wiley

NEWSLETTER

A Privacy and Security Checkup for 2018

January 2018

Privacy in Focus®

Privacy and security are increasingly complicated compliance and operational requirements across a growing range of companies and industries. An enormous profession has grown up over the past 15 years to advise companies on addressing these issues. These concerns must be addressed not just when new laws and regulations emerge and when companies enter new fields; they also require ongoing and almost constant vigilance. For most companies, here are the key items you should use for your company's privacy and security checkup for 2018, to make sure you are keeping abreast of this challenging and risky area.

The European Union's GDPR

The European Union's new General Data Protection Regulation (GDPR) – which takes effect in May 2018 – is the biggest privacy and security story of this year (and the last, and probably the next as well). Enormous sums of money will be spent by companies across the globe to bring themselves into compliance with this new set of requirements, which update and expand on the existing EU data protection rules.

The first step for any company is to determine if the GDPR applies. These provisions will apply not only to the obvious entities – organizations located within the EU; they also will apply to organizations located outside of the EU if they offer goods or services to, or monitor the behavior of, EU data subjects. This means that – generally – the GDPR applies to all companies processing and holding the personal data of data subjects residing in the European Union, regardless of the company's location. If this applies to your company – through employees, customers, business contacts, and

Practice Areas

Privacy, Cyber & Data Governance

even service provider arrangements – this is a substantial undertaking. It needs to be pursued with serious effort and a thoughtful approach to both compliance and appropriate risk management, particularly at this late date.

International Data Transfer

In addition to the GDPR (and other "in country" data protection requirements around the world), many companies also will need to think about how to move personal information from these countries to other countries outside of the geographic regions subject to the law (e.g., outside of the European Union), particularly data transfers to the United States. The Privacy Shield program has emerged – after the collapse of the Safe Harbor program – as one vehicle to transfer data from the EU to the United States. There also are options related to model contract clauses and binding corporate rules. Selecting the appropriate option for your company requires thought, strategy, and attention to operational considerations. There are meaningful compliance obligations and, increasingly, these data transfer obligations become critical elements of business contracting. There are similar programs emerging in other countries and regions around the world (such as the emerging APEC Cross-Border Privacy Rules System). While the United States does not currently have significant restrictions on offshoring U.S. data, pay attention to whether and how this is happening for your company's personal information as well.

Overall, most companies of any significant size need to be in compliance with international privacy and security laws and to develop an appropriate and efficient process for transferring data out of other countries and managing the flow of data into and out of the United States.

Data Security Needs

Data security is an increasingly regulated area, both for specific industries (e.g., health care and financial services, along with all of their vendors), and broadly through regulation by the Federal Trade Commission (FTC) and the state Attorneys General. Data security requirements are emerging around the world as well. At the same time – despite broader regulation and increasingly stringent contractual requirements – security breaches remain an ongoing and growing problem. Because of these breaches – and the associated risks of litigation, adverse publicity, business complications, and potential enforcement – it is critical to remain at or ahead of the curve on actual protections for the security of personal information. Companies should undertake a regular security review. This can include formal, companywide assessment, and other kinds of ad hoc or targeted reviews. However, these reviews cannot be put off indefinitely – each day without attention to these issues creates realistic risks. The emerging best practice is to conduct a meaningful review at least once a year, with other ongoing evaluations as developments require. Make sure you have addressed any new acquisitions, new offices, updated systems, or other meaningful changes to your business environment. Read through the FTC and HHS Office for Civil Rights settlements to identify specific problem areas faced by others – and make sure you do not have the same problems. Appropriate attention to data security requires constant vigilance.

Privacy Update on Data Collection

While compliance with data privacy requirements may not always require the same kind of constant attention as data security (for example, a data access plan for consumers from five years ago may still be good enough today), most companies revise their sources of data over time, and collect, use, analyze, and disclose differing and broader kinds of personal information as business needs increase and technological opportunities expand. So, it is critical to ensure that your privacy policies appropriately reflect the information you are gathering and using today, not what you collected five years ago. Data is coming into your company from new sources – and your marketing teams and many others are moving aggressively to capture, analyze, and act on the implications of this data. It is critical for a General Counsel and privacy officer to understand any new sources of data and to be able to evaluate thoughtfully how this new data is being used by your company.

Social Security Numbers

While most privacy laws cover a broad range of personal information, not all information is created equal. In the United States, the single most "risky" piece of personal information is the Social Security Number (SSN). A security breach involving an SSN almost automatically requires notice to individuals, generates attention from regulators, and leads to litigation. Despite these concerns, in my experience, most companies still collect, use, and disclose SSNs based on the accidents of their history – often for reasons and in projects that make no sense today. *Every company should undertake a project to identify every place in the company where an SSN is collected, used, stored, or disclosed.* You will find that many of these are unnecessary or inappropriate for any reasonable purpose. Every step you can take to reduce the presence of SSNs in your company materially improves the protections for your company, its employees, and its customers.

Complaints/Security Incidents

Many privacy and data security laws and regulations operate primarily in theory – you take actions to reduce or eliminate potential risks and specific potential concerns. So, where the rubber meets the road is when these potential risks and concerns come to fruition. This typically means a security breach or a consumer complaint. Make sure that your company has an appropriate response mechanism for these developments. The goal should not be to stifle further questions – it should be to identify a potential problem, determine if there are actual problems, fix these problems, and take steps to ensure that they do not happen again. By taking appropriate, thoughtful and, often, aggressive action, companies can protect themselves and their audiences. Moreover, make sure you have evaluated and learned from complaints and security incidents even if these incidents did not lead to real problems – there often is a "tip of the iceberg" element to these events that can provide useful learning, but many companies miss these opportunities in the ongoing press of business.

Artificial Intelligence, Big Data, and Profiling

One of the hottest issues of the year (and likely going into the next decade) involves how artificial intelligence is changing so many aspects of day-to-day life. Every company needs to be thinking about how it is using all the new data that is being made available from an increasingly broad variety of new data sources. The challenge for many companies – and where an influential privacy officer can be especially important – is to appropriately balance all the differing considerations within a company about this data. Your marketing team wants more data to be used for all marketing purposes. Your strategic and business development teams want to gather data from any source possible, even before really knowing what might be done with it. Companies want to collect as much data as possible, which is antithetical to some of the emerging compliance issues related to data minimization. The rules for big data analytics and profiling are vague at best, and there is much more movement in relevant technology than there is in relevant regulation. So, companies need to assess and understand what big data they are gathering, how they are using it, and the contexts in which they are making decisions – about business operations, individual consumers, or otherwise – in connection with this data. This kind of big data inventory is enormously important to ensure that companies are drawing the appropriate balances and acting reasonably in a context where there are both tremendous opportunities but also significant risks for both individuals and businesses. Ethics is an element of this discussion, whether in a broad altruistic sense or because a bad judgment on data use today becomes a headline or lawsuit tomorrow. So, companies need to be thoughtful about their usage of data even in an environment where regulation may be lacking.

Privacy Policies on Websites and Elsewhere

In connection with understanding how big data and artificial intelligence are changing your business, one of the places where these developments impact companies directly is in how their websites are used. Advertising and analytics vendors are using more and more data generated through your website, and generated about your website users, with increasingly convoluted and complicated evaluations and disclosures. You should review your website privacy policies to ensure that they are fully and accurately describing how your site uses, gathers, and analyzes personal data (and any data that can be connected to an individual or a specific device). While the rules are evolving, most legal principles involving websites permit broad use and disclosure of information as long as the use and disclosure are accurately and completely defined in a website policy. So, if your business activities are moving faster than your policies, you run a risk that your policies can be used against you. *An annual checkup of your website privacy policy is critical.* You should also evaluate how this policy applies to your subsidiaries and any related companies, as well as how privacy policies are viewed around the world.

Wellness Programs

Most companies that provide health care benefits to employees are subject to at least some of the privacy and security provisions of the HIPAA rules. If your company self-insures these health care benefits, then you are subject to all of HIPAA, including the full HIPAA Security Rule. This is not new – these requirements have applied since HIPAA first went into effect. It is still surprising, however, how many companies are not aware of these HIPAA obligations and have not fully implemented an effective HIPAA compliance program.

What is new – and makes these HIPAA risks even more important – are the privacy and security implications of wellness programs. More and more companies are implementing wellness programs, with expanding roles, benefits, and (sometimes) penalties. Vendors are obtaining more data about your employees. There are new opportunities to gather and use data through a broad variety of mobile applications and wearables. Wellness programs often intersect with other data-monitoring efforts by employers using new technology. And companies are increasingly looking for ways to incorporate wellness ideas across a broader range of employees and in a broader range of situations. Often, this involves efforts to integrate wellness program data with other corporate data. This is a significantly risky area for privacy. The rules are confusing – including the basic question of whether your wellness program is even subject to the HIPAA rules (probably not, if all employees can participate). *Your company should review the current activities of your wellness program, including how data is generated, the benefits/penalties for employee participation, and how the data is being used and integrated with other personal data.*

Due Diligence/Acquisition Integration

Companies also need to make sure that they have appropriately integrated any recent business acquisitions into their overall privacy and security program. Think broadly – not only pure purchases, but new offices, additional product lines, and a full range of business changes that can alter your privacy and security risk profile. You may have protections in a purchase contract from privacy and security problems – but the resulting publicity and potential government enforcement will be your issue, regardless of the contract language. Make sure that you have thought about these issues during the due diligence process (a sophisticated privacy due diligence review is increasingly important), and then follow through after the acquisition to make sure that the right changes are being made and that any activities are consistent with your overall corporate privacy and security program.

Some Final Thoughts

Privacy and security issues need to be on the radar screen for virtually every company – where you have information about customers, employees, or others, whether you operate only in the United States or around the world, and regardless of your industry. While a thoughtful and effective initial privacy and security compliance program is a useful and necessary first step, it is critical to make sure that your program is keeping pace with the enormous range of technological, regulatory, and operational issues affecting most businesses today. This checkup list is likely to apply to your company – at least in part – regardless of who you are. For your company, use this as a starting point but make sure that you are on top of developments in this constantly changing area that impact your specific business operations, your business partners, your customers, and the broad range of individuals and companies that you deal with in your full slate of activities.