



# Privacy Incident Response: From Panic to Prepared

*A practical visual guide for privacy professionals to spot, triage, and respond to incidents before they become breaches.*



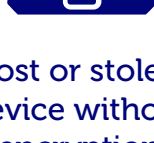
## Is it an incident or a breach?

Not every incident is a breach. But every incident requires attention. These are common incident types that could escalate into breaches depending on severity, scope, and exposure.

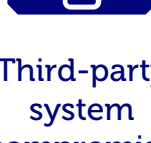
**Your job is to assess, not assume.**



Misaddressed email with personal data



Lost or stolen device without encryption



Third-party system compromise



Misconfigured file or database permissions



Suspicious activity in cloud storage or SaaS tools



**Treat all incidents seriously. You won't know if it is a breach until you investigate.**

## Ask the First Four

*When an incident occurs, gather the facts by asking:*



- What happened?
- When did it happen?
- What data/systems are affected?
- Is the threat still active?

**Use incident classification to prioritize.**

*A P1 or P0 = potential breach = legal, regulatory, and executive-level action.*

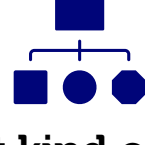
## Assess the “Blast Radius”

*How big is the impact? Start with:*



**Who's affected**

*Customers?  
Employees? Vendors?*



**What kind of data**

*Contact information?  
Health records?  
Financial data?*



**How is it stored**

*Structured systems or an unstructured format, like in documents?*



**How many records**

*10 records or 10 million?*



**What is the harm**





*Legal? Reputational?  
Identity theft?*



**The more you know, the better you can contain, notify, and recover.**

## Know the Law (and the Fine Print)

*Timeframes by region and contract:*

Law/Framework	Notification Timeline
 GDPR (EU/UK)	Within 72 hours notify regulators
 HIPAA	Without undue delay (up to 60 days)
 U.S. State Laws	Varies by state
 Your contract	Sometimes 24 hours or less



**Contracts often have stricter timelines. Know yours.**

## Call in the Team

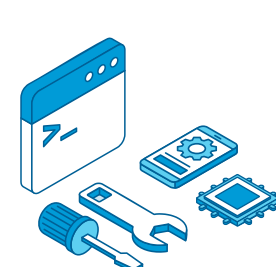
*Incident response is a team sport. Key players might include:*



**Security**



**Legal**



**Engineering**



**Communications**



**HR**



**Leadership**



**Limit communications to a core group. Avoid unnecessary email changes. Understand your legal risks.**

## Notifying the Right People



Only notify when required, but when you do, be:

- **Timely**
- **Clear**
- **Empathetic**
- **Legally correct**



Your audience might include:

- **Regulators**
- **Impacted individuals**
- **Business partners**
- **The public**



**Provide help: FAQs, credit monitoring, support hotlines.**

## Debrief Like a Pro

**After the dust settles:**

- ➔ What happened?
- ➔ Who was involved?
- ➔ What worked, what didn't?
- ➔ What should change?



**Run tabletop exercises. Update your playbook. Strengthen your response muscle.**



## Build Your Playbook Before You Need It

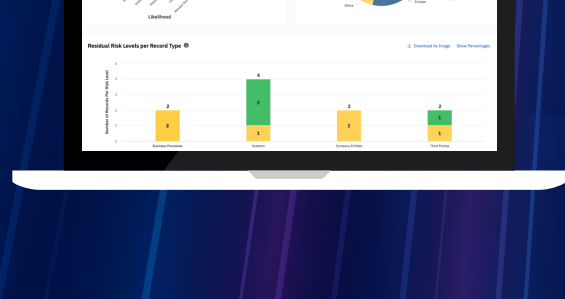
**Your incident response plan should include:**

- ➔ Roles and escalation paths
- ➔ Decision-making authority
- ➔ Documentation standards
- ➔ Communication templates
- ➔ Annual simulations and scenario planning



**Don't improvise when the stakes are high. Prepare. Practice. Protect.**

## Respond Faster. Stress Less.



**TrustArc's Data Mapping & Risk Manager** helps you automate, assess, and act before small issues become big breaches.

**REQUEST A DEMO**

Want more privacy power moves? [Explore the full Privacy PowerUp Series](#) for infographics, articles, and videos that put you in control.