GIR Global Investigations Review

The Guide to Cyber Investigations - Third Edition

Regulatory Compliance in the Context of a Cross-Border Data Breach

The Guide to Cyber Investigations - Third Edition

Data breaches and similar incidents pose a unique challenge – those targeted must both respond and investigate simultaneously. It is an art that is impossible without preparation.

Businesses wishing to prepare will find this volume, The Guide to Cyber Investigations, invaluable. It identifies every issue to consider when creating a response template and implementing it, giving both the law and plenty of practical and tactical advice.

Written by leading contributors, all with broad experience of serious data incidents, it is an indispensable desktop guide and a worthy companion to GIR's larger volume on cross-border investigations, The Practitioner's Guide to Global Investigations.

Generated: April 9, 2024

GIR Global Investigations Review

Regulatory Compliance in the Context of a Cross-Border Data Breach

Evan Norris and **Jennifer S Leete**
Cravath Swaine & Moore

Summary

With the vast amounts of data stored on servers and in the cloud, and the ever-increasing sophistication of threat actors, organisations must contend with a complex multinational regime of data protection laws. Although these laws share many common features, the sheer number of them – and the differences in definitions, standards and exceptions between them – presents a challenge for an organisation when a data breach occurs. Perhaps most notably, the victim of the breach must adhere to regulatory deadlines in an environment of factual uncertainty that characterises the initial days, and often weeks, following a breach. When a significant number of individuals are affected, achieving regulatory compliance is a challenge for any organisation that does business across borders.

As discussed elsewhere in this Guide, one aspect of a breach investigation for an organisation is to assess early whether the breach raises notification obligations and, if so, in which jurisdictions. Although a well-drawn incident response plan will have provided a head start on that assessment, one early aim of the investigation will be to complete the assessment by a careful review of the facts of the breach. In this chapter, we provide an overview of the factors that bear on that assessment, as well as some considerations regarding the provision of notification itself. We then provide some observations about the broader data security compliance and enforcement landscape more generally, as we look to a future in which more and more data regulators and law enforcement authorities have the budgets and experience to address the types of large-scale, cross-border breaches that are increasingly commonplace.

DETERMINING WHETHER AND IN WHAT JURISDICTIONS A DATA BREACH GIVES RISE TO NOTIFICATION OBLIGATIONS

Data breach notification laws across the globe reflect a mixture of rules, standards and approaches. In the European Union, the General Data Protection Regulation (GDPR)-[2] imposes breach notification obligations that apply broadly to all data controllers and processors,[3] while other individual EU Member States maintain additional notification laws that apply more narrowly to specific industry sectors. In the United States, each of the 50 states (as well as most districts and territories) has its own breach notification law, while a number of federal laws (and even some more state laws) regulating different industry sectors also contain breach notification rules for reporting incidents involving medical, financial and other types of data. These types of rules have been adopted in more than 150 countries, including jurisdictions throughout Asia, the Middle East, Africa, Latin America and other regions.[4]

These laws differ in myriad ways, including in the scope of their application, how they define a breach, the level of harm that triggers notification requirements, what exceptions may apply, who is notified, who does the notifying and what regulatory penalties may be imposed for noncompliance.[5] In the context of a cross-border data breach, the challenge this variability poses for organisations is particularly significant.

IDENTIFICATION OF APPLICABLE LAWS

Data protection laws may apply based on different factors, such as the organisation's basis for processing data, the industry in which the organisation operates and the residence of affected individuals.

In the United States, although there is no comprehensive data protection regime at the federal level, a handful of federal laws regulating various industries (including

telecommunications, financial services and healthcare) include breach notification provisions that apply primarily based on the type of personal data a regulated entity may collect. For instance, the Gramm-Leach-Bliley Act imposes breach notification obligations on 'financial institutions', including federally chartered US banks and federal branches and agencies of foreign banks, with respect to non-public customer personal information.[6] Such laws also exist at the state level. In New York State, for example, the Department of Financial Services enforces a cybersecurity regulation notification requirement that applies to financial service companies, including insurance companies and both domestic and non-US banks operating within the state, with respect to material business information and some personally identifying individual data.[7] In some instances, compliance with industry-specific notification requirements in a federal statute will exempt an organisation from compliance with the requirements of a state's general breach notification law.[8] Outside the industry-specific context, US states have consumer-oriented breach laws that typically apply broadly to organisations whenever a security incident involves data belonging to that state's residents. California's breach notification law, for instance, imposes obligations on any person or entity that conducts business in California and holds computerised personal information belonging to California residents.[9] In other words, depending on the type of data compromised in a breach, an organisation may have notification obligations under any number of US federal and state laws.

Although many countries' breach laws are similar in scope to those in the United States, some apply regardless of the industry sector and the residence of affected individuals. The GDPR's data protection and breach regulations apply to data controllers and processors that maintain an 'establishment' in the European Union or conduct processing activities, wherever conducted, that relate to offering goods or services to 'data subjects' in the European Union or to monitoring those subjects' behaviour in the European Union.[10] The post-Brexit data privacy laws in the United Kingdom – the Data Privacy Act of 2018 and the UK GDPR – are effectively identical in substance to the GDPR with respect to the obligations imposed on controllers and processors. The data privacy laws of several other countries also mirror the GDPR, including Brazil's data protection regime (the LGPD)[11] and China's first comprehensive data protection law (the Personal Information Protection Law), which came into effect in November 2021.[12]

DEFINITION OF 'PERSONAL INFORMATION'

Many breach notification laws limit the definition of 'personal information' (or some analogous term) to an enumerated list of data characteristics that are considered sensitive. For example, many US state breach laws narrowly define 'personal information' as an individual's first name (or first initial) and last name combined with any other data elements, such as a social security or driver's licence number.[13] California is one of other states that apply a broader definition covering 'any information that identifies, relates to, describes, or is capable of being associated with, a particular individual', including identifiers such as name, signature, address, employment, social security number, bank account number, credit or debit card number, medical information, health insurance information, biometric data and genetic data.[14] To take a US federal example, the Communications Act of 1934 protects 'customer proprietary network information', defined as information relating to the 'quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier'.[15]

By contrast, some breach notification laws adopt far more expansive definitions of personal information that cover any information relating to natural persons. For instance, the GDPR broadly defines 'personal data' as 'any information relating to an identified or identifiable natural person'.[16] Canada's Personal Information Protection and Electronic Documents Act provides that 'personal information means information about an identifiable individual'.[17] Similarly, South Africa's Protection of Personal Information Act defines 'personal information' as 'information relating to an identifiable, living, natural person' or any 'identifiable, existing juristic person'.[18] These general definitions could extend to almost any information about an individual, whether alone or combined with other data elements possessed by an organisation.

DEFINITION OF 'DATA BREACH'

Across jurisdictions, the definitional elements of a 'data breach' often include one or more of the use, disclosure, acquisition of, or access to data through illegal or unauthorised means.

DIFFERING APPROACHES TO ACCESS AND OTHER ACTIVITIES

Many US states define a data breach as the unauthorised or illegal acquisition of personal information.[19] In contrast, some jurisdictions consider unauthorised access, alone or in combination with another activity or a certain result, sufficient to constitute a breach. Under Singapore's data privacy statute, for example, a data breach broadly includes any 'unauthorised access, collection, use, disclosure, copying, modification or disposal of personal data', regardless of whether any harm or risk of harm was caused by the breach.[20] A few US states also define a breach as simply unauthorised access to personal information, whereas others require that the unauthorised access compromises the security, confidentiality or integrity of protected personal information.[21]

Some jurisdictions incorporate a risk standard into the definition of a data breach. For instance, Australia's mandatory Notifiable Data Breach Scheme defines an 'eligible data breach', in relevant part, as (1) any 'unauthorised access to, or unauthorised disclosure of, the information' or (2) 'information [that] is lost in circumstances where' unauthorised access or disclosure 'is likely to occur', both of which 'would be likely to result in serious harm to any of the individuals to whom the information relates'.[22]

As security incidents increase in sophistication, the definition of a data breach continues to evolve to include wide-ranging activities in addition to acquisition, access, use or disclosure. This evolution is noticeable in the GDPR's definition of a data breach as any 'accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed'.[23]

CHALLENGES IN ASSESSING DATA BREACHES

Threat actors may infiltrate an organisation's cyber infrastructure while obscuring evidence of their activities in computer servers and systems. These anti-forensic techniques can include deleting files, altering logs, encrypting drives or folders and using software scripts.[24] Because these techniques help threat actors avoid detection, they complicate the investigation into whether personal data is breached under applicable notification laws.

An increasingly common technique that obscures evidence of access to personal data is the use of legitimate software scripts to canvas an organisation's environment. Software scripts, or scripting languages, are automated 'instruction statements' that sequentially execute a function on a server or device.[25] Although scripts are legitimate tools used to administer

and maintain an organisation's network, they are often used maliciously in cyberattacks.[26] For instance, PowerShell is a scripting language that has been used by more than 60 threat actor groups to carry out cyberattacks.[27] Script-based cyberattacks execute malicious instructions across an organisation's servers to find, collect and exfiltrate files containing keywords that indicate personal or sensitive data.[28] Because scripts can run automatically across multiple servers or networks, they potentially access thousands of data files at a time. And it may be impossible for organisations to determine whether data files are accessed by an unauthorised person or just read by an automated script. Notwithstanding this challenge, script-based cyberattacks may still trigger a notification obligation, especially in jurisdictions where access alone is a definitional element of a data breach.

Although anti-forensic techniques are constantly evolving, breach notification laws provide limited guidance for organisations to decide whether personal data is actually accessed. For instance, Puerto Rico's breach notification law provides that a reportable '[v]iolation of [a] security system . . . includes both access to the data banks through the system and physical access to the recording media that contain the same and any removal or undue retrieval of said recordings'.[29] Some laws, such as the GDPR, do not define 'access' or provide any guidance for determining when personal data has been accessed. It is crucial, therefore, for organisations to investigate affected systems for evidence of threat actor behaviour and to assess the risk to personal data contained in those systems when determining whether a data breach has occurred.[30]

EXCEPTIONS AND EXEMPTIONS

Once an organisation determines that a breach of protected personal information may have occurred, it must evaluate whether any exceptions or exemptions apply that could obviate the need to make a breach notification.

ENCRYPTION

Some breach notification laws carve out safe harbours for personal information or data that is encrypted (or substantially redacted) at the time of a breach. Although the GDPR does not have an encryption exception, it treats 'state of the art' encryption as a data protection measure that reduces risk to individuals' rights and freedoms,[31] which could potentially excuse an organisation's duty to notify affected individuals.[32] Several US state breach laws, in contrast, explicitly distinguish between encrypted and unencrypted information when defining a data breach of personal information.[33] Some states completely exempt organisations from giving notice to affected individuals so long as the encryption was not compromised in the security incident.[34] In other states, encrypted data elements may be excluded from the legal definition of personal information or data, and the security incident that affects encrypted data elements may be excluded from the legal definition of a data breach.[35]

GOOD FAITH EXEMPTION

Notably, some breach notification laws exempt from the definition of a breach certain good faith access or acquisition of personal information by a company employee or agent. For instance, under the US Health Insurance Portability and Accountability Act (HIPAA), a data breach does not include 'any unintentional acquisition, access, or use of protected information' by employees of covered healthcare entities if 'made in good faith and within the scope of authority and does not result in further use or disclosure'.[36] Several US states, such as California and Virginia, also recognise a good faith exemption if an employee or

agent acquires personal information for a legitimate business purpose and does not make further unauthorised disclosure of the personal information.[37] No similar exemption exists under the GDPR. Brazil also does not recognise a good faith exemption, but 'good faith of the offender' will be taken into consideration to determine appropriate administrative sanctions for data processors that violate the country's data protection law.[38]

HARM THRESHOLDS AS NOTICE TRIGGERS

Several jurisdictions have adopted data breach notification laws that utilise harm thresholds as notice triggers, whereby organisations need only give notice if harm occurred or there is a potential of harm or risk to the individuals whose personal information is breached.

More than half of US states adhere to harm thresholds in their breach notification laws, but there is variance with respect to the risk a breach must present to the resident consumers of those states (the typical group entitled to notice) to require notification. For example, Virginia's breach notification statute requires notification to the state attorney general and any affected individual if there is a reasonable belief that the breach 'has caused, or will cause, identity theft or other fraud to any resident of the Commonwealth'.[39] Florida, on the other hand, does not require notice to individuals if, after appropriate investigation and consultation with federal, state and local law enforcement, the organisation determines that the breach 'will not likely result in identity theft or any other financial harm'.[40] Florida also does not require notification to its data regulator if fewer than 500 Florida residents are affected by a breach.[41] The Federal Trade Commission announced in 2022 a 'de facto breach disclosure requirement' based on the potential of harm to consumers.[42] This requirement directs organisations to 'disclose information to help parties mitigate reasonably foreseeable harm', regardless of whether breach notification is required under US federal or state law.[43]

Harm thresholds are also used outside the United States. Under Canada's data protection law, for example, notification to individuals and the regulator is required only where the breach creates 'a real risk of significant harm to an individual'.[44] Similarly, the implementing regulations to Mexico's data protection law require that the breach 'significantly prejudice the property or nonpecuniary rights of the data subjects' to trigger required notification to individuals.[45] The GDPR requires notification to the relevant supervisory authority if the breach presents a 'risk to the rights and freedoms of natural persons' and to individuals if the breach presents a 'high risk' to the same.[46] These differences in statutory definitions of the harm threshold may result in a determination, for instance, that a data breach occurred that was likely to result in a 'risk to the rights and freedoms' of EU citizens but did not pose a 'real risk of significant harm' to Canadian citizens, thus requiring notification under the GDPR but not under Canada's law.[47]

Some jurisdictions do not impose any harm thresholds either for defining a breach or setting forth the circumstances in which notification is required. For example, South Korea's data protection law applies no harm threshold to the notification requirement.[48] Similarly, California's breach notification law imposes no harm threshold; rather, an organisation must notify affected California residents of any breach where 'unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person'.[49] Under these standards, actual or potential harm to individuals is not considered with respect to whether an organisation must notify individuals of a breach.

If the relevant threshold triggering a mandatory notice requirement is not met, then any notification to individuals or regulators by the affected organisation would be voluntary.

Regulators in some jurisdictions encourage voluntary notification by organisations, even if the breach does not rise to the threshold that would require mandatory notification. Argentina, for example, has no mandatory breach reporting requirement but organisations are encouraged to have a plan to manage breaches and requires that they maintain a record of data breaches that may be given to the relevant regulatory authority on request.[50]

CONSIDERATIONS REGARDING THE PROVISION OF NOTICE

Once an organisation determines that notification is required or prudent, several considerations arise as to the provision of notice itself, most of which can be addressed in advance in a global breach response plan. Again, the variation between different notification regimes is significant and must be carefully considered to ensure an efficient and coordinated approach.

WHO PROVIDES THE NOTICE

Several of the comprehensive data protection laws require that all controllers of personal data notify individuals and regulators of a data breach. Although controllers of personal data are required to provide notice to individuals and regulators (or face penalties), the controller may not always be the entity that discovers a breach. The processors of data may be more likely to find evidence of a breach as they perform their work with the data, and for that reason a number of notification regimes require processors to notify the controller if they discover a breach. For example, the GDPR requires that the processor notify the controller 'without undue delay' after the processor becomes aware of a breach. Virginia's breach notification law also requires that those entities that maintain data they do not own or license (i.e., processors) must report a data breach to the owner or licensee of the data (i.e., controllers) 'without unreasonable delay' after discovery of the breach.[51] These notification requirements for processors ensure that controllers will be able to meet their own notification obligations in a timely manner.[52]

TIMING OF NOTICE

Many data privacy statutes require notification quite soon after the organisation has discovered the breach and the scope of its impact.[53] California's data breach notification statute, for example, requires that notification be made to individuals 'in the most expedient time possible and without unreasonable delay' following discovery or notice of the breach.[54] Notification may be reasonably delayed under California's statute to allow the organisation time to assess the scope of the breach or to prevent any interference with an ongoing criminal investigation. Several other states, including Virginia, New York and Massachusetts, require notice to data subjects without 'undue' or 'unreasonable' delay.[55] The same standard is seen in data privacy laws in other jurisdictions, such as the European Union, which also requires notice to data subjects 'without undue delay'.[56]

The specific requirements vary in some statutes for notification to regulators as opposed to individuals. The GDPR, for example, specifies that notification must be made to the national supervisory authority (or lead supervisory authority in the case of cross-border breaches) 'not later than 72 hours after having become aware of' the data breach; if the supervisory authority is not notified within that window, the organisation must provide reasons for the delay.[57] Other statutes may not require notification to a regulator at all unless a certain number of data subjects have been affected. California's statute, for instance, requires that there be at least 500 affected California residents before requiring that notification be made to the state attorney general.

In other jurisdictions, the notice requirement for regulators is not tied to any number of affected individuals. For example, India's data protection law broadly requires organisations to 'report the cybersecurity incidents to [the regulator] within a reasonable time of occurrence' of the breach.[58] Some jurisdictions have only recently imposed requirements for organisations to notify affected individuals. For instance, Japan amended its notification law in 2022 to require data breach notifications to affected data subjects; previously, notifications were merely recommended.[59]

Organisations affected by a breach thus must assess differing notice timing requirements for regulators and data subjects both within a particular statute and across multiple jurisdictions.

FORM AND CONTENT OF NOTICE

Statutory requirements also vary with respect to the form and content of the data breach notice. The GDPR, for example, requires that the notice to the regulatory authority:

- describe the nature of the breach;
- provide the name and contact details of the company's data protection officer;
- describe the likely consequences of the breach; and
- describe the measures taken or proposed to be taken by the controller to address the breach.[60]

Other statutes are even more prescriptive with respect to the required form and content of the notice. California's breach notification statute, for instance, requires that the notice to individuals use a certain title (Notice of Data Breach) and headings (What Happened?; What Information Was Involved?; What We Are Doing; What You Can Do), that the title and headings be clearly and conspicuously displayed, and even that the text of the notice use a font size no smaller than 10-point.[61] The California statute also provides a model breach notification form that companies may use as a template for their notice, the use of which ensures compliance with the statutory requirements.[62]

PUBLIC MESSAGING

In addition to complying with regulatory requirements in the aftermath of a breach, organisations face the communications challenge of conveying an appropriate public message. Media outlets will quickly discover and report on any large-scale data breach – often triggered by a notification submitted to a data regulator or a public company's securities disclosure (see above). In turn, an organisation's management and directors frequently face pressure to release public statements to the media addressing the breach and any remedial steps taken. There are many facets of the communications strategy that are beyond the scope of this chapter, but from a regulatory standpoint what is critical is including in an organisation's incident response plan – and then following in the event of a breach – a tight internal coordination mechanism involving the legal and relevant global business functions to enable a measured, consistent approach to all public statements.

DATA SECURITY COMPLIANCE AND ENFORCEMENT OBSERVATIONS

Separate and apart from the issue of notification, organisations that have experienced a data breach face a range of other potential regulatory challenges. For instance, all organisations must prepare to respond to regulatory enquiries with the potential to lead to an enforcement

response, whether tied to an underlying security failure, the adequacy of the notification or some other issue. Public companies have the added challenge of evaluating whether the breach is material to their financial performance and (or) operations and thus may be required to be disclosed to investors. As regulators across the globe gain in enforcement experience and begin to coordinate law enforcement activity with one another, organisations must increasingly be prepared to navigate the added complexities posed by these challenges when they arise in the context of multi-jurisdictional investigations of cross-border data breaches.

DATA SECURITY

Many data protection laws contain provisions requiring organisations to maintain the security measures necessary to protect individuals' personal information from unauthorised access. For example, the GDPR requires that companies take 'appropriate technical and organisational measures' to ensure that data is securely stored and processed.[63] The California Consumer Privacy Act (CCPA) requires that organisations 'implement and maintain reasonable security procedures and practices' to protect California individuals' personal data.[64] And Mexico's data protection law requires that all data controllers and certain processors 'establish and maintain administrative, physical, and if applicable technical, security measures' to protect personal data.[65] These and other similar laws establish standards that data protection authorities and other enforcement agencies are increasingly using to hold organisations accountable if a data breach occurs that, in the view of regulators, should have been prevented or mitigated.

The GDPR permits regulators to pursue fines for data security violations equal to the higher of €20 million or 4 per cent of an organisation's annual worldwide turnover.[66] In Brazil, the LGPD permits regulators to pursue roughly half that amount.[67] California takes a different approach and permits the California Privacy Protection Agency (CPPA) or the state attorney general to seek civil penalties (calculated with respect to each affected consumer) of up to US$7,500 per intentional violation and US$2,500 per unintentional violation, with no maximum amount.[68] In addition, California provides individuals with a private right of action for breaches of personal information caused by an organisation's failure to implement and maintain reasonable security procedures and practices; claimants may seek damages of up to US$750 per consumer per incident or actual damages, whichever is greater.[69] In the context of cross-border data breaches, the total amount of regulatory fines that could be imposed on an organisation by multiple enforcement authorities – and the potential for duplicative penalties given different approaches to conceptualising the fine amount and different definitions of data subjects and consumers – are both significant.

PUBLIC COMPANY DISCLOSURES

Public companies affected by a breach face additional regulatory requirements. For instance, in the United States, the Securities and Exchange Commission (SEC) has issued interpretative guidance requiring public companies to disclose material cybersecurity incidents, including data breaches, in their public filings.[70] Even a non-material breach may give rise to a disclosure obligation whereby investors should be informed of potential risks the company faces. Additionally, in March 2022, the SEC proposed another rule intended to 'provide enhanced disclosures regarding [public companies'] cybersecurity risk governance and cybersecurity incident reporting. This rule would require, among other things, mandatory reporting within four business days after determination of a 'material cybersecurity incident' and updated disclosures on previously disclosed cybersecurity incidents.[71]

In the European Union, the Market Abuse Regulation requires EU-listed companies to disclose 'inside information', which potentially includes data breaches and other types of cybersecurity incidents, that directly affect their operations and the price of financial instruments.[72] Public companies, therefore, must carefully determine both whether notification and disclosure of data breaches is required, as well as the potential effect that one determination may have on the other. As the SEC's 2018 settlement with Yahoo and other recent enforcement actions make clear, the issue of disclosure to investors can lead to significant enforcement consequences both for US public companies and foreign private issuers.[73]

THE FUTURE OF ENFORCEMENT

Many data protection authorities around the world are still in the early phases of enforcing data protection laws and managing their budgetary constraints, and organisations will be monitoring enforcement trends closely. For instance, organisations are watching closely for signs of the emerging enforcement priorities of China's and Brazil's data protection authorities and the effects of the California Privacy Rights Act (the successor to the CCPA that divides enforcement between the California AG and the CPPA) on the overall US enforcement landscape.

Organisations will also be closely watching for trends towards coordinated resolutions of enforcement actions among data protection authorities from different countries. We have seen such coordination among US federal and state regulators, and within the European Union, following cross-border data breaches. But although there have been examples of enforcement actions announced by multiple countries at different times in connection with cross-border data breaches (e.g., ***Equifax***, ***Yahoo*** and ***Starwood/Marriott***), it remains to be seen if and when regulators from different countries may begin to announce coordinated resolutions of the type we have come to see in corporate criminal investigations.[74] In the meantime, we anticipate debate about whether the merits of such an approach, such as encouraging cooperation among enforcement agencies and avoiding duplicative penalties for organisations, apply in the data breach context.

CONCLUSION

Today's complex regulatory environment presents great challenges for global organisations contending with a data breach of any magnitude. Compliance with the multitude of international breach notification laws requires an understanding of what facts may trigger statutorily mandated notice obligations and how and to whom that notice must be communicated. Even when breach notification obligations are satisfied, organisations still must be prepared to handle other regulatory challenges as well, including inquiries into security vulnerabilities that may have contributed to the breach. As more countries enact comprehensive data protection laws and cross-border data breach enforcement picks up, organisations that have breach response procedures that are carefully prepared and reflect a nuanced, global perspective will be best positioned to handle a major incident.

Endnotes

CRAVATH

Evan Norris enorris@cravath.com
Jennifer S Leete jleete@cravath.com

Worldwide Plaza, 825 Eighth Avenue, New York, NY 10019-7475, United States

Tel: +1 212 474 1000

http://www.cravath.com

CRAVATH, SWAINE & MOORE LLP