VISTRA

Data Protection Playbook

Contents

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.

Introduction

In 2017, hackers gained access to American credit bureau Equifax's network. The breach compromised the personal data of 147,000 customers and included Social Security numbers, payment card data, dates of birth and other personal information.

Two years later, Equifax agreed to pay $575 million — and potentially up to $700 million — in a settlement for its "failure to take reasonable steps to secure its network."

The Equifax hack and related penalties are far from isolated incidents. In 2020, the US Office of the Comptroller of the Currency assessed an $80 million penalty against Capital One for the bank's "failure to establish effective risk assessment processes" when migrating data to the cloud and "failure to correct the deficiencies in a timely manner." There are countless other examples in jurisdictions around the world.

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 a result, 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.

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 on the next page.

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. Historically, data controllers have had to shoulder this responsibility. In some cases, however, that responsibility has been shared with data processors. Australia, for example, is one of a limited set of countries whose laws have for years not distinguished between data controllers and data processors, which means that the latter can be held responsible for breaches of the law. Much more common had been the approach taken by the EU in Directive 95/46/EC, which placed full statutory responsibility and liability for the protection of personal data with the data controller. Thus, in places like the EU where responsibility rested with the data controller, data processors' exposure was generally limited. That has changed.

The 8 Principles of Data Protection

1.

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.

2.

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.

3.

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.

4.

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.

5.

The Security Safeguard Principle

Holds that personal data should be safeguarded against loss, unauthorized access and disclosure, among other potentially adverse outcomes.

6.

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.

7.

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."

8.

The Accountability Principle

Charges data controllers with compliance with the OECD principles.

Important Developments in Privacy and Data Protection

Revisions to the EU data protection regime have expanded 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.)

One of the most newsworthy examples 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 centres.) 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 US-EU Safe Harbor Framework 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 has significantly intensified its data protection regime. Over the period 2016-2018, it incrementally replaced 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) — has strengthened data protection for individuals and unified

The European Union has significantly intensified its data protection regime. Over the period 2016-2018, it incrementally replaced 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) — has strengthened data protection for individuals and unified data protection across member states.

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, including 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 $1.6 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 GDPR 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 found themselves in hot water with European regulators over potential breaches of data privacy. Facebook, for example, has contended 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 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 has long argued that its European operations are governed by Irish law alone, but 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 data breaches, the unexpected and often unnerving ways companies are using personal data and the lengths governments go to in order to capture and analyse data.

Not only do people feel as though they have lost control over how their personal data is collected (91 percent of Americans in a Pew study), but they also are deeply sceptical 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 percent 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 US-EU 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.

89%

of Americans said that they avoid companies that they do not trust to safeguard their privacy

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 analyse online behaviours.) 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.

In the wake of the European Court of Justice's (ECJ's) 2015 ruling that declared the Safe Harbor Framework invalid, thousands of US-based organizations volunteered to participate in the EU-US and Swiss-US Privacy Shield Frameworks. These frameworks were approved in 2016 and 2017 respectively and gave companies a means to comply with the GDPR when sharing data between the EU and the US, and with the Swiss Federal Act on Data Protection when sharing data between Switzerland and the US.

In July 2020, however, the ECJ struck down the EU-US Privacy Shield, finding that it failed to protect individuals' rights to privacy, data protection and access to remedy. The ECJ's ruling — known as the Schrems II decision — followed a ruling by the High Court in Ireland, which had referred certain questions to the ECJ about the validity of the European Commission's standard contractual clauses (SCCs) and the Privacy Shield. (The SCCs contractually bind non-EU or EEA data receivers to the same EU data privacy standards and liabilities that apply to EU data controllers.) The ECJ's decision confirmed the validity of the SCCs, but invalidated the Privacy Shield.

While the ECJ did find the standard contractual clauses valid, the Court raised concerns about SCC usage. In particular, there may be cases in which national laws prevent the safeguards from being effective.

In order to comply with the GDPR post-Privacy Shield, companies that transfer personal data from the EU to the US must put in place alternative compliance mechanisms.

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.

Recommended actions to take

Identify affected personal data

A company that transfers data from the EU to the US must determine whether its transfers are affected by the Schrems II decision. A company is likely to be affected if it is: a US company that receives data from the EU (such as a US parent with a European subsidiary or European-based customers or suppliers); or a European company that sends personal data to the US (whether to a group company, customer or supplier); or uses cloud software with servers in the US.

Implement GDPR-compliant data processing and transfer agreements

Companies affected by the ruling should implement International Personal Data Processing and Transfer Agreements that incorporate the standard contractual clauses or another appropriate compliance mechanism.

Review other relevant policies and take other actions as needed

For example, companies may also need to review and update external and internal privacy policies where they refer to transfers of personal data from the EU or provide updated data protection training to employees.

Conclusion

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.

About Vistra

With a laser focus on minimising risk and enhancing efficiencies, Vistra provides expert advisory and administrative support to Fund, Corporate, Capital Market and Private Wealth clients; helping capital flow, protecting investors and safeguarding assets across multiple industries.

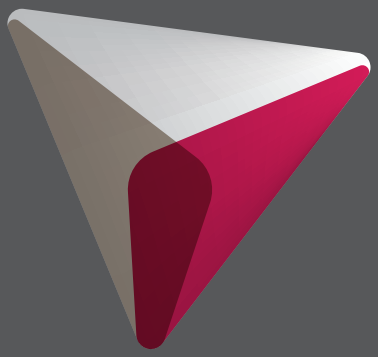
Driven by a high-performance culture of continuous improvement, our hands-on involvement and cutting-edge technology enables organisations to act with speed and confidence as we manage, control, simplify and transact their business activities.

From our physical presence in 46 jurisdictions across Asia-Pacific, Europe, the Americas, Middle East and Africa, we manage over 200,000 legal entities. Our clients entrust us to administer assets valued at more than US$370 billion.

Vistra counts 4,700 professionals as colleagues. Driven by a culture of high values, learning, continual improvement and focus on operational excellence, we work seamlessly with our clients for the long-term. We count 30% of the top 50 Fortune Global 500 companies and 60% of the top 10 private equity firms as our clients and partners.

Through our deep understanding of risk and the opportunity this brings, we deliver the confidence and security our clients and the markets need to seize a world of enduring opportunity.

For more information, please visit www.vistra.com



Registered office
Vistra
19/F, Lee Garden One
33 Hysan Avenue
Causeway Bay, Hong Kong

Tel +852 2521 3661
Fax +852 2845 919
enquiries@vistra.com

@vistra
@vistragroup

vistra.com