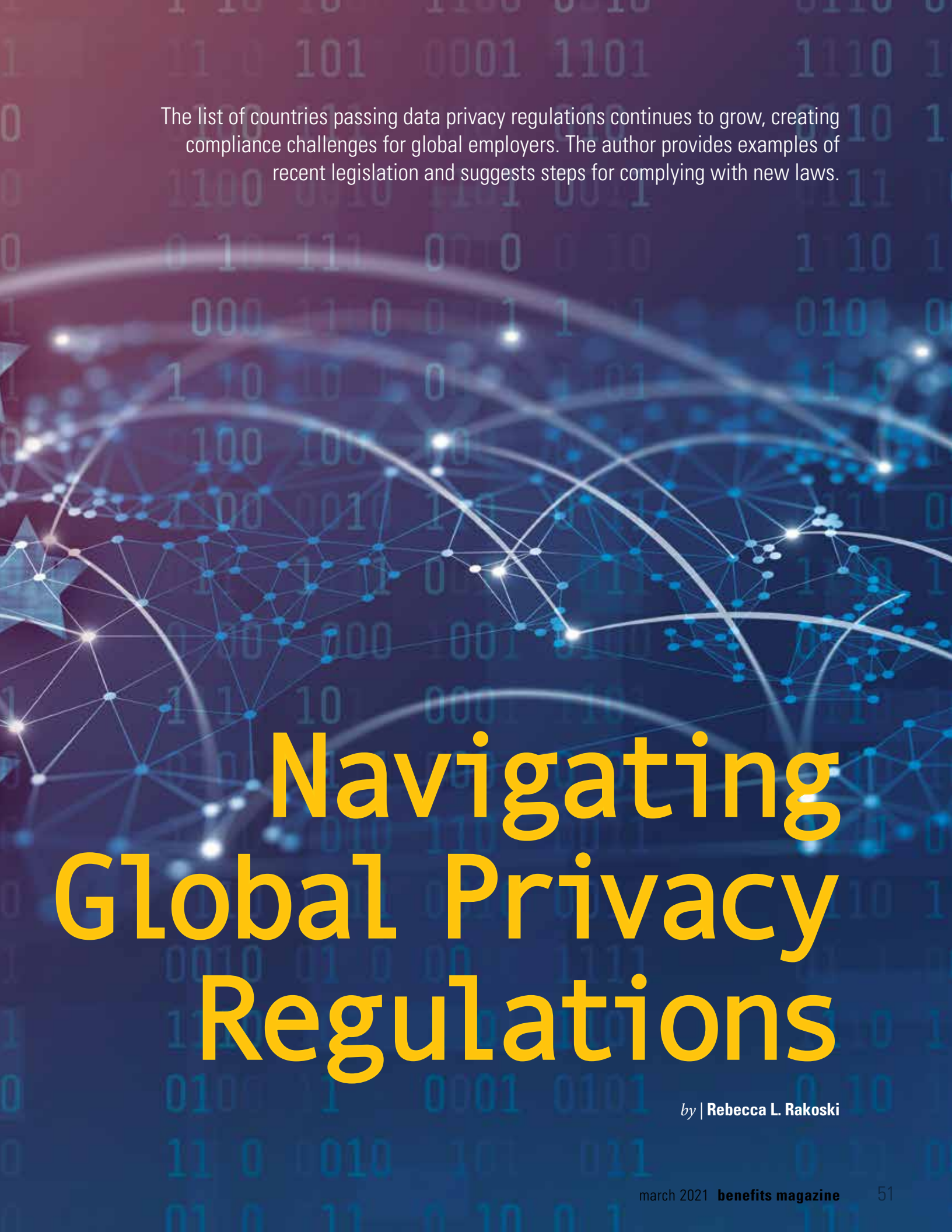
benefits
MAGAZINE



The list of countries passing data privacy regulations continues to grow, creating compliance challenges for global employers. The author provides examples of recent legislation and suggests steps for complying with new laws.

Navigating Global Privacy Regulations

by | **Rebecca L. Rakoski**

The past several years have demonstrated a marked change in the data privacy landscape around the globe and here in the United States.

Global employers must be aware of the changing regulations because they affect not only the data collected from customers and clients but also the data collected from employees. This is of particular importance in administering global employee benefits.

This article will review some of the recent domestic and global data privacy legislation that affects global employers and will provide suggested steps for complying with data privacy laws.

The Global Data Privacy Landscape

Unlike their domestic counterparts, international data privacy laws directly impact employee-related data. The international approach to data privacy tends to be one that follows all data rather than a specific type of data. In that regard, the global data privacy landscape is much broader than what is seen domestically.

For example, the European Union's General Data Protection Regulation (GDPR), which went into effect on May 25, 2018, is possibly the broadest and most comprehensive data privacy law on the books today. With its emphasis on transparency in data collection and processing along with the rights it affords data subjects (i.e., right to erasure,[1] right of access[2]), GDPR has certainly driven substantial changes in the manner in which organizations collect, store, transmit and protect the data they collect.

GDPR does not carve out or exempt employee-related data; in fact, it applies directly to that data. This means that organizations that are not consumer facing (i.e., business-to-business companies) must comply with the law for employee-related data. In addition, GDPR provides the same data privacy rights afforded to consumers (the aforementioned right to erasure and right of access). However, the right to erasure (also known as the *right to be forgotten*) may not apply to all employee-related data, particularly where the data is still necessary for the purpose for which it was collected. GDPR does provide a wide claim to employee data that would protect it from erasure, but it is not absolute and not in perpetuity. Also, certain data collected for employee benefits may constitute a special category of data (i.e., highly sensitive data), including personal data revealing racial or ethnic origin or health-related data. This data is subject to specific processing conditions under GDPR Article 9, Processing of Special Categories of Personal Data.

In addition to the European Union, many other countries, including Japan, Australia, China, Brazil and India, have also passed data privacy laws that impact employee data.

In Japan, for example, the Act on the Protection of Personal Information (APPI) was passed in 2015 but was subject to substantial revisions and did not come into full effect until May 30, 2017. The Personal Information Protection Commission (PPC), which is the regulatory body established pursuant to APPI responsible for overseeing compliance with the law, issued key guidelines on the applicability of the law. Among those guidelines was the handling of health information in employment management. The guidelines address issues ranging from dealing with technical measures regarding personal information in the private pension area to appropriate dealings with employment placement service providers and recruiters.

On August 14, 2018, the Brazilian government approved the Brazilian General Data Protection Law, known as the Lei Geral de Proteção de Dados Pessoais (LGPD). Due to COVID-19, there was some issue as to the effective date of LGPD, but it appears that penalties and sanctions for noncompliance with LGPD will not begin until August 1, 2021. Like other data privacy laws, including GDPR and APPI, LGPD has a broad extraterritorial scope (i.e., it applies to Brazilian companies as well as organizations that process personal data for the purpose of offering or supplying goods and services to individuals in Brazil). As such, employers that hire candidates in Brazil or engage third-party service providers in the country will need to comply with LGPD.

The Domestic Data Privacy Landscape

No discussion of domestic data privacy could even commence without a discussion of the California Consumer Privacy Act of 2018 (CCPA). California enacted CCPA in 2018, and it went into effect on January 1, 2020. This sweeping data privacy law was really the first of its kind in the U.S. Unlike other domestic data privacy regulations that regulated specific industries, such as the Health Insurance Portability and Accountability Act (HIPAA), CCPA applies to all data collected on California consumers, regardless of industry.

To be clear, the January 1, 2020 effective date of CCPA did not apply to

all sectors of a business. In fact, CCPA was not even set to apply to employee-related data until January 1, 2021. Nonetheless, on November 3, 2020, California voters passed Proposition 24, also known as the California Privacy Rights Act (CPRA). CPRA will potentially impact the application of CCPA principles to employees. In addition, it amends CCPA and goes into effect on January 1, 2023. Similar to CCPA, CPRA has a one-year look-back that will govern data collected starting January 1, 2022.

Moreover, CPRA specifically provides that "[t]he interests of employees and independent contractors should also be protected, taking into account the differences in the relationship between employees or independent contractors and businesses, as compared to the relationship between consumers and businesses."[3] This means that employers in California have an obligation to protect the data they are collecting on employees and that employees will soon be afforded the same rights as consumers. The full scope and breadth of CPRA will apply to employees and independent contractors as of January 1, 2023. Until then, under CCPA, which remains in effect until CPRA comes online, employees do have limited rights, including the right to receive a notice at collection and the right to sue in the event their sensitive data is compromised as a result of a data breach.

In addition to California, Nevada and Maine have also enacted data privacy legislation. Other states, in turn, have focused more on cybersecurity, like the New York Stop Hacks and Improve Electronic Data Security (SHIELD) Act and the Pennsylvania Supreme Court decision in *Dittman v. UPMC*, which involved a data breach that impacted employee data. As a result, both New York and Pennsylvania require proactive measures to protect personal data. In particular, Pennsylvania recognized that employers owe a duty to employees to safeguard the sensitive data they are collecting. Regardless of whether it is a specific data privacy law like CCPA or a data security law like the SHIELD Act, employers are facing an unprecedented time where the data being collected on their employees requires specific attention and protection.

What Now?

In today's business landscape, organizations across the globe face seemingly endless changes and challenges posed by data privacy laws. It can feel like every day they are treated to a new proposed law or regulation that will impact the manner in which business is conducted. Because let's face it, business runs on data. And the interesting thing is that the cause of the issue (i.e., the data) is also its solution.

The goal for any business when it comes to data privacy compliance is risk mitigation. Risk elimination is a fantasy, and anyone promising that is seriously misinformed. The following six steps provide a framework for an organization to mitigate its risk. These six steps require an organization to pool resources from compliance, the law and technology. Purely technological solutions are never the answer to this multifaceted problem.

1. Understand the Data

Organizations first need to get a handle on their data. This step is critical in order to understand what laws may be impacting the organization. Having a data map to track data or data classification performed is essential. A good data map looks at each individual data point collected (i.e., first and last names, Social Security numbers, etc.). It then delves into each data point so that the organization can pinpoint the following elements, among others: (1) where the data is collected, (2) how it is collected, (3) where it is stored and (4) with whom it is shared.

Creating a data map is not solely a technology task or the responsibility of the information technology (IT) department; this will require work in every department. But the work is well worth it because it will assist the organization in determining where its most sensitive data is being collected and stored. Data mapping is one of the most important things an organization can do to become not only compliant but also more secure in its data practices. Using a data map to understand the legal basis for the data collection is key. This will enable an organization to more efficiently and effectively respond to data subject access requests, regulatory or customer audits, and data breaches. This information, coupled with the legal basis for collection, will

provide an organization with critical and essential information on its data.

2. Understand Regulations and Cross-Map the Requirements

As an organization gets a better handle on its data, it can begin to unravel and understand which data privacy laws and regulations are being triggered by its data collection practices. Some companies know, basically, what those laws might be, but having a data privacy regulatory assessment is critical to knowing for certain. The assessment is a legal determination, so organizations should consider using a data privacy attorney who understands the laws and brings with them the attorney-client privilege.

Once an organization understands the data and the laws, it can create a comprehensive data privacy and cybersecurity program. A cybersecurity and data privacy program is different for every organization since the type of data a company collects and how it uses that data is unique. Therefore, an out-of-the-box/one-size-fits-all solution is rarely the answer. A data privacy regulatory assessment should identify the gaps in an organization's compliance with the various laws impacting it. The assessment should also include a road map that will allow the organization to create an effective program.

In addition, many organizations are impacted by more than one data privacy or cybersecurity law. However, compliance with one does not equate to compliance with all. Counsel should cross-map standards and practices so that an organization can harness what it is already doing and incorporate that into a global program. This can save both time and money. In addition, a good program can easily adapt and incorporate new laws as they are passed. The trick is to utilize cyber/privacy counsel that takes a global approach.

3. Understand the Contractual Obligations

These contractual obligations are not only with third parties (although an organization will absolutely want to examine and update its third-party vendor/supplier contracts). Organizations should make sure that they track their contractual obligations and use standard contract provisions whenever possible. Data processing addendums are commonplace, and contracts that do not address data privacy and security fall woefully short of protecting an organization. Again, having privacy/security counsel that understands the laws and how they are impacting the data being processed is critical to protecting the corporation.

4. Identify Network Vulnerabilities

Once an organization has a better understanding of its data and contractual obligations, it should examine any network vulnerabilities. This step is informed by the data map and regulatory cross-mapping that it has already completed. Knowing where the sensitive data is collected, processed and stored allows an organization to fully understand which systems house its most sensitive data. In turn, this allows the organization to appropriately identify and defend those systems. This will feed into the next step in the process, which includes documentation.

5. Document Compliance in Written Policies and Procedures

In the world of data privacy and cybersecurity, if it is not documented, it is not done. Therefore, an organization needs to appropriately document its data privacy and cybersecurity practices. Not only does this empower employees and vendors because they know how and why data is treated, but

takeaways

- Global employers must be aware of changing privacy regulations around the world because they affect not only the data collected from customers and clients but also the data collected from employees.
- The international approach to data privacy tends to be one that follows all data rather than a specific type of data, which means that these laws generally apply to employee-related data.
- The European Union's General Data Protection Regulation (GDPR) is possibly the broadest and most comprehensive data privacy law on the books, but many other countries, including Japan, Australia, China, Brazil and India, have passed data privacy laws that impact employee data.
- The California Consumer Privacy Act of 2018 (CCPA) is one of the first of its kind in the U.S. and applies to employee-related data.
- As they work to comply with data regulations, the first step organizations should take is to get a handle on their data by creating a data map to track where and how data is collected, where it is stored and with whom it is shared.
- Training and communication on the specific policies and procedures of an organization are key steps in establishing an efficient and effective data privacy and cybersecurity program.

it also elucidates the importance of data privacy and security practices.

6. Train and Communicate With Employees

Documentation is a key step to establishing compliance, but organizations should keep in mind that one of the biggest issues they face is that their employees are not aware of and/or are not trained on the specific policies and procedures. Training is one of the weakest links in cybersecurity and data privacy practices. Many organizations do "training," but it is often not done well. This is evidenced by the fact that hackers are still able to regularly trick employees into clicking on a bad link or providing personal data.

Training and communication on the specific policies and procedures of an organization are key to closing the loop and establishing an efficient and effective data privacy and cybersecurity program. In addition, many data privacy laws specifically require training on an organization's data practices. This is not a step to overlook or treat lightly. Employees are an organization's largest asset and their biggest liability when it comes to data privacy and cybersecurity.

Conclusion

In short, compliance with these new and evolving laws is not for the faint of heart, but it is not an insurmountable challenge. The key is to take it step by step and avoid getting overwhelmed. The most effective data privacy and cybersecurity programs are designed to be fluid and changeable because data practices are similarly fluid. But these changes cannot be accomplished overnight, so organizations should start as soon as possible.

Using these laws to drive a better understanding of data collection and processing practices in an organization can only ever benefit the organization and help it avoid regulatory bumps down the road. Considering the success of hackers and the potential severity of fines resulting from failure to comply with these laws, waiting is a luxury that businesses likely cannot afford.

bio

Rebecca L. Rakoski is an attorney and the managing partner at XPAN Law Partners, LLP, in the greater Philadelphia area. She counsels and defends global public and private corporations and their boards during data breaches and in their response to state/federal regulatory compliance and enforcement actions. Rakoski also advises on proactive data privacy and cybersecurity measures to identify security weaknesses and threats before they occur. She understands international data privacy regulations in the European Union, Asia, South America and Australia and regularly handles complex contract negotiations involving the transfer of data both domestically and internationally. As a thought leader in the area of data privacy and cybersecurity, she serves on the New Jersey State Bar Association's cyber task force and as vice-chair elect its Bankruptcy Law Section. She also served on the complex business litigation committee that drafted and revised the New Jersey Court Rules involving electronic discovery in complex litigation matters. Rakoski serves on the board of governors for Temple University Health Systems and on Temple's Information Technology, Data Privacy, and Cybersecurity Committee. She is also an adjunct professor at Drexel University's Kline School of Law.

Endnotes

1. The *right to erasure* is also known as the *right to be forgotten* and is contained in Article 17 of the General Data Protection Regulation (GDPR) and gives individuals the right to ask organizations to delete their personal data. See https://gdpr.eu/right-to-be-forgotten/.
2. The *right of access* is contained in GDPR Article 15 and gives individuals the right to obtain a copy of their personal data. See https://ico.org.uk/for-organisations/guide-to-dp/guide-to-the-uk-gdpr/individual-rights/right-of-access/.
3. California Privacy Rights Act (CPRA), Section 8.