Bloomberg Law®

Privacy and Security Law Report®

Data Breaches

A Primer on Personal Data Breach Reporting Under the European Union's General Data Protection Regulation

Data Breach Response

Under the new European Union privacy regime, the General Data Protection Regulation, a data controller must notify the competent regulator and a data processor must notify its data controller of a personal data breach without undue delay and where feasible not less than 72 hours after becoming aware of the breach, so processors and controllers in the U.S. that have cybersecurity insurance should ask their insurance brokers about endorsements that address the areas of exposure presented by the GDPR, the author writes.

By Melissa Krasnow

This article concisely describes personal data breach reporting by data processors and data controllers under the European Union's General Data Protection Regulation (GDPR) in the wake of the Article 29 Data Protection Working Party Guidelines on Personal data breach notification under Regulation 2016/679 adopted on Oct. 3, 2017 and as last revised and adopted on February 6.

Data processors and data controllers in the U.S. that have cyber liability insurance or are contemplating the purchase of cyber liability insurance should ask their insurance brokers about endorsements that address the areas of exposure presented by the GDPR.

Melissa J. Krasnow is a partner with VLP Law Group LLP, in Minneapolis, Minn., and practices in the areas of domestic and cross-border privacy and data security, technology transactions, and mergers and acquisitions. Krasnow is a Certi##64257;ed Information Privacy Professional/US and a National Association of Corporate Directors Board Leadership Fellow.

Personal Data Breach Reporting By a Data Processor and GDPR Definitions A data processor must notify the data controller without undue delay after becoming aware of a personal data breach. Art. 33(2). Data processor means a person that processes personal data on behalf of the data controller. Art. 4(8). Data controller means a person which, alone or jointly with others, determines the purposes and means of the processing of personal data. Art. 4(7). Personal data breach means 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. Art. 4(12). Personal data means any information that relates to an identified or identifiable living individual; 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. Art. 4(1). Processing means any operation or set of operations performed on personal data or on sets of personal data, whether by automated means. Art. 4(2). Data subject means a natural person to whom the personal data relates. Art. 4(1).

 ISSN 1538-3423

Personal Data Breach Reporting By a Data Controller

A data controller must notify the competent supervisory authority of a personal data breach without undue delay and where feasible not less than 72 hours after the data controller becomes aware of the personal data breach, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Art. 33(1).

When a data controller assesses the risk that is likely to result from a breach, the data controller should consider a combination of the severity of the potential impact on the rights and freedoms of individuals and the likelihood of these occurring. As noted in the Guidelines, the European Union Agency for Network and Information Security (ENISA) has issued recommendations for a methodology of assessing the severity of a breach, which data controllers and data processors may find useful when designing their breach management response plans.

The data controller should consider the following criteria when assessing the risk to individuals as a result of a breach:

- the type of breach that has occurred;
- the nature, sensitivity and volume of personal data;
- the ease of identification of individuals;
- the severity of consequences for individuals;
- special characteristics of the individual;
- special characteristics of the data controller; and
- the number of affected individuals.

In the first notification, the data controller should inform the supervisory authority if the data controller does not have all the information required for reporting and subsequently will provide more details. Art. 33(4). If it is not possible to provide the information required for reporting at the same time, the information may be provided in phases without undue further delay. Id.

When the notification by the data controller to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay, which is permissible if the data controller provides reasons for the delay. Art. 33(1) and . However, delayed notification should not be viewed as something that regularly takes place.

If in doubt, the data controller should err on the side of caution and notify. Id. There is no penalty for reporting an incident that ultimately transpires not to be a breach. Id.

The information required for reporting includes the name and contact details of the data protection officer or other contact point where more information can be obtained and a description of:

- the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and of personal data records concerned;
- the likely consequences of the personal data breach; and
- the measures taken or proposed to be taken by the data controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects. Art. 33(3).

In certain circumstances, where justified, and on the advice of law enforcement authorities, the data controller may delay communicating the breach to the affected individuals until such time as it would not prejudice such investigations. However, data subjects would still need to be promptly informed after this time. Recital 88.

A data controller must communicate the personal data breach to the data subjects without undue delay when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons and the data controller has not either:

- implemented appropriate technical and organizational protection measures which were applied to the personal data affected by the personal data breach and render the personal data unintelligible to any person who is not authorized to access it (e.g., encryption) or
- taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialize. Art. 34(1) and Art. 34(3).

Where such communication of the personal data breach to the data subjects would involve disproportionate effort, there instead shall be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

The communication must describe in clear and plain language the nature of the personal data breach and include the name and contact details of the data protection officer or other contact point where more information can be obtained and a description of:

- the likely consequences of the personal data breach; and
- the measures taken or proposed to be taken by the data controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects. Art. 34(2) and Art. 33(3).

There is a high risk to the rights and freedoms of individuals where the breach:

- may lead to physical, material or non-material damage for individuals whose data have been breached and such damage includes discrimination, identity theft or fraud, financial loss, damage to reputation, loss of control over personal data or limitation of rights, unauthorized reversal of pseudonymization, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned. Recital 75 and Recital 85; and
- involves personal data that reveals racial or ethnic origin, political opinion, religion or philosophical beliefs, or trade union membership, or includes genetic data, data concerning health or data concerning sex life, or criminal convictions and offenses or related security measures. Id.

The data controller must document any personal data breaches, comprising the facts relating to the personal data breach (including its causes, what took place and the personal data affected), its effects and consequences and the remedial action taken by the data controller. Art. 33(5). It also is recommended that the data controller document its reasoning for the decisions taken in response to a breach.

Annex A to the Article 29 Data Protection Working Party Guidelines is a flowchart showing notification requirements and Annex B to the Guidelines provides examples of different types of breaches involving risk or high risk to individuals.

BY MELISSA KRASNOW

To contact the editor responsible for this story: Donald Aplin at daplin@bloomberglaw.com

  PVLR ISSN 1538-3423