BCLP. Client Intelligent

Insights

DATA BREACH LITIGATION PREPARATION: HOW DO EUROPEAN UNION BREACH NOTIFICATION REQUIREMENTS DIFFER FROM THE U.S.?

Feb 06, 2020

As of January 1, 2020, California became the first state to permit residents whose personal information is exposed in a data breach to seek statutory damages between $100-$750 per incident, even in the absence of any actual harm, with the passage of the California Consumer Privacy Act ("CCPA"). The class actions that follow are not likely to be limited to California residents, but will also include non-California residents pursuing claims under common law theories. A successful defense will depend on the ability of the breached business to establish that it implemented and maintained reasonable security procedures and practices appropriate to the nature of the personal information held. The more prepared a business is to respond to a breach, the better prepared it will be to defend a breach lawsuit. To help our clients prepare for the CCPA, Bryan Cave Leighton Paisner is issuing a series of data security articles to empower organizations to focus on breach readiness.

Communications with Supervisory Authorities and Individuals in the European Union

The General Data Protection Regulation ("GDPR") is a bit like the U.S. breach notification laws on steroids. The GDPR applies to establishments in the EU (*e.g.,* a retailer has stores located in the EU) as well as to companies outside the EU that "offer goods or services" to people located in the EU (*e.g.*, a U.S. company selling tours of New York City to people in France) or to companies that monitor the behavior of people in the EU. If your company is regulated by the GDPR and you suffer a data breach, it is important to understand the ways in which the GDPR differs from U.S. breach notification laws.

First, the definition of "personal data," the EU-equivalent of what the U.S. laws refer to as Personally Identifiable Information ("PII"), is much broader. Article 4 states that "'personal data' means any information relating to an identified or identifiable natural person ('data subject')" – and it means *anything*, including identifiers that you might not expect, like personal IP addresses or business contact information.

Second, the definition of data breach also is broader. Like its U.S. counterparts, the GDPR applies where personal data is accessed by or disclosed to an unauthorized third-party, known as a confidentiality breach.

Unlike its U.S. counterparts, the GDPR also requires notification to impacted individuals if personal data is inadvertently lost or destroyed such that a person may no longer have access to it – referred to as an availability breach. It also applies if personal data is inadvertently altered or modified so that it is no longer accurate – referred to as an integrity breach. As a result, if a situation arises in which data is destroyed or altered, notification may be required pursuant to the GDPR *even if* the data was not accessed or acquired by an unauthorized party – a result that would not be required under current U.S. laws.

If your organization is regulated by the GDPR, you may have notification obligations if you are serving as a processor of personal data for another company, or if you are a joint controller.

While the definitions under the GDPR are more expansive than U.S. law, the GDPR does not require notification in the event of every breach. Instead, notification to the supervisory authorities – the EU regulators – must be made only if the breach results in a risk to the rights and freedoms of individuals. If notification is required, the breach must be reported to the relevant supervisory authorities within 72 hours of becoming aware of it. This is the opposite of U.S. law, which requires regulator notification only if individuals will be notified.

In contrast, in the EU, the standard for notification to the individuals themselves is higher – the breach must result in a "high risk" to the rights and freedoms of individuals, and the 72-hour requirement does not attach to individual notice. Instead, the GDPR recognizes that notification to the individuals likely will take longer, and it requires that communication to impacted individuals should be made as soon as reasonably feasible.

If a company is required under the GDPR to notify individuals of a data breach, the communication should describe in clear and plain terms and in the native language of the recipient the following:

1. A description of the nature of the breach;

2. The name and contact details of a data protection officer or other contact point;

3. A description of the likely consequences of the breach; and

4. A description of the measures taken or proposed to be taken by the controller to address the breach, including, where appropriate, measures to mitigate its possible adverse effects.

Should an organization decide notification is not required, the GDPR provides that the breach be documented in the company's records. Since the GDPR took effect on May 25, 2018, supervisory authorities in the various EU member states have seen an influx of breach reporting by companies. How regulators will enforce compliance, particularly against companies lacking an EU physical

presence, remains to be seen. Regardless, organizations subject to its jurisdiction are well advised to ensure that the GDPR is closely analyzed in the event of a breach.

Breaches Outside the US or EU

Other countries are increasingly regulating the use and unauthorized disclosure of PII or personal data. Brazil, for example, recently enacted its own legislation parallel to the GDPR which contains breach notification requirements. Canada recently expanded its data security laws to include additional breach notification requirements. If your organization does business in multiple countries, you should review the laws of those countries and include the timing and notification requirements in your organization's incident response plan.

For additional information, BCLP's Data Security Breach Handbook provides a comprehensive guide on how to respond when a breach happens and how to prepare your organization before one occurs. Click here for the handbook. BCLP is working with clients to assess – and mitigate – risks by putting in place the policies, procedures, and protocols needed to address data security breach issues.

For more information and resources about the CCPA visit http://www.CCPA-info.com.

RELATED PRACTICE AREAS

- Data Privacy & Security
- California Consumer Privacy Act

MEET THE TEAM

Linda C. Hsu

Los Angeles

linda.hsu@bclplaw.com
+1 310 576 2192