HBR
CONSULTING

Creating a Culture of Privacy

Complying With Domestic and Global Requirements by Changing the Way We Value Data Privacy

hbrconsulting.com | info@hbrconsulting.com | 312.201.8400

advisory | managed services | software solutions | insights

Introduction

The General Data Protection Regulation (GDPR) has raised the stakes for how companies handle data, with impacts extending far beyond the EU. Organizations around the globe have been on high alert to bring their data management practices into compliance with the new law, seeking to avoid its significant fines and penalties for noncompliance. Yet many U.S. organizations approach their GDPR compliance initiatives with a checkmark mentality, creating laundry lists of activities without changing their underlying culture or values regarding data privacy. For these companies, privacy-related tasks are "checked off" the list and, in some cases, promptly forgotten again.

This reflects a fundamental difference, on a cultural level, in how organizations in the U.S. consider privacy. That difference poses unacknowledged challenges to how these organizations approach and attain true, ongoing compliance with the GDPR and the expanding roster of privacy regulations. In many jurisdictions around the world, privacy has long been considered a constitutional right. In the U.S., by contrast, privacy has historically been more of an afterthought, addressed only by a patchwork of narrowly targeted regulations governing specific types of data. The result is that, in a legal sense, the U.S. does not recognize an overall expectation of privacy.

In this white paper, we explain how organizations can design privacy programs that will comply with the stringent requirements of the GDPR by moving away from a checkmark mentality and truly embracing privacy as one of their core values. We will explore the differences in our views of privacy, along with the deep cultural roots underpinning those beliefs, and discuss the critical success factors needed to develop strategies for consistent and repeated practices that will shape the new culture over time.

Approaches to Privacy in the United States

Before we launch into a conversation about data privacy, let's clarify what data we are referring to. The GDPR and some other recent laws have vastly expanded the definition of "personal data" that is entitled to privacy protections. These interpretations encompass not only standard identifiers like names, identification numbers, addresses and contact information but also biometric data, demographic data, descriptive information and any other data that could be used, alone or in combination with other data, to identify an individual. Most U.S. privacy protections are not so broad; they are restricted to standalone identifiers like names and Social Security numbers and specific categories of information like account numbers in a financial setting or patient identifier numbers in a healthcare setting.

The founding fathers did not explicitly contemplate a right to privacy. In fact, the word "privacy" does not appear anywhere in the Constitution. To the extent that the U.S. government does recognize a right to privacy, it has inferred that right based on elements of the Bill of Rights, such as the Fourth Amendment's ban on unreasonable searches and seizures.

General Views on Privacy In The U.S.

This has historically reflected the priorities of U.S. residents. While people in the U.S. cherish the right to be left alone to do as they please in their homes—a right that courts have generally supported—that right to privacy quickly dissipates once a person leaves the home, either physically or virtually.

As a result, there is no single, comprehensive federal law that regulates the collection or use of personal data. Instead, the right to privacy in the U.S. is established by a patchwork of federal laws regulating specific sectors and a host of state laws. These are primarily reactive and breach-oriented rather than proactive and protective, though the most comprehensive U.S. privacy law to date, the California Consumer Privacy Act (CCPA), promises to change this. Additionally, a hodgepodge of other authorities, from nongovernmental agreements to treaties, create a limited right to privacy in the U.S.

> The founding fathers did not explicitly contemplate a right to privacy. In fact, the word “privacy” does not appear anywhere in the Constitution.

Federal Laws and Regulations Governing Privacy In The U.S.

An assortment of U.S. federal laws establish limited rights to data privacy. These include the following:

- The Federal Trade Commission Act (15 U.S.C. §§ 41–58), a federal consumer protection law that prohibits unfair or deceptive practices and that has been applied to offline and online privacy and data security policies;
- The Financial Services Modernization Act, also known as the Gramm-Leach-Bliley Act (GLBA) (15 U.S.C. §§ 6801–6827), which regulates the collection, use and disclosure of financial information by financial institutions such as banks, securities firms, insurance companies and other businesses that provide financial services and products;
- The Health Insurance Portability and Accountability Act (HIPAA) (42 U.S.C. § 1301 *et seq.*), a healthcare law that regulates the protection of patients’ medical information;
- The Children’s Online Privacy Protection Act (COPPA) (15 U.S.C. §§ 6501–6506), which is intended to protect the privacy of children under 13 years old from the collection of their personal information online;
- The Fair Credit Reporting Act (15 U.S.C. § 1681) and the Fair and Accurate Credit Transactions Act (Pub. L. No. 108–159), which amended the Fair Credit Reporting Act; both protect consumer
- Information used by consumer reporting agencies, those who use consumer reports (such as lenders) and those who provide consumer-reporting information (such as credit card companies);

- The Electronic Communications Privacy Act (18 U.S.C. § 2510), which protects private electronic communications from unauthorized wiretapping, and the Computer Fraud and Abuse Act (18 U.S.C. § 1030), which addresses hacking and electronic fraud; and
- The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99), a law that intended to protect the privacy of student education records.

State and Local Laws Establishing Privacy Rights

Currently, all 50 states, plus the District of Columbia, have enacted some form of privacy legislation. The majority of state laws regarding data privacy have been reactive, primarily addressing data breach notification requirements after the fact rather than requiring responsible data use or front-end data protection. But states—and now even cities—are increasingly passing date privacy laws to protect the personal and sensitive information of residents within their jurisdictions; a few have recently enacted laws that give consumers the right to control or limit the information about them that companies may retain or use.

Foremost among the many state regulations, the California Consumer Privacy Act ("CCPA"), effective January 1, 2020, is gaining the most attention. The CCPA provides California consumers with the right to:

- Know what personal information is being collected about them
- Access that information
- Know if their personal information is shared, and with whom
- Know if their personal information is sold and be given the right to opt out of the sale

The CCPA also guarantees that residents cannot be penalized through differential service or pricing, should they choose to exercise their privacy rights, and grants the right to sue under a private cause of action for a data breach, wherein statutory penalties are substituted for actual damages. Given California's prominence as a home for technology companies, it will be interesting to see how the CCPA's provisions migrate across the rest of the country.

States—and now even cities—are increasingly passing date privacy laws to protect the personal and sensitive information of residents within their jurisdictions.

How The U.S. Views Data Privacy

While privacy is important to U.S. citizens, many are pessimistic about just how much protection is afforded their data, believing that they do not, and presumably cannot, have a great deal of control over their personal data. Hampered by a pervasive sense that they may be under surveillance and a (sometimes realistic) lack of confidence in the privacy and security of the records maintained by a variety of institutions in this digital age, U.S. citizens have low expectations for digital privacy. The failure of social media sites, governmental actors, utility providers including phone companies, digital marketers, search engines and others to protect personal data contributes heavily to this defeatism.

In a 2014 survey, Software Advice found that: 61 percent of Americans believe some version of the right to be forgotten is necessary; 39% want a European-style right to be forgotten, without restrictions; and nearly half of respondents were concerned that "irrelevant" search results can harm a person's reputation.

According to a 2019 article by the Pew Research Center, U.S. citizens are distrustful of how businesses collect and share their information. As far back as 2014, a tremendous 91 percent of Americans felt they had lost control over their personal information. However, in 2018, 69 percent of American adults reported using social media, although two-thirds said that current laws are not good enough at protecting people's privacy.

These attitudes toward data privacy differ markedly from those that are prevalent in other countries, especially in the EU.

Global Culture and Expectations Around Privacy

In contrast to the exasperation regarding data privacy in the U.S., European residents are unrelenting in their expectation for protection of personal information.

Global Requirements For Data Privacy

The European view firmly establishes privacy as a universal human right. European survey respondents value their privacy by an overwhelming margin; in a 2017 survey, Digiday found that only 20 percent of European respondents said they were OK with sharing their data with third parties for advertising purposes. Regardless of whether these companies were using that information to develop new services—even services that the respondents might enjoy using—European respondents were not interested in sharing their data. Rather, their privacy mattered substantially more.

Similarly, Europeans resist some of the "why not" arguments that companies have successfully used in the United States. In their view, personal data should not be kept on hand simply because storage is cheap and there's a low cost to retaining that data. Likewise, companies should not process their data even though their algorithms are carefully refined and targeted to particular commercial uses. The right of citizens to have their data safeguarded trumped these countervailing arguments.

In the interest of maintaining the benefits of the digital economy and Europeans' ability to participate in it, European regulators recognized the need to build consumer trust through strict data protection laws. This, in short, led to the provisions of the GDPR. As Elizabeth Denham, Commissioner of the UK's ICO, put it, "This law is not about fines. It's about putting the consumer and citizen first."

To comport with European attitudes about the importance of data privacy, a range of requirements must be met, including these:

- Companies cannot collect personal information without the direct permission of consumers, who must also be given the right to review their data and correct inaccuracies;
- Companies that process data must register their activities and their justifications with the government;
- Employers cannot read private emails of their workers, even when those emails are sent from work;
- Companies cannot share personal information with other companies or across borders without receiving express permission from the data subject to do so; and
- Checkout clerks cannot ask for shoppers' phone numbers.

The critical importance that Europeans place on data privacy is so divergent from U.S. views that it begs the question, how did these opposing views develop?

> In contrast to the exasperation regarding data privacy in the U.S., European residents are unrelenting in their expectation for protection of personal information.

Historical Bases for Europeans' Enhanced View of Privacy

The heightened sensitivity to privacy in Europe may stem, at least in part, from the horror of the Holocaust. During World War II, significant intrusions to citizen's privacy were conducted under the guise of national security. However, these infringements often went far beyond the needs of national security and instead were means to identify individuals of targeted religious, ethnic or political groups. As the Nazi regime rose to power, state control of businesses brought with it state control of information technology. Nazis used public and church records to identify Jews before rounding them up and sending them to concentration camps. In the 1930s, German census workers went door-to-door filling out punch cards that indicated residents' nationalities, native language, religion and profession. These records, counted with early data processors, were used to systematically weed out the Jewish population. Similarly, in the occupied Netherlands, the Nazis exploited official registers of

Dutch citizens to earmark Jews for deportation to death camps. To this day, Europeans see the intrinsic value in safeguarding their personal data.

Another basic divergence in attitude centers around the differences in how business disputes are resolved in European countries versus the United States. In Europe, the state acts as the first line of defense against private wrongdoing. In the U.S., private actors can—and clearly do—sue one another directly. The U.S. approach to information discovery for litigation has no true equivalent in the European court system.

As one example of this difference, a French court previously ruled that Nikon France could not fire one of its employees for performing freelance work on the job. *Nikon France v. Onos*, Cass. Soc. Arret No. 41-6410/2/01 (France 2001). While Nikon France found incriminating emails about the unauthorized work, those emails were marked "personal." They therefore could not be used as grounds for dismissal. In the U.S., by contrast, employees surrender most of their rights to privacy when they enter their place of work or when they use company property.

The misunderstandings between the U.S. and the EU persist today, in the form of ongoing debates about the effect of the GDPR. Many argue that the new regulation will be terrible for business competition, giving large businesses a significant advantage over smaller organizations. Others claim that consumers are suffering due to their inherent mistrust of businesses; they predict that privacy regulations will shift that burden by making businesses think more deeply about what data they collect and why. Needless to say, there is a fair bit of suspicion on both sides of the Atlantic right now. Many in the U.S. view the EU approach as excessive, claiming that it stifles innovation and impedes the flow of information. For their part, many in the EU view the U.S. approach as unprincipled, contrary to individuals' rights and essentially the equivalent of no regulation at all.

Heightened Expectations for Privacy are Expanding

Whatever an organization's individual beliefs about data privacy, the GDPR's effective date marked the beginning of a new era. Already, an avalanche of similar data protection regulations has been unleashed. U.S. organizations must adapt if they wish to continue operating in the global digital economy.

This change is urgently needed, as we are rapidly approaching the third stage of digital behavior change. In the initial naiveté phase, consumers did not really understand how technology could collect their data or how companies would use it. In the careless phase, people saw their data rights or the right to privacy as either unimportant or as an acceptable price to pay to obtain customized online marketing and services. Now, as we enter the demand phase, we are seeing the emergence of a more savvy, engaged and alarmed digital consumer. That evolution gives rise to the current movement to create and enforce consumer rights.

To ensure full compliance with the still-expanding right to privacy, it's not enough to check off tasks on a one-size-fits-all preparation list. Proactive organizations should instead create an organizational culture that truly understands and embraces the importance of data privacy.

Designing an Organizational Culture That Values Privacy

The benefits of data privacy do not flow only to the individual whose data is subject to corporate use. Organizations themselves have a substantial amount to gain by collecting less data and defensibly disposing of unneeded personal data. In a sense, the emphasis on data privacy is one of the best things to ever happen for information governance professionals, since it provides yet one more driver for "defensible disposition."

By focusing on a minimum rather than a maximum data retention window, organizations can now expedite data destruction, winnowing down the data stores they must maintain, secure and pay for. In place of a "culture of keep" where data is retained "just in case," organizations can confidently dispose of outdated data. This further reduces the following:

- Unnecessary e-discovery costs;
- Time and effort spent on excessive collection, review and production;
- The likelihood of a sensitive data breach;
- The delay in finding and retrieving—or the total inability to find—needed information; and
- Data duplication and redundancy.

Of course, keeping less data also reduces the likelihood that an organization will be penalized by costly fines associated with data privacy violations.

Designing Your Approach to Creating a Culture of Privacy

Defensible data disposition depends on clearly defining the legal, regulatory, privacy and operating requirements under which an organization functions. The foundation of data governance is—as it has been—the retention, disposition, preservation, privacy and security of individual pieces of information. Implementation strategies should be built atop that foundation, ensuring that governance requirements are applied to all organizational information, regardless of media or repository. Finally, tactical action plans address the on-the-ground "how" surrounding the performance of those strategies.

Start by knowing where you stand today. Run a privacy risk analysis if you haven't already. Evaluate your policies, practices, roles, responsibilities, accountability structures, training materials and technologies to see where you currently underplay the importance of privacy. Map your organization's data to determine where your most sensitive data can be found. This may be in finance, HR, marketing, sales, customer service or somewhere else altogether.

Avoid the trap of assuming that data security or privacy belong solely in the realm of the IT department. Individual employees are often the "single point of failure" in a security breach, so you need everyone on board with your cultural shift. Build a cross-functional team that incorporates

a diversity of perspectives to ensure you identify and address issues before they arise. Include staff from IT, security, compliance, legal and any business departments or functions that work with private information.

While designing your approach, do not overlook the following critical success factors.

1. **Ensure executive team buy-in and active engagement.** The "tone at the top" will set you up for success—or for failure. Bookend your efforts with a focus on initial as well as continued executive support. You are extremely unlikely to be successful in effecting an organizational culture change without the firm support of your executive team.
2. **Create a sense of urgency.** Educate staff about both the benefits of honoring data privacy and the consequences of failing to do so. Compile some real-life examples where privacy violations damaged an organization's brand, reputation, bottom line or all three.
3. **Build a sense of value.** Figure out how an enhanced sense of data privacy will contribute to your organization's bottom line, and then be sure to communicate that return on investment to your team.
4. **Align the message around data privacy to your organization's guiding principles.** Whether it's your mission, organizational vision, values or another touchstone guidance document, determine how data privacy complements your existing philosophy.
5. **Integrate mindfulness of privacy into your existing business processes.** From new employee orientation to annual training sessions, ensure that privacy permeates your methodology. Revise your employee manual or code of conduct to include the importance of privacy, build "privacy by design" into new system development processes and incorporate privacy impact assessment criteria into your day-to-day operations.

Applying Change Management Principles to Cultural Transformation

It can be helpful to apply the three stages of change management—prepare, enact and maintain—to this cultural transformation.

Prepare for change. Where does your organization stand now with its cultural acceptance of privacy? How does your organization typically respond to change? What has worked in the past when introducing systemic changes? Identify sponsors and change champions—both in the executive office, as mentioned above, and among the ranks—to drive the initiative to create a culture of privacy. Develop or update your policies and procedures as you learn where you can enhance your protection of personal data.

Enact the change. In designing your privacy awareness campaign, focus on your key messages and aim to produce highly visible, consistent and engaging communications around those messages.

Include relatable, real-life experiences and memorable catchphrases such as “If you collect it, you’d better protect it.” Emphasize both multimedia and multi-channel communications with on-demand and in-person training options.

Maintain the change. The goal should be to permanently embed a value of privacy into the culture of the organization—but it’s not enough to “set it and forget it.” Remember the importance of executive support and establish a regular schedule for executive messaging regarding the benefits and consequences of privacy protection. Refresh your organization’s focus through periodic campaigns and internal compliance audits.

Developing a true culture of privacy within your organization will naturally provide GDPR compliance as well as an enterprise-wide appreciation, acceptance of and adherence to data privacy requirements—regardless of their origin.

Connect With Our Experts

To learn more about legal innovation trends or to discuss your organization’s initiatives, please contact us:

Laurie Fischer
Managing Director

O 312.638.5127
E LFischer@hbrconsulting.com

HBR
CONSULTING

HBR Consulting (HBR) delivers advisory, managed services and software solutions that increase productivity and profitability, while mitigating risk for law firms, law departments and corporations. As trusted advisors with deep industry experience, clients partner with HBR to achieve significant, sustainable results.

hbrconsulting.com | info@hbrconsulting.com | 312.201.8400

advisory | managed services | software solutions | insights