Introduction

In October 2015, hackers gained access to British telecommunications company TalkTalk’s internal servers. The breach compromised the personal data of 157,000 customers and included more than 15,000 bank account numbers. The TalkTalk hack was far from an isolated incident. In 2013, 70 million Americans had their personal data compromised when retailer Target was infiltrated. In France and Belgium, hackers stole personal data from more than 600,000 Domino’s Pizza customers. By the time the smoke cleared in the United Kingdom, TalkTalk had lost 95,000 customers and approximately $87 million (USD). Clearly, the stakes of data protection and consumer privacy are high and the task of ensuring them immense.

Protecting the personal data and privacy of customers and employees and complying with applicable laws has never been as hard as it is today. Significant ongoing changes to data protection laws around the world have made navigating data protection particularly fraught. Information technology and compliance professionals must monitor these changes, and those whose companies operate internationally must be aware of the frequent variation in countries’ laws.

Failing to properly protect data can have severe repercussions, including heavy fines and reputational damage. Fortunately, a robust approach to data protection can help your business avoid legal trouble and stay out of the headlines. Moreover, it can generate positive public relations, gain customer trust and be a source of competitive advantage.

A note to US multinationals: The United States has among the least onerous data protection and privacy regimes of the developed world. As such, you must be particularly vigilant in complying with other countries’ laws, many of which are likely to be far stricter than those you are accustomed to.
Key Terms

- **Data Privacy**: Concerns the collection, use, sharing, retention and protection of personal data of customers, users, employees and others.

- **Personal Data**: Data that relates to a living individual who can be identified from that data, including financial records, prospective customer files, social media content and employee data, among many other types.

- **Data Processing**: Obtaining, recording or holding personal information or data or carrying out any operation or set of operations on the information or data.

- **Data Subject**: An individual whose data is being collected or processed.

- **Data Controller**: A business or individual who determines the purpose and manner in which data is processed.

- **Data Processor**: A business or individual (other than an employee of the controller) who processes data on behalf of the data controller.

- **Right to be Forgotten**: A right that holds that individuals are entitled to have certain no-longer-relevant data from their past deleted.

- **International Safe Harbor Privacy Principles**: An agreement that enabled US companies to join a voluntary framework of data privacy standards, which allowed them to process EU personal data in the US sent to them from European Economic Area (EEA) data controllers.
Principles of Data Protection

Though data protection laws vary across jurisdictions — and as we will see, those variations are often wide and meaningful — they are generally founded upon a scaffold of eight principles adopted by the Organization for Economic Cooperation and Development (OECD). The principles guide the protection of data in both the private and public sectors and are intended to prevent the exposure of information that would pose a “risk to privacy and individual liberties.” Understanding the OECD principles provides a strong foundation from which one may approach country-specific data protection laws. The principles are outlined below:

- **The Collection Limitation Principle:** Holds that there ought to be limits to the collection of personal data and that the data ought to be collected lawfully and with the knowledge or consent of the data subject where appropriate.

- **The Data Quality Principle:** Holds that the data collected ought to be relevant to the purposes for which it is to be used and that, to the extent necessary for those purposes, the data is accurate.

- **The Purpose Specification Principle:** Holds that the purpose for data collection be disclosed prior to or at the time of collection and that subsequent uses of the data are consistent with the stated purpose.

- **The Use Limitation Principle:** Holds that personal data may not be disclosed except when the data subject consents or when the law compels its disclosure.

- **The Security Safeguard Principle:** Holds that personal data should be safeguarded against loss, unauthorized access and disclosure, among other potentially adverse outcomes.

- **The Openness Principle:** Holds that “there should be a general policy of openness about developments, practices and policies with respect to personal data.” In addition, knowledge of the existence and purpose of data as well as the identity of the data controller should also be available.

- **The Individual Participation Principle:** Holds that individuals should have the right to find out whether a data firm has their personal data and what it is without undue delay or cost. In addition, data subjects must have the ability to challenge data pertaining to them and have the data “erased, rectified, completed or amended.”

- **The Accountability Principle:** Charges data controllers with compliance with the OECD principles.

While many data protection laws are guided by these principles, the degree, relative emphasis and manner in which the laws address each can be markedly different, to say nothing of how the laws are enforced.
One key area of variation is the assignment of responsibility — that is, who is responsible for protecting personal data as prescribed by the law. After all, personal data is often handled by multiple parties, not just the entity with which the data subject interacts. Generally speaking, data controllers are made to shoulder this responsibility. In some cases, however, that responsibility is shared with data processors. Australia is one of a limited set of countries whose laws do not distinguish between data controllers and data processors, which means that the latter can be held responsible for breaches of the law. Much more common is the approach taken by the EU in Directive 95/46/EC, which places full statutory responsibility and liability for the protection of personal data with the data controller. Thus, in places like the EU where responsibility lies with the data controller, data processors’ exposure is generally limited. But this is changing.

Important Developments in Privacy and Data Protection

Forthcoming revisions to the EU data protection regime will expand responsibility for data protection to data processors as well as controllers. This change is but one highly visible example of the rapidly evolving state of data privacy laws. By its nature, technology is dynamic. This creates a frequent need for data protection laws to be revisited and updated. (Cloud computing is emblematic of this reality. The dramatic growth of the cloud has muddled the question of who controls data and what jurisdictions’ laws apply.)
Perhaps the most newsworthy example of the dramatic change affecting privacy is the European Court of Justice’s October 2015 decision invalidating the long-standing safe harbor data sharing agreement between the United States and Europe. The decision, which reverberated well beyond the legal and diplomatic circles through which the case had percolated, has affected thousands of companies and millions of people.

The 15-year-old agreement, which provided for the sharing of Europeans’ personal digital information with US business operations, was fundamental to many companies. (For example, Facebook used it to maintain European citizens’ data in US data centers.) The Court’s holding cast doubt on the continued legality of the scheme, given that the data is open to the surveillance activities of US government agencies (discussed below). Technology companies are far from the only firms to have been affected. The EU-US safe harbor agreement covered more than 4,000 companies and enabled everything from the sharing of employee payroll data across borders to the processing of customer orders to the tracking of user activity on digital platforms. If your business operates in both the United States and the EU, there is a good chance that it relied upon safe harbor.

The European Court’s decision is vivid evidence of the fast evolving and ever more strict global privacy environment in which companies must operate. Inspired by large-scale hacks of consumer data and dismayed by Edward’s Snowden’s revelations about widespread US government cyber-espionage, government regulators, supranational authorities and consumers have moved to restrict what data companies can collect, how they may use it and how they must protect it.

The European Union is significantly intensifying its data protection regime. Over the period 2016-2018, it is slated to incrementally replace its long-standing Directive 95/46/EC, which permitted member states significant latitude in achieving the Directive’s objectives. The new law — the General Data Protection Regulation (GDPR) — will strengthen data protection for individuals and unify data protection across member states. It’s worth noting here that the distinction between an EU directive and an EU regulation is an important one. A directive prescribes an end state without dictating to each member state what specific laws and regulations to put in place to achieve it. This contrasts with a regulation, which is directly applicable across all EU member states and applies uniform rules.
Among other provisions, the GDPR: imposes new data handling, record-keeping and consent requirements; broadens the application of statutory duties to include data processors not just data controllers; introduces mandatory data breach alert requirements; requires larger organizations to appoint data protection officers; applies to businesses that collect and process EU residents’ data regardless of whether or not that business is established in the EU; and expands upon data subjects’ right to be forgotten. Failure to comply with the GDPR can result in substantial monetary penalties — fines of up to 4 percent of a company’s global gross revenue. That means a technology giant such as Facebook could, if found in violation, be faced with a fine of nearly $1 billion.

Canada is another example of the rapidly changing regulatory environment. In 2015, it updated its privacy laws to include new breach notification requirements, broadened the definition of personal information to include employee data, and raised the bar on what constitutes consent to the collection and use of personal data.

Sometimes changes to data protection laws are as much about geopolitics as they are about protecting individual privacy. Following several years of public dissatisfaction over the open nature of the internet (President Putin has claimed that the internet is a product of the Central Intelligence Agency), Russia adopted legislation that mandates that Russian citizens’ data be collected and processed on Russian servers. Though cloaked in the language of “digital sovereignty,” the move is regarded by many analysts as a means of giving domestic security agencies access to the internet activity of the populous. Nevertheless, compliance is advisable.

Just as the power of technology advances, the role it plays in people’s lives invariably grows more central. Technology giants have an ever increasing amount of data about their users. This has increased the focus on the right to be forgotten, the concept that certain pieces of personal information from the past ought not be retained or made accessible to third parties. Though still a relatively new concept, the right to be forgotten is included in the new EU regulation and it would not be surprising if it becomes more widely accepted.
In some respects, legislation and rulemakings are only half of the data protection equation. The other half is enforcement. Large US technology companies have lately found themselves in hot water with European regulators over potential breaches of data privacy. Facebook, for example, is contending with an onslaught of investigations and lawsuits in at least five EU member states regarding how it accesses, uses and cares for individuals’ personal information. A Belgian court recently barred Facebook from collecting personal information of non-users. The French data protection authority similarly ordered Facebook to cease tracking the online activities of non-users. Facebook is appealing the Belgian decision and has long argued that its European operations are governed by Irish law alone. Thus far, it has failed to extricate itself from this heightened level of scrutiny.

Regulators are not alone in focusing on data protection and privacy. More than ever, individuals are aware of the volumes of their data maintained by companies and concerned by how it is being protected and used. This apprehension is unlikely to fade, moreover, as media reports regularly highlight recent data breaches, the unexpected and often unnerving ways companies are using personal data and the lengths governments go to in order to capture and analyze data.

Not only do people feel as though they have lost control over how their personal data is collected (91% of Americans in a recent Pew study), but they also are deeply skeptical of the application of that data to commercial purposes. This has serious implications for businesses: In another study, by the National Cyber Security Alliance, 89% of Americans said that they avoid companies that they do not trust to safeguard their privacy. Data security and respect for customer privacy has become a competitive differentiator. Just as profound, individuals are increasingly vigilant and proactive when it comes to making sure that their data is protected in accordance with the law, scrutinizing privacy policies and making regulators aware of privacy gaps.

The activist spirit has proven powerful. In fact, it was an individual, Max Schrems, who mounted the legal challenge that ultimately invalidated the EU-US safe harbor agreement. Schrems, an Austrian student and privacy activist, citing revelations from Edward Snowden, argued that his Facebook data stored in the United States was subject to US government surveillance without adequate legal protections. His successful challenge and the resulting shakeup of US-EU data sharing demonstrates the power of individuals who care about their privacy. All companies, regardless of size, must be proactive to ensure compliance and, where possible, positive public relations when it comes to privacy and data protection.
Recommended Steps to Assure Compliance

Given the stakes of protecting customer data and complying with all applicable privacy laws, it is incumbent on businesses to do everything they reasonably can to be good and compliant stewards of personal data. First and foremost, businesses should develop rigorous privacy and data protection policies that adhere to all applicable laws. Depending on the jurisdictions in which the company operates, it may be necessary to develop multiple policies, each tailored to an individual country’s specific laws and each ensuring internal controls.

So what should these policies contain? Though they will differ between companies and across geographies, they generally must address the collection, maintenance and transfer of data. Ownership of certain responsibilities is also an important consideration. Most countries are introducing data breach notification requirements, and many more have requirements for a designated privacy officer. India’s 2011 Information Technology Rules, for example, require the designation of a “Grievance Officer.”

Compliant data protection begins with the collection process. You must ensure that the data subject is fully informed about what data you will collect and how it will be used, and that the data collected is relevant and necessary to your purposes. These disclosures should be documented along with evidence that the subject gave his or her consent. (Some prominent US multinationals such as Google and Facebook have been in legal trouble for failing to fully notify individuals of all the ways in which their data will be used, including using data to analyze online behaviors.) In addition, you must provide subjects the opportunity to opt out of direct marketing as prescribed by law.
Properly maintaining data once it has been collected is also critical. The security of the data must be safeguarded with adequate security measures, both physical and technological, including everything from requiring complex passwords to using a strong firewall to monitor your network for intrusions or improper data leakage. In addition, proper maintenance requires governing who has access to data, how long it is retained and how it is destroyed.

Your responsibilities as a data controller do not end at your server’s firewall. They extend well beyond that to include third parties with which you share the data. Even in jurisdictions that have expanded responsibility beyond controllers to processors, data controllers are not indemnified from liability should their third-party partner violate data protection laws. Thus, it is important to include data protection clauses in contracts with third parties. It is also necessary to verify that third parties are abiding by their obligations to protect data that you control.

You must also be cognizant of your responsibilities should a data breach occur. Depending on the jurisdiction and the nature of the breach, you could be required to notify affected data subjects.

For companies that share data between the United States and Europe, navigating data collection and storage following the demise of safe harbor can be confusing. Until the EU-US safe harbor agreement is replaced, US companies have three options: Cease the collection of Europeans’ data and destroy the data currently stored in the United States; store the data in the EU, thus obviating the need to transfer the data in the first place; or, use one or more of three possible workarounds to continue current data transfer practices. As the first of these options is likely a non-starter for most, we will focus on the latter two.

Since the invalidation of safe harbor makes it more difficult to store and process the data of Europeans in the United States, one option is to simply keep the data in Europe. Amazon and Microsoft have both moved to do just this, with Amazon storing customer data in Dublin and Frankfurt and Microsoft recently announcing plans to go a step further, both storing its data in Europe and ring-fencing European data in such as a way as to prevent US intelligence agencies from gaining access. Making such changes will entail significant logistical and technological efforts and may well be out of reach for all but the largest companies.
This leaves the third option, which is a series of workarounds endorsed by the European Commission. Transferring data to the United States is permitted outside of safe harbor if the data subject consents to the transfer. Unfortunately, the consent must be secured each time data is transferred, which makes it an untenable strategy for many scenarios. Alternatively, the transfer is permissible if the receiver of the data has signed a qualifying data transfer agreement that binds it to the same data privacy standards and liabilities as apply to EU data controllers (referred to as EU Standard Clauses). Finally, data can be transferred if the data controller has in place Binding Corporate Rules (BCRs) that apply consistent and EU-compliant data protections across all group companies in an organization. Note that BCRs are only an internal measure and do not facilitate the transfer of data to a third party.

For now, business leaders have reason to hope that these additional measures will not be required for too much longer. After a lengthy and urgent negotiation, officials from the European Union and United States announced that they had agreed on a framework to replace the safe harbor pact. The framework, the final language of which must still be worked out and approved, provides for the transfer of EU data to the United States with supplemented privacy safeguards. Among other provisions, the framework, which will be referred to as the EU-US Privacy Shield, subjects companies to heightened privacy standards and provides for regular reviews of their practices. In addition, the United States provides assurances that intelligence services will only access the data “subject to clear limitations.” Finally, the shield gives Europeans access to a dispute resolution process should they feel their privacy is violated and requires the United States to create an ombudsman to monitor surveillance by its intelligence agencies. As is so often the case, the devil is in the details so we must wait until a final agreement is drafted and approved to be sure of the best data-sharing model. (Final agreement likely won’t be until mid-2016 at the earliest.)
A point that many US multinationals fail to appreciate is that the safe harbor arrangements were only ever effective in permitting EU data to be processed in the US. For EU transfers to other non-EEA countries, the workarounds described above (i.e., EU Standard Clauses, BCRs and consent) have always been and continue to be required.

We hope this playbook has furnished a high-level understanding of what data protection policies should contain. However, simply writing policies is insufficient to ensure compliance. Businesses must take measures to ensure that policies are properly executed. This means everything from translating policies into local languages for your workforce to instituting a meaningful training program. If the old adage that culture trumps strategy is true, it must be doubly true that culture trumps policy. Thus information technology, legal, compliance, human resources and finance departments along with business line leadership ought to make protecting personal data a point of professional pride.

Conclusion

Digital privacy and data protection are among the most important and fast changing issues facing international businesses today. With frequent reports of fresh breaches of customer data and novel (and often unnerving) applications of private data as well as revelations of government surveillance, these matters are unlikely to fade from public consciousness anytime soon. This notoriety, in tandem with rapid advances in technology and equally rapid advances in cyberattacks, is fueling significant changes to data protection laws, both in the form of stricter laws and tougher enforcement.

In this dynamic regulatory landscape the stakes have never been higher: legal penalties, both financial and otherwise, are growing; consumer awareness is mounting; and a company’s ability to protect its customers’ privacy is increasingly a point of competition. Given these challenges, it is critical to know the laws of every country in which you operate, to ensure that you have in place policies and procedures to comply, and that you are actively monitoring changes to laws and responding appropriately.
Resources

Blog Articles


Checklists

Webinars
“Data Protection Requirements in a Shifting Global Regulatory Landscape,”

“European Data Protection Requirements Post-Safe Harbor: Now What?,”
About Radius’ Advisory Services Team

If you’re concerned about protecting your company from data protection risks or if you’re facing other international challenges, Radius’ seasoned advisory team can help you understand your options and recommend practical, compliant solutions.

Our advisors are senior practitioners with real-world experience in international expansion and operations. They include former Big Four international consultants, CPAs, auditors, lawyers, international HR experts, business school graduates and tax specialists. Many have broad expertise in functional and geographic areas, and many have niche specializations in subjects such as data protection, anti-bribery legislation, HR obligations, indirect tax and transfer pricing.

Let us help ensure that your international offices are in compliance with all applicable laws, that you’ve completed all necessary registrations, and that you’ve developed and implemented optimal policies and procedures to reduce risk and gain a competitive advantage.

For information on how Radius’ experts can help, contact us.

About Radius

Radius helps companies expand and win globally. Clients from startups to larger multinationals take advantage of Radius’ international accounting, finance, banking, tax, HR, legal and compliance support to simplify their core operations, reduce their risk exposure and improve the management and control of their overseas businesses.

Radius delivers support and expertise through managed services, advisory services and OverseasConnect, our integrated cloud-based software platform, to create solutions that meet the needs of over 600 clients operating in 110 countries around the world. Headquartered in Bristol, UK with offices in the US, Brazil, China, India, Japan and Singapore, we are the global growth experts. For more information, please visit www.radiusworldwide.com.