How to Report a Data Breach as per GDPR?

VISTA INFOSEC®
TRUSTED ADVISORS ASSURED COMPLIANCE

The General Data Protection Regulation (GDPR) Act is a broad set of data privacy rules that define how an organization must handle and protect the personal data of citizens of the European Union (EU). The Regulation also outlines the way a personal data breach must be handled and reported.

Articles 33 and 34 outline the requirements for breach notification, however, most businesses are still unaware of their responsibilities. Details, such as what an organization should report, when, and to whom it should be reported, and what should be included in the breach notification are some of the major aspects that businesses overlook. This negligence can result in substantial fines.

As a Data Controller (the business that stores, or handles data), the business has several key responsibilities, including taking necessary measures, notifying concerned authorities and affected individuals in an event of a data breach. Let's first understand what a personal data breach is, as per the GDPR Regulation.

What is a Personal Data Breach?

GDPR Regulation is a data privacy law established to protect the personal data of citizens of the EU. Technically, the applicability of the GDPR breach notification requirements apply to only the personal data breached. For a better understanding, let us break down the term "personal data breach" into two parts.

According to GDPR, "personal data" can be defined as any information that relates to a natural identifiable person, such as their name, contact details, or health records, and similar identifying information, specifically of the citizens of the EU. A data breach is an event that results in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access of personal data. A data breach often occurs when an unauthorized individual or a cyber-criminal gets access to an organization's database, whether through intrusion, or due to the negligence of an employee handling sensitive personal data.

GDPR contemplates a personal data breach as an incident that eventually results in the accidental loss or destruction of data, or unauthorized disclosure, alteration, or unauthorized access to personal data of citizens of the EU.

Whatever the reason or cause of a data breach, the incident that puts the consumer's rights, privacy, and freedom at risk, and violates the trust between an organization and its users, will result in regulators taking action against the organization.

When should a Data Breach be reported?

While it is important that the data breach incident be reported, it is also essential for organizations to understand that not all information security incidents are classified as a personal data breach. Since a breach may, "if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned", as listed in Recital 85 of GDPR, the incident needs to be reported. The organization must report data breaches to the authorized supervisory authority within 72 hours of becoming aware of the incident.

Who should be reported about the Data Breach?

Once the incident is identified as a personal data breach, organizations are required to report the breach to the relevant supervisory authority, in accordance with Chapter 6.

If a company has no officially established presence in the EU, but still suffers an incident involving EU citizen data, then it must inform the local supervisory authorities of every Member State in which they are active, and which is affected by the incident. As stated previously, organizations are required to inform within 72 hours of becoming aware of the breach incident.

After notifying the supervisory authority, the organization must also inform all affected individuals. At the very least, they should issue a statement that lets them know that an incident has occurred. Although not specifically codified in the regulation, an organization can demonstrate extra transparency by setting up a web page and helpline for people to contact your organization to find out more and have their questions answered about the incident.

What to report in a Data Breach as per GDPR?

While the organization must notify the relevant supervisory authority and the affected individuals, it is also important to include necessary information concerning the data breach incident. Some of the details that should be included in the data breach notification include:

- When the breach incident occurred, and how was it discovered.
- The categories or types of personal data that were affected.

- The severity of the breach both in terms of records lost and the number of people affected.
- The potential impact of the breach on data subjects.
- The impact to the organization in terms of services provided to users.
- Recovery time from the impact of the data breach.
- Measures taken to remediate and prevent such an incident in the future.
- Name and contact details of the Data Protection Officer (DPO) for obtaining further information about the breach incident.

It is important to note that when informing the people affected by the incident, organizations are required to share details, such as describing the nature of the personal data that was breached, and recommendations for the impacted person to mitigate the potential harm of the incident. Again, depending on the industry, reporting breach incidents under the GDPR will also mean reporting the incident under other data protection regulations such as HIPAA, PIPEDA, or other local regulations, which should also be considered.

Conclusion

Following the Breach Notification rules as outlined in the GDPR is essential for every organization. While that does not lower the consequences of the incident, it definitely helps in reducing the impact of the incident, or escalation of the incident. Organizations can look at it in a way to lower the risk involved in personal data breaches.

While the regulators understand that there cannot be a complete investigation of the personal data breach within 72 hours, hence, Article 33(4) allows organizations to provide the required information in phases, without any undue further delay. However, organizations are also expected to expedite the process, prioritize the investigation, and submit further information at the earliest possible time. If all the details cannot be provided within 72 hours, the organization will have to give a valid reason for the delay, and provide a time frame for submitting more information.

Orginally published on:- Tripwire

Written By:- VISTA Infosec

Do write to us your feedback, comments and queries or, if you have any requirements:
info@vistainfosec.com

You can reach us on:

USA +1-415-513 5261 | INDIA +91 73045 57744 | SINGAPORE +65-3129-0397 | UK +442081333131