Updates
April 12, 2018

6 Ways to Improve Your Incident Response Plan for GDPR

The *General Data Protection Regulation* (*GDPR*), which is effective May 25, 2018, requires notification to European regulators within 72 hours of the discovery of many types of data breaches. This deadline requires speed and organization that no other jurisdiction currently requires, especially in the United States. Organizations that hold personal data of EU residents and do not have an incident response plan should promptly develop one so they can comply with the GDPR's requirements.

But what if you already have a plan? It likely does not have key elements needed to comply with the GDPR's requirements, including the accelerated timeline. We pose six key questions that highlight recommended areas to review, revise and test before GDPR becomes effective in May.

1. What is an "incident"?

Many incident response plans are triggered when data has been accessed or acquired without authorization—those incidents that traditionally required notification or signal corporate espionage. But GDPR goes beyond that. Companies must be prepared to evaluate, respond to, and document all incidents that involve "accidental or unlawful ***destruction***, ***loss***, ***alteration***, unauthorized disclosure of, or access to" personal data. Destruction, loss, and alteration now need to be on your radar and trigger your incident response process. Note that even *temporary* loss, such as during a ransomware attack where data is later restored from backup, is considered a breach under this definition and must be treated accordingly.

Also check that your plan is not limited to incidents involving "unencrypted" data (the concern of many U.S. state laws). Under GDPR an incident that involves encrypted data is still a "data breach" that must be documented, even if there is no reason to believe that data itself was exposed.

2. How fast do you move?

Controllers must report security incidents that involve personal data of EU residents (unless exceptions apply) to data protection authorities as soon as possible and not later than 72 hours. Processors must also promptly report breaches to their controllers—and the controllers then have the same 72-hour period to evaluate the incident to determine if they must report to the supervisory authority. These thresholds are considerably more strict than any U.S. jurisdictions, or any other jurisdictions that previously had requirements worldwide, and will require careful planning in order to meet.

In order to make these notifications effectively—and understand if you must make them at all—your plan needs to allow for quick escalation and decision making. Issues to consider include the following:

- How quickly does an incident go from detection to analysis?
- Does your plan identify 24-hour contact information for key incident response team members, and their backups?
- Does your investigatory lead have the tools to quickly vet and investigate incident reports concerning the most likely types of incidents to hit your organization?
- Do you know who on your team will analyze the legal notification requirements, decide whether notification is required and draft the notification?

- If your plan operates differently depending on the significance of the incident, will small and relatively lower risk incidents get the attention they need to make a report in 72 hours?
- How quickly can you determine where affected individuals live (and therefore what legal regime will apply to your notice)?

3. What personal data triggers notification?

In the United States, an incident triggers notification only if certain specific types of personal data are implicated. Many of these information types—social security numbers, financial account numbers, passwords—are often segregated from other data. It can therefore often be fairly easy to determine promptly whether those types of information are involved and notice is required.

But GDPR regulates all personal data—all data concerning an identified or identifiable individual. Any incident involving personal data, from names to IP addresses to nationality to national ID numbers, is a data breach under the regulation. Only those incidents that might cause harm to data subjects must be disclosed, but all incidents must be tracked and analyzed.

Review the portion of your plan that addresses notification, and analyze how team members identify incidents as potentially triggering notice. Ensure that incidents are not excluded from the identification process based on the types of personal data that may have been exposed, without reference to the residence of the data subjects.

4. What do you need to know to make a notice decision?

Under GDPR, it is critically important to understand as quickly as possible the incident and its potential impact. This is not just a question of acting quickly, as described above, but also ensuring that the incident response team looks for the right kinds of information.

Regulators must be notified unless an incident is "unlikely to result in a risk to the rights and freedoms of natural persons." This is a wide-ranging inquiry, but it should take into account whether the data was encrypted or otherwise protected, the volume of data exposed, the type of data and data subjects involved, and the potential consequences of the incident. As a result, to the extent your plan highlights key questions, ensure that the list is comprehensive enough to support a GDPR-style risk analysis.

5. Whom should you notify?

If you are processing another company's data, GDPR requires you to tell that company about the incident as soon as possible, and the company's 72-hour reporting clock will start to run as soon as you report the incident. While processors commonly have an obligation to tell the controller of an incident (this is an obligation under U.S. state laws, as well as commonly in contracts), controllers must be able to reliably receive, assess and act on these reports more quickly than ever before.

Under the GDPR, a controller must notify the regulatory authority, not the affected individuals, first. Moreover, unlike in the United States, where the test for notifying a regulator is whether individuals in a given state are being notified, the GDPR expects that there will be situations where a regulator must be notified but individuals need not be: EU regulators must be notified of all security incidents unless harm to the data subjects is unlikely, while the data subjects themselves must be notified only if the incident is likely to result in a high risk to the rights and freedoms of data subjects.

If your plan has a section regarding specific legal requirements and contacts, GDPR requirements need to be added. In addition, check for any assumptions within the rest of the plan regarding how notice will proceed and to whom to ensure your plan covers your potential GDPR obligations.

6. Are you recording all breaches?

Under GDPR, data controllers must document each data breach, its effects and remediation, regardless of whether the controller reports it to the supervisory authority. In other words, all incidents that affect personal data must be documented, in a form that can later be demonstrated to a regulator. Thus, not only must the incident-reporting funnel ensure that all incidents are covered by the incident-response process, but the outcome of each incident must be an entry in the ongoing record. This entry should reflect the final outcome of the investigation, rather than the investigative record itself.

GDPR becomes effective on May 25, 2018. Its penalties for noncompliance can be severe. Given the quick action required under the new regime, companies are well served to review their incident response plans and related procedures now.

Authors

Todd M. Hinnen

Partner
THinnen@perkinscoie.com 206.359.3384

Amelia M. Gerlicher

Partner
AGerlicher@perkinscoie.com 206.359.3445

Explore more in

General Data Protection Regulation (GDPR) Privacy & Security Technology Transactions & Privacy Law Communications Retail & Consumer Products

Related insights

Update

CFPB Finalizes Proposed Open Banking Rule on Personal Financial Data Rights

Update

FDA Food Import and Export Updates for Industry