How to use this template: fill in the names and contact details in [brackets], check the steps against how your organisation works, and make sure every employee knows step 1. Log every breach in the Breach_Register tab of the workbook. This template is a starting point, not legal advice. Adapt it to your organisation and check it against the law of your country and your supervisory authority's guidance.

Personal data breach procedure, [Organisation name]

Version [1.0], [date]. Owner: [name, role]. Applies to all staff, temporary staff and contractors.

1. What is a personal data breach?

A breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data (Art 4(12) GDPR). Examples: an email with customer data sent to the wrong person, a lost laptop or phone, ransomware, a hacked mailbox, paper files in the wrong bin, a supplier that reports a leak.

2. Who does what

Role	Name	Contact
Breach lead	[name]	[phone, email]
Deputy	[name]	[phone, email]
IT support / supplier	[name or company]	[phone, email]
Supervisory authority	[e.g. Autoriteit Persoonsgegevens / CNIL / BfDI]	[breach notification web form]
Insurer (cyber policy, if any)	[company]	[policy number, phone]

3. Steps

1. **Report it at once.** Anyone who notices a possible breach tells the breach lead immediately, by phone if possible, also outside office hours. Say what happened, when, which data and who may be affected. Do not wait until you are sure.
2. **Log it.** The breach lead records the date and time the organisation became aware in the Breach_Register. You are aware when you are reasonably certain that a security incident has led to personal data being compromised (EDPB Guidelines 9/2022). A short check to establish that is fine; a long delay is not.
3. **Contain it.** Stop the leak and limit the damage: recall or ask the recipient to delete an email, reset passwords, remote-wipe a device, disconnect an infected system, ask the supplier what happened.
4. **Assess the risk to people.** Consider the type of data, how sensitive it is, how many people, whether they can be identified, whether the data was encrypted, and what could happen to them (fraud, identity theft, distress, discrimination). Write down your reasoning.
5. **Decide on telling the authority (Art 33).** Notify [supervisory authority] without undue delay and, where feasible, within 72 hours of becoming aware, unless the breach is unlikely to result in a risk to people. If you notify later than 72 hours, give the reasons for the delay. If you do not yet have all facts, notify what you know and add the rest later (Art 33(4)).

Sample — lerider.com

Sample — the full pack: lerider.com/shop/gdpr-records-workbook-eu/

6. **Decide on telling the people affected (Art 34).** If the breach is likely to result in a high risk to them, tell them without undue delay in clear language: what happened, the likely consequences, what you did and what they can do, and a contact point. Not required if one of the Art 34(3) cases applies (for example the data was encrypted and the key is safe); record which one.
7. **Record everything.** Every breach goes in the register, also the ones you do not report: facts, effects, measures taken and your reasoning (Art 33(5)).
8. **Learn from it.** Within [two weeks], review what went wrong and what to change. Note the actions.

4. What the notification to the authority contains (Art 33(3))

- the nature of the breach, including where possible the categories and approximate number of people and records concerned;
- the name and contact details of the [privacy contact / data protection officer];
- the likely consequences;
- the measures taken or proposed, including to limit possible harm.

5. Breaches at our suppliers

Our processors must tell us without undue delay after becoming aware of a breach (Art 33(2)); our data processing agreements say so. Our 72 hours start when we become aware, usually when the supplier informs us.

6. Other duties

Other rules may also require a report, for example [the NIS2 law of your country, sector rules, your insurer's policy terms, the police in case of crime]. Check them in step 5.

Sample — lerider.com

Sample — the full pack: lerider.com/shop/gdpr-records-workbook-eu/

How to use this template: fill in the [brackets], tell all staff about section 2, and log every request in the DSAR_Log tab of the workbook. This template is a starting point, not legal advice. Adapt it to your organisation and check it against the law of your country and your supervisory authority's guidance.

Procedure for requests from individuals, [Organisation name]

Version [1.0], [date]. Owner: [name, role]. Covers requests under Articles 15 to 22 GDPR from customers, staff, applicants and anyone else whose data we hold.

1. Deadlines

- Answer without undue delay and at the latest within one month of receipt (Art 12(3)).
- If a request is complex or there are many, the deadline can be extended by two further months. Tell the person within the first month, with the reasons.
- If we do not act on a request, tell the person within one month why, and that they can complain to the supervisory authority or go to court (Art 12(4)).
- The workbook calculates the dates. When the last day falls on a weekend or a public holiday, it moves to the next working day.

2. Recognising a request

A request does not need special words, a form or a reference to the GDPR. It can come by email, letter, phone, social media or in person, and to any employee. Anyone who receives something that looks like a request passes it to [privacy contact] the same day.

3. Steps

1. Log it in the DSAR_Log on the day it arrives (date received, who, which right).

2. Check identity only if there is reasonable doubt (Art 12(6)). Ask for no more than you need. Do not ask for a copy of an ID card when an email from a known address is enough.

3. Clarify if needed. For large amounts of data you may ask the person what they are looking for (Recital 63). Our default: the clock keeps running. The EDPB accepts a pause in limited cases: while you wait for information you asked for, without undue delay, to confirm the requester's identity, or for an access request to specify the processing it relates to where Recital 63 applies (EDPB Guidelines 01/2022, para 159). Use that pause only in those cases and note the dates in the DSAR_Log.

4. Search all places where data may be: [systems, mailboxes, shared drives, paper files, suppliers].

5. Prepare the answer (see section 4). Remove data about other people where giving it would harm their rights (Art 15(4)).

6. Send it securely, in the form the person asked for where possible; electronically if they asked electronically (Art 12(3)).

7. Close the log entry: date answered and what was sent.

Sample — the full pack: lerider.com/shop/gdpr-records-workbook-eu/

4. What each right means for us

Right	What we do
Access (Art 15)	Confirm whether we process their data; give a copy and the information in Art 15(1): purposes, categories, recipients, retention period, rights, source, automated decisions, transfer safeguards.
Rectification (Art 16)	Correct or complete the data.
Erasure (Art 17)	Delete the data if one of the grounds in Art 17(1) applies and none of the exceptions in Art 17(3) (for example a legal duty to keep it).
Restriction (Art 18)	Keep the data but stop using it, in the cases in Art 18(1).
Portability (Art 20)	Give data the person provided, in a structured, machine-readable format, where processing is based on consent or contract and is automated.
Objection (Art 21)	Stop processing based on legitimate interests unless we have compelling grounds; always stop direct marketing.
Automated decisions (Art 22)	Offer human review where a decision is based only on automated processing and has legal or similar effects.

After rectification, erasure or restriction, tell the recipients of the data unless this is impossible or takes disproportionate effort (Art 19).

5. Costs and refusals

Requests are free. Only when a request is manifestly unfounded or excessive, in particular because it is repetitive, may we charge a reasonable fee or refuse (Art 12(5)). We must be able to show why. Decisions to refuse are taken by [name, role].

Sample — lerider.com

Sample — the full pack: lerider.com/shop/gdpr-records-workbook-eu/