Data leak or exposure

Version 1.0 · Reviewed Oct 11, 2026 · TLP:CLEAR · For: IT, data and legal leads, and management.

What to do when personal or confidential information is left exposed, was copied without authorization or turns up published. The goal is to close the exposure, know precisely what leaked and notify those affected honestly.

Signs it is happening

- A database, backup or folder reachable from the internet without a password.
- The organization's data for sale or published on a forum.
- A notice from a researcher, customer or journalist about exposed information.
- Unusual bulk downloads or queries on an internal system.
- A lost or stolen device that held unencrypted information.

How serious it is

Critical	Sensitive data on many people (health, financial, minors) or data already published.
High	Personal data or credentials exposed, with publication not confirmed.
Medium	Non-sensitive internal information, or a brief exposure with no evidence of access.

First hour

- [ ] **1.** Close the access: take the resource off the internet or restrict its permissions.
- [ ] **2.** Do not delete anything: preserve the state and the access logs of the exposed resource.
- [ ] **3.** Change the passwords and keys that appear inside the exposed data.
- [ ] **4.** Save evidence of the publication (screenshot, address, date) if the data is online.
- [ ] **5.** Convene IT, legal and management; define who makes the decisions.
- [ ] **6.** Start the inventory: what data, on how many people and from what dates.

Preparation (before the incident)

- Keep an inventory of what personal data you hold and where.
- Keep only what is necessary and delete what is no longer used.
- Encrypt data at rest and portable devices.
- Periodically review which cloud resources are public.
- Have a notification template for affected individuals already drafted.

Detection and Analysis

- Confirm that the data is authentic and which system it comes from.
- Determine the exposure window: from when and until when.
- Review the logs to find out whether anyone accessed it and what they took.
- Classify the data: identification, contact, financial, health, credentials.

Containment

- Revoke the related access, API keys and tokens.
- Request removal of the content from the site or platform where it is published.
- Force a password change if user credentials were exposed.

Eradication

- Fix the cause: configuration, vulnerability or compromised account.
- Look for the same flaw in similar systems.
- Ask the search engines to remove the cached copies.

Recovery

- Restore the service with the controls fixed and verified.
- Watch for misuse of the data: fraud, impersonation, targeted phishing.
- Offer those affected a channel for questions and concrete guidance.

Lessons Learned

- Document the cause, scope and decisions, with dates.
- Reduce the stored data that was not necessary.
- Add the exposure review to the periodic controls.

Evidence to preserve

- Access logs of the exposed resource.
- A copy or sample of the leaked data, stored with restricted access.
- Screenshots of the publication, with address and date.
- Communications received from third parties about the leak.

What not to do

- Denying or downplaying the leak before knowing the scope.
- Deleting the exposed resource without having saved the logs.
- Notifying those affected with vague information or without telling them what to do.
- Negotiating with anyone offering to “return” the data.

Who to notify

- Affected individuals: what data, since when, what risk they face and what they should do.
- Management and legal counsel, to assess contractual and regulatory obligations.
- Your sector's regulator, if applicable.
- The Public Ministry (Ministerio Público), if there was unlawful access.
- cert.gt, for guidance and coordination.

When to close the incident

- The exposure is closed and verified from outside the network.
- The scope is documented: data, people and dates.
- Those affected have been notified.
- The root cause has been fixed in all similar systems.

cert.gt is a private, community-driven initiative of Devel Group.

cert.gt · devel.group · Report an incident at cert.gt/en/reportar or email incidentes@cert.gt

General good-practice guidance; it does not replace legal or specialized technical advice for your case. This is not a document from a government entity. You may copy and adapt it with attribution (CC BY 4.0).