Legal Incident Response

What's Truesec Legal Incident Response?

When disaster strikes, many different workstreams are kicked into gear, with cybersecurity often being the primary focus. However, the legal perspective (e.g., GDPR) has become critical for mitigating and managing regulatory, contractual, and financial risks while interacting in a customer-focused and socially responsible manner.

When an organization suffers a breach, for example, after sending an email to the wrong recipients, losing a laptop, having a server break down, or being the victim of a ransomware attack, personal data is often affected. Such organizations have to investigate whether the security breach constitutes a personal data breach that needs to be notified to supervisory authorities and communicated to the victims.

Truesec's Legal Incident Response team helps you navigate legal and contractual obligations, contact and correspond with lawyers in affected countries, contact and correspond with competent authorities, etc. Our focus in this work is to relieve you of the regulatory and contractual burden to minimize legal risks and let you focus on returning your business to a new steady state. We then provide you with a legal expert to stand in your corner, who can advise you on what steps should be taken, when, and how. This legal expert advises you and ensures the required information is investigated and substantiated and that completed notifications are sent to the correct authorities.

Legal Incident Response will provide you with:

- Investigated, substantiated, and completed notifications (preliminary and supplementary).
- Communication with affected persons in accordance with legal requirements.
- Final documentation prepared in accordance with legal requirements.
- Any preventative and other measures deemed necessary to strengthen privacy and security posture.

Who It's For

All organizations with employees, customers, partners, website visitors, etc., from the EU are subject to the GDPR. In the event of a personal data breach, this must be managed correctly. Some incidents must be reported to competent supervisory authorities, in the correct manner, within the correct time. Some incidents also require you to inform affected persons. All of this should be documented correctly to explain what has happened, what has been done, what measures have been undertaken to prevent a recurrence, etc.

Our primary focus is to help your organization ensure you are prepared and assist with the actual handling of personal data incidents and post-incident follow up.

About Us

As a global cybersecurity company, we're proud to be at the forefront of protecting organizations and our society against cyber threats. Our purpose has been clear since day one: Creating safety and sustainability in a digital world by preventing cyber breach and minimizing impact. We never cease to challenge and reinvent ourselves to help defend your most valuable data assets every day.

TRUESEC

A Safe Digital Future

Contact Us

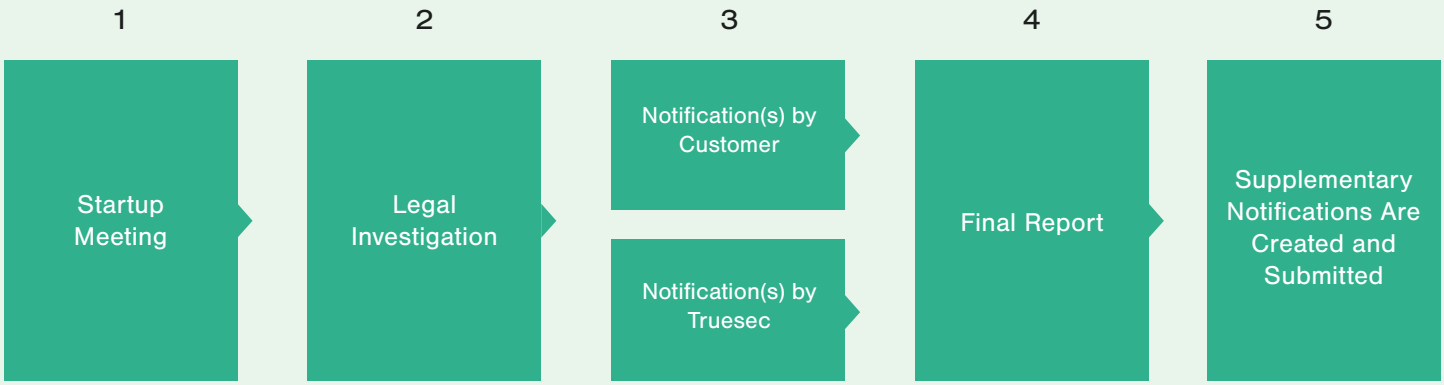
truesec.com hello@truesec.com

The Truesec Promise

We always strive for the best results for our customers.
That's a Truesec promise.

Methodology

When you contact Truesec, we gather the appropriate experts and follow our proven workflow. This includes, among other things, the following steps:



1. Startup Meeting

At this meeting, we'll ask you some questions to gather and establish facts. These may include:

- What type of data is stored in the affected system(s)?
- Who has been affected?
- Why has this data been stored?
- Where are the data and the affected individuals geographically located?

2. Legal Investigation

Truesec conducts a legal investigation and assessment to determine if there is a risk to the data subjects' freedoms and rights. If such a risk is likely to exist, the personal data incident must be reported to a supervisory authority. If there is a high risk, the person must also be informed in accordance with specific regulatory requirements.

The assessment is undertaken to determine, for example, who determines the purposes and means of the processing of the affected personal data, where the affected data subjects are located, where the affected personal data is stored, and where the organization has its primary place of business. Answering these questions clarifies, among other things, questions regarding geographical scope, the severity of potential risks, which supervisory authority is deemed competent to receive notification(s), if and how data subjects shall be informed, etc. In addition, it clarifies who is deemed to be the data controller and, if your organization is deemed to be the processor, who you must inform.

To ensure that the provided advice is correct, and that the process is moving forward as safely and quickly as possible, Truesec Cyber Law works in close collaboration with the Incident Response team's experts in cybersecurity, crisis management, and crisis communication. To provide global coverage, Truesec Cyber Law also works in close collaboration with law firms that specialize in data privacy and data breach response.

Contact Us
truesec.com
hello@truesec.com

The Partnership

We see our work with our customers as a partnership.
We work together to get the best results and prevent incidents.

3. Notification(s) to Competent Supervisory Authority(ies)

This can be done in one of two ways: Either you prepare and submit the notification(s) following the investigation, or as is most often preferred by our customers, we prepare and submit the notification(s) on your behalf.

4. Final Report

When the investigations and legal reviews are completed, a final report on the personal data incident is created. This report sets forth relevant facts regarding the incident, its effects, and remedial actions taken to constitute such documentation that is required under the GDPR.

The final report can also be used by management to provide insight into the legal readiness and posture of the organization.

5. Supplementary Notifications

If preliminary notifications are provided initially, supplementary notifications are drafted and submitted on your behalf.

How To Obtain the Benefits of Legal Incident Response

If you have an ongoing personal data breach, contact us immediately! Legal advice should be obtained promptly to mitigate the risk of administrative sanctions, supervisory measures and sanctions, claims from data subjects, and litigation risk.

If you would like to begin your journey to increase your legal readiness and strengthen your posture regarding personal data in general and legal incident response specifically, then start by talking to your sales contact or any of our experts. Together we can determine your next step and investigate whether there are some quick wins that we can accomplish together today.