight
- [ ] I saved no customer data on my phone
- [ ] I shredded data papers I don't need
- [ ] I shared no photos or videos of customers
- [ ] I passed customer data requests to the officer
- [ ] I reported anything lost or odd

Tip: print this slide and post it somewhere visible.

Remember



Ask for little



Use it well



Keep it safe



Delete it on time



Report quickly

People's data isn't ours: we only look after it.

Questions?

TANARO

contacto@tanaro.cl · www.tanaro.cl