Publications
April 11, 2018
GDPR Data Breach Notification Requirements

Requirements of General Data Protection Regulation (GDPR)

Regulation (EU) 2016/679, Arts. 33-34.

Effective May 25, 2018

Application. Any person or entity (collectively, Entity) that is established in the European Union or processes the personal data of EU residents when offering them goods or services.

- The provisions regarding data breaches apply to both controllers and processors of personal data of EU residents.

Security Breach Definition. A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

- Unlike in the United States, an incident may qualify as a "data breach" without triggering notification to either individuals or a regulatory body.

Supervisory Authority Notification Obligation. The controller shall notify its lead supervisory authority of the data breach.

- An Entity is not required to notify the supervisory authority of the data breach if the breach is unlikely to result in a risk to the rights and freedoms of natural persons.

The notification to the supervisory authority shall include:

- the nature of the personal data breach, including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
- the name and contact details of the data protection officer or other contact point where more information can be obtained;
- the likely consequences of the personal data breach; and
- the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Third-Party Notification Obligation. A processor shall notify the data controller of any data breach without undue delay.

Data Subject Notification. The controller must notify data subjects of the data breach when it is likely to result in a high risk to the rights and freedoms of natural persons.

Notification is not required if either of the following are true:

1. the controller has implemented appropriate technical and organizational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorized to access it, such as encryption; or

2. the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialize.

Timing of Notification. The notification to the supervisory authority shall be made without undue delay and, where feasible, not later than 72 hours after having become aware of it. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

Notification to data subjects must be made without undue delay.

Personal Information Definition. Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Data Subject Notice Form and Content. The regulation does not specify required methods of notification, only that the information be communicated directly to data subjects. Acceptable communication methods include direct messaging (e.g., email, SMS, direct message), prominent website banners or notification, postal communications and prominent advertisements in print media.

The notice must be in clear plain language and contain at least the following:

- The nature of the data breach;
- The name and contact details of the data protection officer or other contact point where more information can be obtained;
- The likely consequences of the personal data breach; and
- The measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Substitute Notice Available. If direct notification to data subjects would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

Documentation Requirement. The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this article.

Authors

Explore more in

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