

Anticipating the Burden of Risk:

Breach Notification Compliance

International risk assessment

This *Bloomberg Law* report provides an assessment of the international risk landscape surrounding breach notification compliance. The goal of this report is to provide global businesses, and the law firms and consultants who provide counsel to those companies, an objective assessment of the overall global risk environment, as well as country-specific benchmark analytics on the burden in meeting compliance requirements, and the risk stemming from non-compliance. That analysis is based on data from *Bloomberg Law's Compliance Risk Benchmarks* tool, which leverages a proprietary algorithm to produce risk benchmark scores for ten topics across more than 45 countries, based on eight quantitative and qualitative risk factors—e.g., enforcement level, potential criminal and civil monetary penalties, potential criminal imprisonment—as well as editorial textual analysis of the relevant laws and regulations.

Privacy counsel and global businesses face tough obstacles in evaluating risk, as well as in developing and evolving global privacy compliance programs. Notably, rationalizing privacy controls across several countries' varying and nuanced laws and regulations, as well as their regulators and enforcement climate, poses a distinct challenge. Similarly, the task of assessing and advising on comparative risk between countries tends to prove exceedingly difficult, involving multiple factors beyond a straight comparison of the laws themselves.

The challenges in global program and risk management vis-à-vis incident preparedness and response are particularly emblematic of these larger issues, and in that vein this report utilizes *Bloomberg Law's Compliance Risk Benchmarks* to provide a look at the compliance risk landscape, and the countries at the epicenter of the challenges faced by chief privacy officers, in-house counsel, privacy practices, and privacy consultants.

The threat landscape

Data breaches in the U.S.—by number and severity—have increased dramatically over the past 10 years. In a much publicized case, Yahoo's CEO lost a bonus and stock award because security breaches at the company were mishandled by senior executives (also affected was the company's sale price of internet properties to Verizon, discounted by \$350 million). Similarly, recent security breaches at JPMorgan, EBay, Target, and Home Depot involving credit card numbers and e-mail addresses have proven embarrassing reminders of the need to protect customers' privacy.

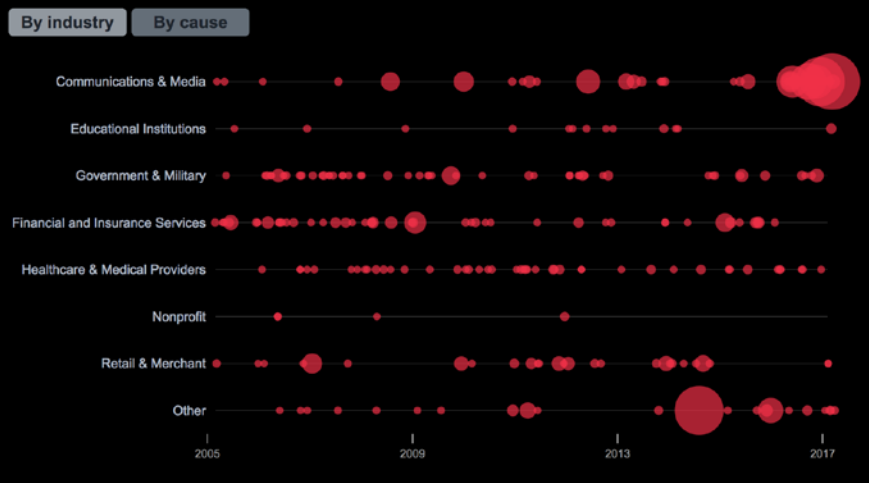
While news coverage has made privacy a topic of intense interest in the U.S., understanding the international regulatory environment is no less important to U.S. companies doing business abroad. For example, while the European Union has sought to harmonize data security oversight and enforcement among its members, there remain country-specific variations and the regulatory infrastructure of each country remains essentially unchanged by EU harmonization.

Top 10 Breaches of Personal Records

1. River City Media	March 08, 2017	1.4B
2. Yahoo (12/2016)	December 14, 2016	1.0B
3. Unknown (Russian Hacking)	August 05, 2014	1.0B
4. Yahoo (9/2016)	September 22, 2016	500.0M
5. FriendFinder	November 16, 2016	412.0M
6. MySpace	May 31, 2016	360.0M
7. Unknown (Nation Builder)	December 28, 2015	191.0M
8. LinkedIn (2012)	June 06, 2012	167.0M
9. Heartland Payment Systems	January 20, 2009	130.0M
10. LinkedIn (2016)	May 17, 2016	117.0M

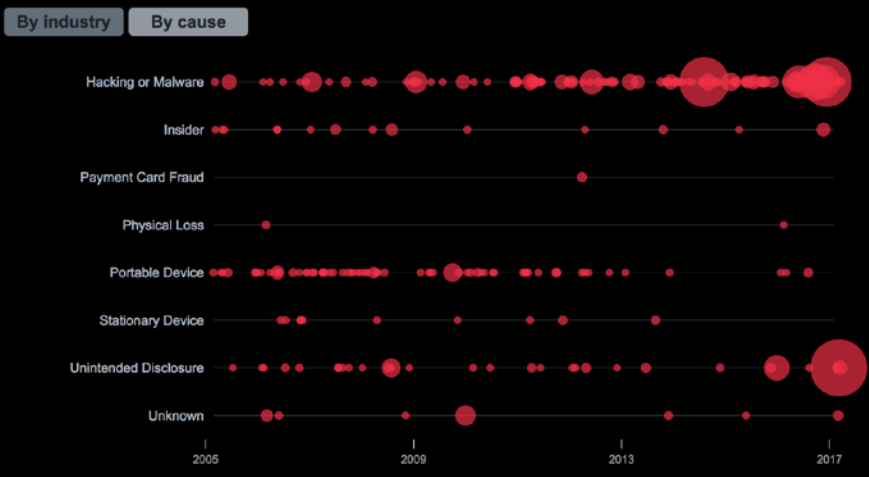
Data Breaches Over Time

Since 2005, more than 300 data breaches in which 200,000 or more records were compromised have been publicly disclosed.



Data Breaches Over Time

Since 2005, more than 300 data breaches in which 200,000 or more records were compromised have been publicly disclosed.



Mitigating international risk exposure



Bloomberg Law's **Compliance Risk Benchmarks** provides insight into comparative burden and risk related to Breach Notification and nine additional, critical issues across more than 45 countries so companies and lawyers can operate with a deeper understanding of varying data protection laws, contextualized by potential financial, criminal, and litigation exposure, among other practical considerations. A quick view of the top-10 high compliance-risk countries for Breach Notification shows:

Rank	Country	Burden	Enforcement	Potential Criminal Fines	Potential Civil Fines	Potential Criminal Imprisonment	Private Right of Action
1	South Korea	Very High Outlier	High	\$700,000 (KRW 785,000,000)	\$26,500 (KRW 30,000,000)	Yes	Yes
2	Colombia	Very High Outlier	High	\$0	\$571,000 (COP 1,641,714,000)	Yes	Yes
2	Mexico	Very High Outlier	High	\$0	\$1,935,000 (MXN 38,419,200)	Yes	Yes
3	France	High Outlier	High	\$317,000 (EUR 300,000)	\$317,000 (EUR 3,000,000)	Yes	Yes
4	Japan	High Outlier	High	\$3,000 (JPY 300,000)	\$3,000	Yes	Yes
5	Spain	High Outlier	High	\$0	\$53,000 (EUR 50,000)	Yes	Yes
5	Philippines	High Outlier	High	\$100,000 (PHP 5,000,000)	\$0	Yes	Yes
6	Belgium	High Outlier	High	\$0	\$0	No	No
7	Germany	Normal	High	\$11,600,000 (EUR 10,800,000)	\$335,000 (EUR 300,000)	Yes	Yes
8	Hungary	Normal	High	\$1,500 (HUF 450,000)	\$70,000 (HUF 20,000,000)	Yes	Yes

South Korea, rated an 83 on the *Bloomberg Law* Compliance Risk Benchmark Index of 0–100, stands out with high outlying burden and particularly high relative compliance risk. South Korea tends to be benchmarked quite high across other issues as well, and as with the case of Breach Notification, that is largely due to a fairly aggressive enforcement climate, potential criminal exposure, and relatively high potential financial exposure, particularly with regard to criminal penalties.

A deeper look at the underlying risk factor data leveraged by *Bloomberg Law's* **Compliance Risk Benchmarks**, as well as on-the-ground analysis through excerpts of risk environment analyses from *Bloomberg Law's* practitioner-drafted Country Profiles, is revealing. Among the countries with the highest Compliance Risk Benchmark score:

- Five of the top-ten countries present penalty-based financial exposure of at least \$500,000, with two countries (Mexico and Germany) presenting potential exposure of upwards of \$1,000,000
- There is potential exposure to private litigation stemming from improper handling of a breach in nine of the top-ten countries
- Nine of the top-ten countries have an aggressive enforcement climate
- Eight of the top-ten countries impose requirements that are high-burden or very-high-burden outliers
- Half of the top-ten countries are European countries

In addition to Breach Notification, *Bloomberg Law's* **Compliance Risk Benchmarks** provides similar country-specific insights into the following topics:



- Employee Health Information
- Online Privacy
- Personnel Records
- Electronic Marketing
- Data Transfer
- Employee Background Checks
- Employee Monitoring and Surveillance
- Data Security
- Data Collection and Processing



South Korea

The privacy law regime of South Korea is very complicated and detailed and has been subject to frequent change in recent years. Privacy laws overall have been strictly enforced by regulatory authorities, particularly law enforcement authorities. However, there are differences

in the level of enforcement depending on the specific sector, as there are a number of authorities who are each responsible for enforcing different privacy laws. For example, penalties related to data breach have resulted in administrative penalties of KRW 785 million from the Korea Communications Commission (KCC) for 13.2 million items of personal information being leaked, a three-month business suspension order and administrative penalty of KRW 6 million against each company by Financial Services Commission issued for 100 million items of personal information being leaked, and a penalty surcharge of KRW 4.48 billion and an administrative fine of KRW 25 million by the KCC for the leakage of the personal information of approximately 10 million users. The penalty amount was the heaviest issued by the KCC at the time.

Furthermore, there has been an increase in the number of cases where data subjects affected by large-scale personal information leakages have requested damages from the data handler. Such lawsuits have been filed against companies in various fields, including finance and telecommunications. Usually, compensation between KRW 100,000 and 300,000 is awarded to each plaintiff. Therefore, it has become ever more important for data handlers to ensure compliance with South Korean privacy laws and assess any relevant risks in processing personal information.

South Korea  **83** 

Breach Notification  

Compliance Burden : **High Far**

Is this an Emerging Issue ? **Yes**

Enforcement Level : **High**

Potential Criminal Fines : **\$700,000 (KRW 785,000,000)**

Potential Criminal Imprisonment : **Yes**

Potential Civil Penalties : **\$26,500 (KRW 30,000,000)**

Is there a Private Right of Action ? **Yes**

Number of Authoritative Regulators : **2**

Does this require a DPO ? **Yes**

Risk Benchmark Score: **83**

(Factors that we have used to determine South Korea's score.)



Mexico



The INAI has mainly focused on following up on data subjects' complaints for violations of the LFPDP. It can be seen that it is mainly taking a reactive approach, responding to complaints from data subjects, rather than affirmatively verifying data controllers' compliance with the law.

Fines may range from approximately 8,004 to 25,612,800 Mexican pesos (MXN), depending on the current minimum wage in Mexico City. During the first half of 2016, the INAI initiated 30 procedures for the implementation of sanctions. Of those procedures, 22 imposed economic sanctions on data controllers, totaling 50,611,145 pesos in fines. Sectors subject to the most sanctions included financial and insurance services, mass media, and education. Between January 2012 (when data subjects were first able to exercise ARCO rights) and June 2016, the total amount of fines imposed by the INAI totaled 235,669,887 pesos.

There has been activity from the INAI, but it is little activity compared to that of other data protection authorities, such as those in the European Union or the United States. There is still a lot to be done by the INAI, but also by the data subjects, starting with being acquainted with their rights.

The lack of compliance with the law, apart from resulting in a fine, may have serious reputation implications for a company, which may lose the confidence of its clients, consumers, employees, and business partners for not respecting privacy rights.

Mexico  **73** 

Breach Notification  

Compliance Burden : **High Far**

Is this an Emerging Issue ? **No**

Enforcement Level : **High**

Potential Criminal Fines : **\$0**

Potential Criminal Imprisonment : **No**

Potential Civil Penalties : **\$2,579,000 (MXN 51,225,600)**

Is there a Private Right of Action ? **Yes**

Number of Authoritative Regulators : **1**

Does this require a DPO ? **Yes**

Risk Benchmark Score: **73**

(Factors that we have used to determine Mexico's score.)

Colombia

The Colombian data protection laws provide for the possibility of penalties imposed up to 1500 (Law 1266) and 2000 (Law 1581) minimum legal monthly wages (between US\$338,730 and \$451,640 at 2016 minimum legal monthly wage and current exchange rates). However, up to this

date, the Superintendency of Industry and Commerce (SIC) has not imposed fines higher than US\$76,000 (at current exchange rates). This is mostly due to the fact that the SIC is aware of the fact that data protection laws are very recent in Colombia and there is an important lack of awareness among data subjects, data controllers, and data processors. This is why the SIC has undertaken very seriously the task of educating all stakeholders in the new regime and making them aware of the importance that data protection has.

The SIC, as many other data protection authorities around the world, has limited resources, making enforcement via investigations and fines very burdensome. As a result, the SIC, following international trends and based on provisions contained in Decree 1377, has taken steps to adopt the accountability principle as a way to achieve compliance in data protection. This is why, in June 2015, the SIC issued a set of Guidelines to Implement the Accountability Principle, which provides guidance to companies seeking to adopt data protection measures consistent with or exceeding Colombian standards, and which in turn will result in leniency from the SIC in the amount of fines imposed for any violation of data protection laws.

Colombia

73

×

Breach Notification

🔒💡

Compliance Burden: High Far

Is this an Emerging Issue? No

Enforcement Level: High

Potential Criminal Fines: \$0

Potential Criminal Imprisonment: No

Potential Civil Penalties: \$571,000 (COP 1,641,714,000)

Is there a Private Right of Action? Yes

Number of Authoritative Regulators: 2

Does this require a DPO? Yes

Risk Benchmark Score: 73

(Factors that we have used to determine Colombia's score.)

France

While CNIL is very active in ensuring companies' compliance, it is not the most aggressive authority in terms of financial sanctions compared to other EU Data Protection Authorities.

The sanctions that have been pronounced by CNIL are mainly administrative financial sanctions. The highest sanction pronounced in 2016 was €100,000 against Google. Other sanctions ranged from €10,000 to €30,000.

The harshest sanction, in practical terms, is a public warning, which may affect a company's reputation and which CNIL often uses to pressure companies.

The French Digital Republic Act, which took effect Oct. 7, 2016, significantly increasing the maximum level of fines for violations of the FDPA, allowing the CNIL to impose a fine of up to €3 million until the GDPR becomes applicable. The reform of the EU framework for data protection, will certainly change the risk landscape by increasing the data controller's liability through a principle of accountability, and increasing the liability of data processors.

France

70

×

Breach Notification

🔒💡

Compliance Burden: High

Is this an Emerging Issue? No

Enforcement Level: High

Potential Criminal Fines: \$317,000 (EUR 300,000)

Potential Criminal Imprisonment: Yes

Potential Civil Penalties: \$3,170,000 (EUR 3,000,000)

Is there a Private Right of Action? Yes

Number of Authoritative Regulators: 1

Does this require a DPO? No

Risk Benchmark Score: 70

(Factors that we have used to determine France's score.)

Japan

The risk level of enforcement generally depends on the industrial sector to which a business operator belongs and the type of data that the business operator handles. If the business operator belongs to regulated business sectors, such as financial services, medical services or

telecommunications services, generally stricter standards will apply, and if the nature of the affected data is sensitive—such as medical data or credit data—generally stricter responses will be given.

The APPI provides for penalties to be assessed against any business that fails to follow the law or any mandatory provisions of the guidelines. Under the APPI (art. 42), the PPC may issue a recommendation for corrective measures to a business found to be in violation of the law or guidelines. If the business fails to comply with such a recommendation, the PPC may issue “further orders.” If a business operator fails to comply with such orders, the business operator may be fined up to 300,000 yen or be subject to imprisonment for up to six months. (arts. 84, 87).

In addition to the administrative and criminal penalties described above, a business operator may be subject to claims from data subjects who were harmed by a data security breach, through breach of contract and/or tort actions under the general principles of the Civil Code.

Japan

66

×

Breach Notification

🔒💡

Compliance Burden : High

Is this an Emerging Issue ? No

Enforcement Level : High

Potential Criminal Fines : \$3,000 (JPY 300,000)

Potential Criminal Imprisonment : Yes

Potential Civil Penalties : \$3,000 (JPY 300,000)

Is there a Private Right of Action ? Yes

Number of Authoritative Regulators : 1

Does this require a DPO ? No

Risk Benchmark Score: 66

(Factors that we have used to determine Japan's score.)

Mitigate risk

The global landscape is changing daily and the ability to navigate the uncertain risk environment is essential. *Bloomberg Law's Compliance Risk Benchmarks* empowers you to advise on risk mitigation and privacy program design and implementation in the context of global business operations. Leverage a high-level view of the compliance risk and burden across countries and topics, and zero in with in-depth, expert assessments of individual countries' risk environments.

Need Assistance?
24/7 Help Desk & Live Chat
888.560.2529

blawhelp@bna.com
www.bloomberglaw.com

Stay Connected
#BloombergLaw
@BloombergLaw



**Bloomberg
Law®**

© 2017 The Bureau of National Affairs, Inc.
0417-JO23416 04-1308