ALSTON & BIRD

WWW.ALSTON.COM

Privacy & Data Security ADVISORY ■

DECEMBER 3, 2020

Breach Notification in the EU and U.S.: Practical Implications of 5 Key Distinctions

***by* Wim Nauwelaerts, Kim Peretti, *and* Nameir Abbas**

The state of California passed one of the first breach notification laws in the early 2000s, and since that time every U.S. state has passed some form of breach notification law. These laws generally require notification to the individuals affected by a data breach as well as potentially a state regulator. While there are some nuances and key differences, the information covered, triggers for reporting, threshold for regulatory reporting, and timing and content of notifications are generally consistent.

On the other hand, the EU General Data Protection Regulation (GDPR) became effective in 2018, introducing the EU's first unitary standard for breach notification. In broad strokes, the GDPR contains similar obligations for breach notification, but differences in the triggers and thresholds for notification, required timing of notification, and regulatory landscape have important implications for how companies may want to handle a data breach. Furthermore, trends over the past two-plus years suggest that companies are still adjusting to GDPR requirements, with breach reports generally trending downward over time as companies become more comfortable navigating notification thresholds and analyses.

Five key distinctions between the U.S. state data breach notification regimes and the GDPR could drive differences in a company's investigation and notification approach (though of course there are other, sector-specific notification requirements in both the U.S. and the EU that are not as wide-reaching).

Key Distinctions

1. Data elements that trigger notification

U.S. state data breach notification laws are generally triggered by a compromise involving an individual's name in combination with specified data elements, including sensitive data elements such as Social Security numbers, driver's license or state identification numbers, or financial account information. While this list of data elements has expanded over time as states amend their laws – for example, to include some form of health or medical information in over 20 states – it is not nearly as broad as the analogous GDPR definition of "personal data."

GDPR breach notification requirements are triggered by a personal data breach, and "personal data" is defined as "any information relating to an identified or identifiable natural person." Unlike the U.S. state-law definitions, this could cover data elements such as email addresses or other forms of contact information relating to an individual.

Notably, countries in other parts of the world that have passed breach notification legislation generally follow the GDPR approach, triggering potential notification requirements based on a broad definition of "personal data" or "personal information."

This difference in scope has important consequences beyond just the types of data elements that could trigger a notification obligation and could impact the focus of the investigation. For an incident that occurs in the U.S. and impacts only U.S. residents, determining whether any of the impacted personal information could trigger a breach notification obligation is often a priority, placing the focus on the forensics to determine what types of personal information could have been impacted. For incidents in which the GDPR and its broad definition of personal data is in scope, this initial analysis may be quicker, placing more of a focus on the threshold for notifying. Of course, as a practical matter, companies in the U.S. at times make "courtesy" notifications for certain types of data breaches when the state breach notification laws are not technically triggered (e.g., breaches involving email addresses and other contact information), though the increasing risk of litigation (in particular with the California Consumer Privacy Act) could make this less likely going forward.

2. The extent to which the legal threshold for notifying is an evolving standard

In the U.S., notification requirements could be triggered if there has been a breach of personal information. The definition of "breach" varies by state, but the most common formulations include either "unauthorized access" or "unauthorized acquisition." Furthermore, for many but not all U.S. states, notifications are only required if a certain risk-of-harm threshold has been met. The exact formulation of this risk-of-harm threshold varies by state but generally ties back to the risk of misuse of the information or of harm to the individual. For both the definition of breach and risk-of-harm provisions, there has been minimal guidance from state regulators and no case law, and there is little in the way of cultural norms or expectations that factor into the analysis.

On the other hand, GDPR breach notification requirements could be triggered by any "personal data breach," meaning "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data." Unlike the U.S., data protection regulators in the EU have provided extensive guidance on breach notification obligations, making clear that companies need to have a broad conception of what qualifies as a reportable breach (consistent with this definition). For example, the European Data Protection Board has indicated that "destruction" occurs when the impacted data "no longer exists or no longer exists in a form that is of any use to the controller"; "damage" occurs when the impacted data "has been altered, corrupted, or is no longer complete"; and loss occurs when the controller "has lost control or access … or is no longer in possession" of the data.

Furthermore, unlike the U.S., the GDPR incorporates two risk-of-harm thresholds. Notification to a data protection authority is always required "*unless* the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons," and notification to affected individuals is required *only if* a breach is likely to result in a *high* risk to the rights and freedoms of natural persons. In addition to these thresholds, cultural norms and regulatory expectations that vary by EU Member State could factor into the decision whether or not to notify.

Like the differences in the definition of "personal information" and "personal data," the varying U.S. and EU thresholds for notification could impact the focus of an investigation. In the U.S., where the definition of breach is more discrete, there may be more of an emphasis on assessing whether an "access" or "acquisition" has occurred from a forensic perspective. On the other hand, the analysis of risk of harm may be comparatively concrete, focusing more on defined risks to the individual – for example, whether a criminal actor was involved. In the EU, where breach notifications are still relatively new, the decision of whether to notify could be more complex because there are more types of

incidents that could result in a notification obligation, the risk-of-harm provisions are less concrete, and there is more (and potentially shifting) regulatory guidance to take into account.

3. The application of privilege

The application of attorney-client privilege and work product privilege in forensic investigations in the U.S. remains in flux. That said, years of litigation have provided a general framework for lawyers and companies to follow in their efforts to manage investigations in a privileged fashion.

On the other hand, EU concepts of privilege in this context could vary meaningfully by EU Member State and are often less well-developed than in the U.S. These distinctions are most likely to have practical consequences in a regulatory inquiry, particularly for a data breach. A regulatory authority may decide to request a copy of the forensic investigation report, forcing the company to decide whether to provide the report or claim privilege instead. Declining to provide the report could be more difficult in a jurisdiction with weaker or less developed privilege protections. Depending on the jurisdiction, this risk of disclosure of a forensic report could be a factor in assessing how to engage and manage a third-party forensics firm in connection with an investigation.

4. The relationship with the regulator to be notified

The regulatory landscape also varies significantly between the U.S. and the EU. In the U.S., while each state has a data breach notification law, the laws are enforced by the state attorney general and not a regulator that focuses exclusively (or even primarily) on data protection. And while the landscape is shifting, these regulators do not generally conduct data protection audits or have ongoing relationships with companies subject to their jurisdiction. In the EU, GDPR breach notifications are made to a supervisory authority that specifically regulates data protection. In some ways, these supervisory authorities function similarly to financial regulators in the U.S. They are more likely to conduct audits or reviews of companies – often triggered by a data incident – and to have a preexisting relationship that deal with data protection specifically.

This difference in relationship could be an important factor in making notification decisions. For example, companies may be more likely to notify a data protection authority with whom they have an ongoing relationship, particularly in situations where there is some legal ambiguity around whether notification is required. Also, if the GDPR's "one stop shop" applies to them, companies in the EU that have experienced a cross-border breach may need to notify their "lead" supervisory authority. For these companies, it will be key to determine beforehand (e.g., in their breach response plan) which supervisory authority is their lead authority for notification purposes. In contrast, in the U.S., there is no concept of a lead supervisory authority, and notification to several state AGs is expected in most large reportable data breaches. These differences – i.e., the existence of an ongoing regulator relationship and the expected interaction with one or many regulators – are significant factors in shaping a company's regulatory response to data breach incidents.

5. Timing

The GDPR requires companies to notify the relevant data protection authority within 72 hours of becoming "aware" of a breach. Guidance from the EU data protection authorities makes clear that the standard for awareness is relatively low – it is simply the point at which the "controller has a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised," subject to a "short period of investigation" when a security incident is first detected. This interpretation is subject to the general requirement that the GDPR requires the implementation of "appropriate technical protection and organizational measures to establish immediately whether a breach has taken place," and the test of awareness is more generally dependent on the "circumstances of the specific breach." "Prompt action to investigate an incident" to determine whether personal data has been breached is also a key element of compliance.

In the U.S., on the other hand, while 30 days is generally considered to be a reasonable standard for notification, most states do not have a have a specific timing requirement, and those states that do have a specific timing requirement vary meaningfully (e.g., 30 days after the determination that a breach has occurred for Florida, but 60 days in Delaware). Furthermore, with the exception of specific sectoral laws (e.g., the New York Department of Financial Services cybersecurity regulations), no state has a notification timeline as short as 72 hours (or even close).

The GDPR's 72-hour requirement poses many practical challenges. It would be difficult to gain certainty about a more complex breach in such a short timeframe, and risk-averse companies may instead find themselves notifying appropriate parties of data incidents that at first sight do not appear to meet the GDPR's notification requirements. Although this practice is increasingly being discouraged by EU data protection authorities, these companies choose to notify out of an abundance of caution rather than a firm belief that a breach has occurred in order to preemptively satisfy the 72-hour timing requirement. Some of these reported breaches may end up being a non-issue, with forensic evidence later confirming that there was no impact to personal data. In that case, the notification may have to be revoked or amended.

For many, the rapid timing requirement fosters a conservative approach to notification, forcing companies to commit significant resources early in an investigation to assessing whether to notify and to actually making the notification. This quick decision making may also result in companies making preliminary notifications and later updating the data protection authority with additional details, an approach that is not common in the U.S., where companies generally have more time to investigate and determine whether notification to regulators (and which regulators) is required.

Practical Takeaways for Developing a Global Notification Approach

The differences between U.S. state data breach notification laws and the GDPR do not just represent differing compliance burdens. More importantly, they could weigh in favor of a different approach to investigation and could drive diverging U.S. and EU approaches to notification for the same incident, requiring companies to take into account distinctions in the types of information, incidents, and risks to affected individuals that trigger notification obligations. Similarly, differences in privilege and the regulatory landscape could factor into how companies handle investigations – e.g., whether they request a report from a third-party forensics firm – and how companies assess their notification obligations – e.g., whether they conservatively notify a data protection authority or decide not to notify based on an assessment of the risks to affected individuals. Of course, companies might instead prefer to take a single approach for all impacted jurisdictions, even if notifications are not technically legally required across the board.

Taking proactive steps to plan for global incidents can help smooth out any response to a live incident. Steps to consider include:

- Revising your incident/breach response plans or procedures to highlight cross-border differences in the legal landscape and how those differences might require different handling of security incidents within the scope of U.S. state data breach notification statutes and the GDPR.
- Ensuring that roles and responsibilities for global incidents are mapped out clearly.
- Practicing responding to a global incident via a training or tabletop scenario involving the relevant actors in your organization both in the U.S. and EU, and using the outcomes of the training or scenario to make enhancements to your plans and processes.

As more and more countries implement breach notification laws, taking these steps could help to address the growing complexity of investigating and responding to global data breaches.

You can subscribe to future ***Privacy & Data Security*** advisories and other Alston & Bird publications by completing our **publications subscription form**.

If you have any questions or would like additional information, please contact your Alston & Bird attorney or one of the following:

James A. Harvey
404.881.7328
jim.harvey@alston.com

David C. Keating
404.881.7355
202.239.3921
david.keating@alston.com

Kelley Connolly Barnaby
202.239.3687
kelley.barnaby@alston.com

Kathleen Benway
202.239.3034
kathleen.benway@alston.com

Chris Baugher
404.881.7261
chris.baugher@alston.com

Alexander G. Brown
404.881.7943
alex.brown@alston.com

Elizabeth Broadway Brown
404.881.4688
liz.brown@alston.com

Kristine McAlister Brown
404.881.7584
kristy.brown@alston.com

Angela T. Burnette
404.881.7665
angie.burnette@alston.com

David Carpenter
404.881.7881
david.carpenter@alston.com

Lisa H. Cassilly
404.881.7945
212.905.9155
lisa.cassilly@alston.com

Kimberly K. Chemerinsky
213.576.1079
kim.chemerinsky@alston.com

Cari K. Dawson
404.881.7766
cari.dawson@alston.com

Maki DePalo
404.881.4280
maki.depalo@alston.com

Derin B. Dickerson
404.881.7454
derin.dickerson@alston.com

Clare H. Draper IV
404.881.7191
clare.draper@alston.com

Christina Hull Eikhoff
404.881.4496
christy.eikhoff@alston.com

Sarah Ernst
404.881.4940
sarah.ernst@alston.com

Peter K. Floyd
404.881.4510
peter.floyd@alston.com

Daniel Gerst
213.576.2528
daniel.gerst@alston.com

Jonathan M. Gordon
213.576.1165
jonathan.gordon@alston.com

Elizabeth Helmer
404.881.4724
elizabeth.helmer@alston.com

John R. Hickman
404.881.7885
john.hickman@alston.com

Donald Houser
404.881.4749
donald.houser@alston.com

Stephanie A. Jones
213.576.1136
stephanie.jones@alston.com

William H. Jordan
404.881.7850
202.756.3494
bill.jordan@alston.com

W. Scott Kitchens
404.881.4955
scott.kitchens@alston.com

John L. Latham
404.881.7915
john.latham@alston.com

Dawnmarie R. Matlock
404.881.4253
dawnmarie.matlock@alston.com

Amy Mushahwar
202.239.3791
amy.mushahwar@alston.com

Wim Nauwelaerts
+32.2.550.3709
202.239.3709
wim.nauwelaerts@alston.com

Kimberly Kiefer Peretti
202.239.3720
kimberly.peretti@alston.com

Cara M. Peterman
404.881.7176
cara.peterman@alston.com

T.C. Spencer Pryor
404.881.7978
spence.pryor@alston.com

Karen M. Sanzaro
202.239.3719
karen.sanzaro@alston.com

Jessica C. Smith
213.576.1062
jessica.smith@alston.com

Lawrence R. Sommerfeld
404.881.7455
larry.sommerfeld@alston.com

Peter Swire
240.994.4142
peter.swire@alston.com

Katherine M. Wallace
404.881.4706
katherine.wallace@alston.com

Richard R. Willis
+32.2.550.3700
richard.willis@alston.com

ALSTON & BIRD

WWW.ALSTON.COM

Follow us: On Twitter @AlstonPrivacy
On our blog – www.AlstonPrivacy.com