Start by listing every outside service that holds your customers' data

In autumn 2026, the largest data leaks in Japan happened at services that companies had hired to send their emails. When one delivery service is breached, hundreds of organizations that entrusted it with data end up disclosing leaks at the same time. Knowing where you keep what matters as much as locking your own doors.

81.33 million
Email addresses leaked from ARARA message, an email delivery service. Up to about 380 client companies

5 in 16 days
Email delivery services where intrusions were found between October 11 and 27, 2026

5 → 58
Incidents in the information and communications sector caused by breached SaaS or contractors (2025 → 2026 through October)

1 List the outside services that hold your customers' data

Departments often sign up on their own, so nobody in the company knows the full picture. Write them down in the table overleaf.

- ☐ Went through each department for email delivery, booking, member apps, online shops, surveys, campaign entries and recruiting tools
- ☐ Checked who runs each service and whether they subcontract it to another company

2 Hand over only the fields they need

Of the 81.33 million records leaked at ARARA, about 47.04 million included more than an email address, such as names and dates of birth.

- ☐ Listed, for each service, the fields we hand over (name, address, phone, date of birth, purchase history and so on)
- ☐ Stopped handing over fields the service does not need for its job

3 Have data deleted from services you stop using

At Ymirlink, about 420,000 unencrypted passwords leaked from a service that had been shut down in February.

- ☐ Got written confirmation that our data was deleted when a contract ended
- ☐ Also looked for services we only trialled and accounts left behind when staff moved on

4 Decide what to do when a vendor reports an incident

SEGA heard from ARARA on November 1 and disclosed on November 9. The first figures announced can change a great deal in later reports.

- ☐ Named who receives the call and who decides next (see "Steps" overleaf)
- ☐ The people in charge know the deadlines for notifying customers and the Personal Information Protection Commission

Sources: MM Research Institute (Nov 4, 2026), piyolog (Nov 9, 2026), ANN (Nov 11, 2026), Nikkei xTECH, @IT and company announcements.
Full article: "Japan's autumn 2026 data breaches spread through the services companies use." Data is CITY (teleport.jp/dataiscity/en) November 2026

Outside services that hold customer data

Each department fills this in; then combine them into one company list. The first row is an example.

Service What it is used for	**Operator** Incl. subcontractors	**Department** Person in charge	**Fields shared** Cross out what isn't needed	**Approx. records**	**Contract** Active / ended	**If ended** Deletion confirmed
Newsletter delivery	(Delivery service provider)	Marketing	Email, name, ~~date of birth~~	~50,000	☐ Active ☐ Ended	☐ Done
					☐ Active ☐ Ended	☐ Done
					☐ Active ☐ Ended	☐ Done
					☐ Active ☐ Ended	☐ Done
					☐ Active ☐ Ended	☐ Done
					☐ Active ☐ Ended	☐ Done
					☐ Active ☐ Ended	☐ Done
					☐ Active ☐ Ended	☐ Done
					☐ Active ☐ Ended	☐ Done
					☐ Active ☐ Ended	☐ Done
					☐ Active ☐ Ended	☐ Done
					☐ Active ☐ Ended	☐ Done

Steps when a vendor reports a possible leak

The notice can arrive suddenly by email or phone. Write down in advance who takes it and what to check.

Receives the notice	(name, phone)
Decides next	(name, phone)
Ask the vendor	When, which data, how many records, whether exfiltration is confirmed, whether it is still going on
How to tell customers	(email, website, phone line)
Who follows updates, how often	(e.g. check the vendor's announcements every evening)

Reporting in Japan: when a leak (or possible leak) of personal data must be reported to the Personal Information Protection Commission, a **preliminary report is due within roughly 3–5 days** of learning of it and a **final report within 30 days** (60 days where it may have been done for a wrongful purpose). The individuals concerned must also be notified. Even when the incident happened at a vendor, the company that entrusted the data may be the one obliged to report. (Source: PPC, Guidelines on the Act on the Protection of Personal Information, General Rules)

Feel free to copy and adapt this sheet for internal use. Data is CITY (teleport.jp/dataiscity/en) November 2026